

ArcSight™ ESM User's Guide

ArcSight™ ESM 4.5 SP1

April 16, 2009



ArcSight™ ESM User's Guide ArcSight™ ESM 4.5 SP1

Copyright © 2001-2009 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:
<http://www.arcsight.com/company/copyright/>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
11/11/08	ArcSight Express and ArcSight ESM v.4.5	See "Getting Started" on page 5 for information about this release.
04/16/09	ArcSight ESM v.4.5 SP1	See "Getting Started" on page 5 for information about this release.

Document template version: 1.0.2.9

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://forum.arcsight.com

Contents

About this Guide	xxxv
Power User Help Features	xxxvi
Help Display Preferences	xxxviii
Text Conventions	xxxviii
Related Documentation	xxxix
Feedback	xl
 Chapter 1: What's New	 1
 Chapter 2: Getting Started	 5
Quick Start Tools and Content	5
Network Model Wizard	6
Configuring ESM and Using Standard Content	6
ArcSight Express	7
ArcSight Web	7
Getting Started Configuring ArcSight Express	7
ArcSight Express Documentation	8
 Chapter 3: Standard Content	 9
What is Standard Content?	9
Standard Content Foundations	10
ArcSight System Content	11
Shared Resources	12
Anti-Virus	12
Conditional Variable Filters	12
Network Filters	12
Standard Content Packages	13
Navigating to Standard Content	13
Set Up Connectors and Model the Network	14
Standard Content-Related SmartConnectors	15
Network Modeling	16
Apply Standard Asset Categories to Assets	16
Categorize Internal Assets	16
How ESM Determines the Protected Network	16

Categorize Critical Assets	17
Configure Notification Destinations	17
Configure Active Lists	18
Configure Asset Auto-Creation Filters	18
Configure Connector Asset Auto-Creation Controller Filter	19
Configure Device Asset Auto Creation Controller Filter	21
Configure SNMP Trap Forwarding Filter	22
Configure Rules to Send Notifications and Open Cases	24
Configure Rules with Notifications to the Cert Team	25
Configure Rules with Notifications to the SOC Operators	26
Schedule Reports	26
Default Trends Schedule	26
ArcSight Administration Trends	27
Configuration Monitoring Trends	27
Intrusion Monitoring Trends	28
Network Monitoring Trends	28
Workflow Trends	29
How to Enable/Disable Trends	29
Getting Started Using Standard Content	30
Monitoring with Standard Content	30
Active Channels	30
Dashboards	31
Investigating with Standard Content	32
Reporting with Standard Content	32
Chapter 4: ArcSight Express Solution	35
What is ArcSight Express Content?	35
How ArcSight Express Is Organized	36
Set Up Connectors and Model the Network	36
ArcSight Express-Related SmartConnectors	37
Network Modeling	38
Apply Standard Asset Categories to Assets	39
Categorize Internal Assets	39
How ESM Determines the Protected Network	39
Categorize Critical Assets	39
Create ArcSight Express Users	39
Configure Notification Destinations	40
Configure Asset Auto-Creation Filters	41
Configure Connector Asset Auto-Creation Controller Filter	41
Configure Device Asset Auto Creation Controller Filter	42
Configure Rules to Send Notifications and Open Cases	44
Schedule Reports	47
Tuning ArcSight Express Content	48

Chapter 5: Learning Paths	51
For the User	53
ArcSight ESM User Certification Subjects	53
Active Channels	53
Login Process	53
For the Administrator	53
ArcSight Administrative Certification Subjects	53
Access Control Lists (ACLs)	53
Active List Resources	53
Dashboards	53
Data Monitor Resources (statistical)	53
Database Full Response	53
Filters	53
Firewalls, Ports, Switchover Database Cable, Security Domain	54
Reports	54
Resource Editors	54
Resources	54
Rules	54
Rule Actions	54
Shell Commands	54
Secure Sockets Layer (SSL) Communications Encryption	54
Threat Level Formula	55
User Groups (Administrator, Author, Operator)	55
Users	55
Chapter 6: Working in the Console	57
Navigating	58
Navigator Panel Resource Tree	59
Using SmartFolders	60
Creating a Case-Search SmartFolder	61
Creating a Reports SmartFolder	61
Editing Groups	61
Editing a Group	61
Categories Tab	61
Viewing Group Cases in a Grid View	62
Batch Editing	62
Batch-Editing Cases or Connectors	62
Cases Reminder	63
SmartConnector Reminders	63
Reconnecting to the Manager	63
Viewing	63
Viewer Panel	63
Console Look-and-Feel	65

Inspecting and Editing	66
Overview of Inspect/Edit Features and Utilities	67
Searching for Fields in Event Inspector, Resource Editors or CCE	68
Controlling the Console	70
Error and Warning Messages	72
Using the Network Tools	72
Running a Tools Command	72
Network Tool Default Options	73
Adding a Tool	73
Configure (Edit) a Tool	74
Deleting a Tool	75
Staying Informed	75
Using Notifications	76
Acknowledging a Page	76
Acknowledge a Cell Phone Message	76
Acknowledge an E-mail Message	76
Acknowledge Notifications at the Console	76
Using Notes	76
Adding a Note	76
Viewing a Note	77
Deleting a Note	77
Using the Menus	77
File Menu	77
Edit Menu	78
View Menu	78
Window Menu	79
Tools Menu	80
System Menu	81
Help Menu	81
Keyboard Shortcuts (Hot Keys)	82
Moving Copying, Linking, and Deleting Resources	83
Move, Copy, or Link a Resource	83
Delete a Resource	83
Printing from the Console	83
Printing Navigation Tree Views of Resources	84
Printing Resource Definitions	85
Saving as an HTML File	86
Printing Grid Views	86
Printing Conditions Tree Summary	87
Using Column Flip Limit to the Control Format of Grid View Printouts	88
Chapter 7: Monitoring Events	91
Monitoring Active Channels	91

Using Views	91
Selecting a View	91
Changing View Layouts	91
Floating a View	92
Closing one View or All Views	92
Closing all Views Except the Current One	92
Viewing and Using Channels	92
Viewing an Active Channel	92
Sorting Events in an Active Channel	93
Creating an Active Channel	93
Applying a Field Set to an Active Channel	94
Using an Active Channel Header	95
Filtering an Active Channel	95
Saving Copies of Active Channels and Filters	95
Editing an Active Channel	96
Active Channel Options	96
Defining Grid Fields Options	97
Discovering Patterns in an Active Channel	98
Deleting an Active Channel	98
Adding a View Format	98
Changing View Layouts	98
Investigating Views	98
Using an Event Attribute to Show a New Filtered View	99
Refining a Filter with an Event Attribute	99
Adding an Event Attribute to a Filtering Condition	100
Permanently Modifying an Active Channel	100
Showing an Exploited Vulnerability	100
Showing a Targeted Asset	100
Using Field Sets	101
Creating a Field Set	101
Editing a Field Set	102
Sharing a Field Set	103
Using Charts	103
Charting an Active Channel's Contents	103
Charting a Data Monitor's Contents	103
Exploring the Events Behind a Chart	104
Using Grids	105
Monitoring Events in the Grid View	105
Sorting Columns in the Grid View	105
Adding, Replacing, or Removing a Column in the Grid View	105
Sizing a Column in the Grid View	106
Showing or Hiding Grid View Column Text and Icons	106
Exporting Events to a File	107

Choosing Grid View Menu Commands	107
Filtering Grid Views with Inline Filters	109
Customizing Grid Columns	111
Creating a Custom Column	111
Showing a Custom Column	112
Advanced Example: Creating a Custom Column with Velocity	112
Using Dashboards	113
Monitoring Dashboards	113
Loading Dashboards	113
Inspecting Events in Dashboards	113
Displaying Dashboards	113
Rotating Dashboards Automatically	113
Changing Dashboard Layouts	113
Using Dashboard Menu Options	114
Zooming In or Out of Dashboards	114
Fitting all Data Monitors within Dashboards	114
Saving Dashboard Layouts	114
Closing a Dashboard	114
Editing Dashboard Data Monitors	114
Changing a Dashboard's Layout	114
Managing Dashboards	114
Creating a Dashboard	114
Adding a Data Monitor to a Dashboard	115
Data Monitor Display Formats	115
Editing a Dashboard	115
Deleting a Dashboard	115
Managing Dashboard Groups	116
Creating a Dashboard Group	116
Renaming a Dashboard Group	116
Editing a Dashboard Group	116
Moving or Copying a Dashboard Group	116
Deleting a Dashboard Group	116
Using Data Monitors	117
Creating a Data Monitor	117
Editing a Data Monitor	118
Deleting a Data Monitor	118
Enabling or Disabling a Data Monitor	118
Enabling or Disabling a Data Monitor from the Editor	119
Enabling or Disabling a Data Monitor in the Navigator	119
Overriding a Data Monitor's Last State	120
Data Monitor Types	120
Managing Data Monitor Groups	122
Creating a Data Monitor Group	123

Renaming a Data Monitor Group	123
Editing a Data Monitor Group	123
Moving or Copying a Data Monitor Group	123
Deleting a Data Monitor Group	123
Enabling or Disabling Data Monitor Groups	123
Monitoring Active Lists	124
Viewing Active List Contents	124
Refreshing Active List Views	124
Adding to or Subtracting from an Active List	124
Filtering Active Lists	124
Editing Active Lists	124
Clearing Active List Views	125
Customizing Active View Grid Columns	125
Active List Grid Context Menu Commands	125
Graphing Attacks	125
Creating Static Event Graphs	125
Creating Live Event Graphs	126
Event Graph Notes	127
Pattern Discovery	127
Creating a Profile	128
Editing a Profile	130
Deleting a Profile	130
Profile Properties	130
Taking a Snapshot	131
Pattern Options	132
Scheduling a Snapshot	133
Showing a Snapshot	133
Deleting a Snapshot	133
Exploring a Snapshot	133
Inspecting a Pattern	135
Creating Rules	136
Showing Event Graphs	136
Showing Related Events	136
Annotating Patterns	136
Viewing a Pattern	137
Viewing a Filtered Pattern	137
Deleting a Pattern	137
Chapter 8: Selecting and Investigating Events	139
Handling Events in Grid Views	139
Selecting Events to Investigate in a Grid View	139
Inverting Event Selections in a Grid View	139
Selecting Events with Matching Cells in a Grid View	139

Exporting Data Fields to a .CSV File	139
Showing Event Details and Rule Chains	140
Displaying Event Details	140
Displaying Simple Event Rule Chains	140
Displaying Detailed Event Rule Chains	140
Displaying Correlation-Event Rules	140
Executing or Clearing Rule Actions in a Grid View	140
Launching Event Details in a Browser	140
Hiding Empty Rows in the Event Inspector	141
Investigating Session Events	141
Investigating a Session Event	141
Collaborating on Events	141
Viewing Annotations for an Event	142
Annotating an Event	142
Event Annotation Fields	142
Comments Field	143
Mark Similar Events Fields	143
Creating New Stages	143
Stage Editor Fields	143
Editing Stages	144
Showing Event Payloads	145
Finding Payloads	145
Retrieving Payloads	145
Preserving Payloads	145
Discarding Payloads	145
Saving Payloads to Files	145
Viewing Payloads in Other Viewers	146
Getting Knowledge Base Articles	146
Displaying Articles from the Knowledge Base Window	146
Displaying Articles from a Grid View	146
Displaying Articles from the Event Inspector	146
Chapter 9: Filtering Events	147
Creating Filters	147
Creating a New Filter	148
Changing a Filter	148
Creating an Inline Filter	148
Debugging Filters to Match Events	151
Applying Filters	155
Adding Filters to Resources	155
Applying Resources as Filters to Active Channels	155
Removing a Filter Condition or Resource	155
Investigating Views	156

Using an Event Attribute to Show a New Filtered View	157
Refining a Filter with an Event Attribute	157
Filtering Out ArcSight Events or Other Customizations	157
Adding an Event Attribute to a Filtering Condition	158
Permanently Modifying an Active Channel	159
Showing an Exploited Vulnerability	159
Showing a Targeted Asset	159
Modifying Views	159
Modifying a View Inline	159
Undoing an Inline Filter	159
Permanently Modifying a View	160
Chapter 10: Query Viewers	161
What are Query Viewers?	161
Navigating to Query Viewers	163
Pre-Built and Custom Query Viewers	163
Standard Content	163
Custom Query Viewers	164
Tweak Query Viewers as Needed	164
Query Viewers Need Base Queries	164
Running Queries and Viewing Results	164
Working with Query Viewer Results	168
Results in Table Format	168
Results in Chart Formats	172
Filtering Query Viewer Results	173
Adding a Filter	173
Adding Query Viewers to Dashboards	174
Making Query Viewer Results Available to ArcSight Web	175
Adding Query Viewers as Startup Views	175
Generating Reports from Query Viewers	176
Defining and Using Baselines	177
Why Baselines are Useful	178
Planning for Baseline Comparisons	179
Adding a Baseline	179
Comparing Displayed Results to a Baseline	181
Show or Hide Baseline Columns	182
Sort Baseline Data	182
Filter Baseline Data	183
Removing a Baseline	183
Customizing Query Viewers	184
Creating a New Query Viewer	184
Defining Query Viewer Settings	185
Query Viewer Attributes	185

Query Viewer Fields	189
Query Viewer Variables	192
Query Viewer Drilldowns	193
Editing a Query Viewer	197
Deleting a Query Viewer	197
Example Queries for Common Scenarios	197
Basic Analysis High Level Summaries	198
Analyst's First View of Events	198
Drill-Down Example	200
How the Drilldowns are Built	202
Non-Event Analysis Example	203
Baseline Analysis for Data Comparison	203
History Analysis Example	203
Chapter 11: Building Reports	205
Understanding Reporting Workflow	205
1. Build a Query	206
2. Build a Trend (Based on a Query)	206
3. Build a Query (Based on a Trend)	207
4. Select or Design a Report Template	207
5. Create a Report	207
6. Run a Report	208
7. Archive and Maintain Reports	208
Managing Dependencies for Reports Resources	209
Using Report Templates	209
Navigating to Templates	209
Using Standard Templates	210
Applying a Template to an Existing Report	210
Creating a New Report Based on a Template	211
Copying a Template	211
Opening the Designer to Edit a Template	211
Designing Custom Templates	211
Opening the Template Designer to Edit Existing Templates	211
Creating a New Template	212
Template Designer User Interface	212
Setting Report Page Options	219
Designing Report Flow Layout	220
Designing Report Tabular Layout	222
Building Report Elements into a Template	223
Building Queries	228
How Queries Work	229
Using Queries and Trends Together for Reports	229
Using Queries in Query Viewers	229

Building a Query	230
Creating a New Query	230
Defining Query Settings	230
General Attributes	231
Query Fields	233
Query Fields: Select	233
Query Fields: Order By	234
Query Fields: Group By	237
Creating Conditions on a Field	239
Editing a Query	241
Building Trends	241
How Trends Work	241
Snapshot Trend	242
Interval Trend	242
Query-Trend Relationships in Reporting	242
Building a Trend	243
Navigating to Trends	244
Creating a New Trend	244
Defining Trend Settings	245
Trend Attributes	245
Trend Schedule	248
Trend Parameters	249
Testing a Trend	249
Viewing Trend Data	249
Refreshing Trend Data	250
Editing or Viewing a Trend Definition	251
Using a Trend in a Query or Report	251
Creating Reports	251
How Reports Work	251
Building a Report	252
Navigating to Reports	252
Creating a New Report	252
Defining Report Settings	253
Report Attributes	253
Report Templates	254
Report Data	257
Report Parameters	267
Setting Special Parameters for Running Large or Complex Reports	270
Setup and Parameters to Generate PDF Reports with Asian Fonts	271
Editing a Report	272
End-to-End Reporting Examples	272
Quick Start Example of Creating a Simple Report with the Wizard	273
Advanced Reporting Example Overview	276

1. Build the VPN Logins Outcome Query	276
2. Build the VPN Logins Outcome Hourly Trend	278
3. Filter the Trend Data (Login Attempts, Successes, Failures)	280
4. Create the VPN Logins Outcome Report on Trend Data	282
5. Run the Report	285
Chapter 12: Running and Managing Reports	287
Running Reports	287
Running a New or Archived Report	287
Running a Defined Report	288
Run-Report Options	289
Report Parameters	289
Displaying an Archived Report	290
Running a Delta Report	290
Running Reports from a Grid View	291
Running a Rule-Context Report from a Grid View	291
Running an Event-Context Report from a Grid View	291
Running a Channel Report from a Grid View	291
Managing Reports	291
Editing a Report	291
Creating Focused Reports	292
Importing and Exporting Reports	292
Importing Reports	293
Exporting Reports	293
Moving or Copying a Report	293
Managing Report Groups	293
Creating a Report Group	293
Renaming a Report Group	294
Editing a Report Group	294
Moving or Copying a Report Group	294
Deleting a Report Group	294
Archiving Reports	294
Archiving a Report	294
Parameterized Report Entries	296
Viewing an Archived Report	297
Scheduling Report Tasks	297
Scheduling Individual-Report Archiving	297
Scheduling Report Archiving by Resource Group	298
Editing a Report Archiving Schedule	299
Editing Report Archiving Parameters	299
Deleting a Report Archiving Schedule	300

Chapter 13: Rules Authoring	301
Choosing How Rules Work	301
Managing Rules	302
Creating Rules	302
Editing Rules	302
Moving or Copying Rules	303
Deleting Rules	303
Managing Rule Groups	303
Creating Rule Groups	303
Renaming Rule Groups	303
Editing Rule Groups	303
Moving or Copying Rule Groups	304
Deleting Rule Groups	304
Specifying Rule Conditions	304
Creating New Rule Conditions	304
Adding Filter Conditions to Rules	305
Adding Asset Conditions to Rules	305
Adding Vulnerability Conditions to Rules	306
Negating Event Conditions	306
Creating Matching or Join Conditions	306
Editing or Deleting Join Data Field Conditions	308
Specifying Rule Thresholds and Aggregation	308
Setting or Changing Rule Thresholds	308
Aggregation Time Criteria	309
Deleting Aggregation from a Rule	310
Creating Rule Actions	310
Adding a Rule Action	311
Editing a Rule Action	311
Remove a Rule Action	312
Activating or De-activating a Rule Trigger	312
Enabling or Disabling a Rule Action	312
Threshold Triggering Options	312
Rule Actions	314
Applying Rule Actions	315
More Rule Actions	315
Enabling and Disabling Rules	317
Enabling Rules	317
Disabling Rules	317
Automatically and Manually Disabled Rules	317
Disabling Rule Components	318
Importing and Exporting Rules	319
Scheduling Rules	319
Scenarios for Using Scheduled Rules	319

Scheduling a Rule Group	320
Example of a Scheduled Rule (Badge Swipes and Logins)	322
Testing Rules	324
Testing a Rule from the Rule Editor	325
Showing Rule Errors	326
Verifying Rule(s) with Events	326
Verify Rule(s) from the Resource Tree	326
Deploying Real-time Rules	329
Deploying a Rule	329
Removing or Un-deploying a Rule	330
Loading Rules	330
Automatic Disabling	330
Chapter 14: Use Cases	333
What are ESM Use Cases?	333
Master Use Cases	334
Installing Use Cases	335
Navigating to Use Cases	336
Opening Use Cases	336
Accessing Resources from the Viewer Panel	337
Configuring Use Cases	338
Step 1 - Model Your Network	338
Step 2 - Install Use Case Package Bundles	338
Step 3 - Launch the Use Case Wizard	338
Step 4 - Introduction Panel	339
Step 5 - Prerequisites Panel	339
Step 6 - Confirm Event Sources Panel	340
Step 7 - Configuration Panels	341
Step 8 - Summary of Settings to Apply Panel	342
Step 9 - Configuration Complete Panel	343
Configuration Panels	344
Categorize Assets/Zones Panels	344
Define Data Sets Panels—Used to Populate Active Lists	346
Specify the Notification E-mail Address Panel	348
Specify the Expiration Time Period Panel	349
Set the Notification Rate Panel	349
Schedule Daily Report Panels	350
Schedule Weekly Report Panels	351
Schedule Monthly Report Panels	353
Schedule Yearly Report Panels	355
Chapter 15: Identity Correlation	357
Understanding Session Correlation	357

How Session Correlation Works	357
Creating a Session List Rule	358
Creating a Variable	360
Managing Session Lists	361
Creating a Session List	361
Editing Session Lists	363
Moving or Copying Session Lists	363
Exporting Session Lists	364
Deleting Session Lists	364
Adding a Session List Entry	364
Adding a Session List Entry Based on an Existing Entry	364
Deleting a Session List Entry	364
Terminating a Session List Entry	365
Using Session Lists to Correlate Session Data on User Logins (Example)	365
Example Overview	365
1. Create a Session List to Store Windows Sessions	366
2. Create Rules to Populate the Session List with Windows Logins	367
Rule 1: Triggers on Windows Session Logins	368
Rule 2: Triggers on Termination of Windows Sessions	370
3. Verify Rules	372
4. Use the Session List in a Report	374
Using Active Lists to Correlate Users (Example)	375
Example Overview	376
1. Build and Populate the Active List with User IDs	376
Populating an Active List with User Data	377
2. Create a Rule that Uses Active List Values to Correlate User IDs	379
Chapter 16: List Authoring	385
Managing Active Lists	385
Creating an Active List	385
Case-Insensitive Lookup in Active Lists	386
Using Rules to Populate an Active List	387
Example	387
Editing Active List Entries	390
Editing an Active List	390
Move or Copy an Active List	390
Importing an Active List	390
Exporting an Active List	391
Deleting an Active List	391
Managing Active List Groups	391
Navigating to Active Lists	391
Creating an Active List Group	391
Renaming Active List Groups	392

Editing Active List Groups	392
Moving or Copying Active List Groups	392
Deleting Active List Groups	392
Managing Session Lists	392
Creating a Session List	393
Using Rules to Populate a Session List	394
Editing a Session List	395
Moving or Copying a Session List	395
Exporting a Session List	395
Deleting a Session List	395
Adding a Session List Entry Based on an Existing Entry	395
Adding a Session List Entry	396
Deleting a Session List Entry	396
Terminating a Session List Entry	396
Chapter 17: Case Management and Queries	397
Managing Cases	397
Create a New Case	397
Case Properties	398
Creating a Case from Displayed Events	398
Editing a Case	399
Finding Cases	399
Attaching a File to a Case	399
Viewing a Case Attachment	400
Adding Events to a Case	400
Showing Event Details for Cases in Channels	401
Deleting Events from a Case	401
Creating a Channel for a Case	401
Exporting a Case to an External System	401
Moving or Copying a case	401
Deleting a Case	402
Managing Case Groups	402
Creating a Case Group	402
Renaming a Case Group	402
Editing a Case Group	402
Moving or Copying a Case Group	402
Deleting a Case Group	403
Running Case Queries	403
Setting Up an Automatic Case Query Group	403
Chapter 18: Integration Commands	405
What are Integration Commands?	406
Operations Synergy Scenarios	406

TRM and CounterACT Scenarios	406
Console Integration Scenarios	406
Third-Party Integration Scenarios	406
How it Works	407
Supported Command Types	407
Understanding Integration Configurations	407
Planning Checklist and Workflow	409
Navigating to Integration Command Resources	410
Quick Example	411
Constructing the Example Command	411
Running the Example Command	413
Adding and Editing Commands	413
Command Types and Attributes	415
Script Commands	415
URL Commands	416
CounterACT Commands	417
Adding and Editing Command Parameters	418
TRM Command Syntax and Examples	419
Creating and Editing Configurations	421
Configurations Attributes	423
Configurations Contexts	424
Configurations Commands	425
Adding a Command to a Configuration	425
Editing Commands in a Configuration	425
Removing Commands from a Configuration	425
Configurations Targets	426
Adding a Target to a Configuration	426
Editing Targets in a Configuration	426
Removing Commands from a Configuration	426
Specifying Targets	427
Target Attributes	427
Target Integration Parameters	427
Setting User Login Parameters	428
Setting Logins and Other Parameters to Prompt for Values at Runtime	429
Access Control Lists (ACLs) on Integration Commands	429
Running Integrated Commands	430
Entering/Saving Command Parameters at Runtime	431
Network Tools as Integration Commands	431
Chapter 19: Knowledge Base Authoring	433
Managing Knowledge Base Articles	433
Creating Knowledge Base Articles	433
Showing a Knowledge Base Article	434

Editing a Knowledge Base Article	434
Moving or Copying a Knowledge Base Article	434
Deleting a Knowledge Base Article	434
Managing Knowledge Base Article Groups	435
Creating a Knowledge Base Article Group	435
Renaming a Knowledge Base Article Group	435
Editing a Knowledge Base Article Group	435
Moving or Copying a Knowledge Base Article Group	435
Deleting a Knowledge Base Article Group	435
Getting Knowledge Base Updates	436
Refreshing the Knowledge Base Tree	436
Associating Knowledge Base Articles	436
Associating resources with Knowledge Base groups or Articles	436
Associating Grid View Elements with Knowledge Base Articles	436
Chapter 20: Managing Resources (for Administrators)	437
Managing Users	438
Handling Users	438
Creating a User	438
Editing a User	440
Resetting User Passwords	440
Moving or Linking a User	440
Deleting a User	440
About the System User	441
Handling User Groups	441
Creating User Groups	442
Renaming User Groups	442
Editing User Groups	442
Moving or Linking User Groups	442
Deleting User Groups	442
Setting Startup Views	443
Managing Permissions and Resources	443
Editing Access Control Lists (ACLs)	443
Granting or Removing Resource Permissions	444
Granting or Removing Operations Permissions	446
Granting or Removing User Group Permissions	447
Granting or Removing Event Permissions	448
Granting or Removing Sortable Field Sets Permissions	450
Sharing Resources	451
Controlling Who Has Permissions to Deploy Data Monitors	452
How Upgrades Affect Data Monitor Deploy Permissions	453
Deployment Permissions on Imported Data Monitors	454
Locking and Unlocking Resources	454

System Core Content	454
User Created Content	454
Unlocking a User-locked Resource	455
Modeling Your Network and Managing Assets	456
Network Model	456
Populating the Network Model with Assets	456
Understanding ESM Asset Resources	457
Assets	457
Locations	458
Zones	458
Networks	459
Vulnerabilities	459
Asset Categories	459
Populating the Network Model Using the Wizard	459
Specifying CSV Column Types	460
Zones CSV File Format	462
Assets CSV File Format	464
Asset Ranges CSV File Format	466
Increasing the Number of Rows Displayed	467
Summary of Data to Import	467
Network Data Imported into Manager	468
Selecting Assets in the Common Conditions Editor	469
Managing Assets	469
Creating an Asset	470
Working with Locations, Zones, Networks, Vulnerabilities, and Categories	470
Editing an Asset	473
Moving or Copying an Asset	473
Deleting an Asset	473
Showing Assets in a Channel	473
Auto Zoning an Asset	474
Managing Asset Groups	474
Creating an Asset Group	474
Renaming an Asset Group	474
Editing an Asset Group	474
Moving or Copying an Asset Group	475
Deleting an Asset Group	475
Asset Scalability	475
Viewing Assets in Active Channels	475
Finding Assets	475
Selecting Vulnerabilities	475
Managing Vulnerabilities	476
Creating a Vulnerability	476
Editing a Vulnerability	477

Moving or Copying a Vulnerability	477
Retrieving Vulnerable Assets	477
Adding an Asset to a Vulnerability	478
Deleting an Asset From a Vulnerability	478
Deleting a Vulnerability	478
Managing Vulnerability Groups	478
Creating a Vulnerability Group	478
Renaming a Vulnerability Group	478
Editing a Vulnerability Group	478
Moving or Copying a Vulnerability Group	479
Deleting a Vulnerability Group	479
Reporting on Scanners	479
Reporting Vulnerable Assets	479
Managing Filters	480
Using Filters	480
Editing a Filter	480
Importing and Exporting filters	481
Moving or Copying Filters	481
Deleting Filters	481
Using Filter Groups	481
Creating Filter Groups	481
Renaming Filter Groups	481
Editing Filter Groups	482
Moving or Copying Filter Groups	482
Deleting Filter Groups	482
Managing Notifications	482
Managing Received Notifications	482
Managing Notification Groups and Levels	483
Creating Notification Groups	483
Renaming Notification Groups	484
Editing Notification Groups	484
Deleting Notification Groups	484
Adding Escalation Levels	484
Deleting Escalation Levels	484
Managing Notification Destinations	484
Creating Destinations	484
Editing Destinations	485
Moving or Copying Destinations	485
Deleting Destinations	485
Changing Notification and Acknowledgement Settings	485
Changing E-mail Settings	486
Adding New Pager Service Providers	486
Editing Pager Service Provider Settings	487

Deleting Pager Service Providers	487
Changing Wait Time Settings	487
Testing Notification Groups and Destinations	487
Testing Group Notifications	487
Testing Destination Notifications	487
Managing File Resources	488
Uploading Files and Creating a File Resource	488
Viewing Files	490
Downloading Files Locally	490
Editing File Resource Attributes	490
Replacing File Resource Contents	490
Deleting File Resources	490
Adding a File or Folder to a Package	490
Finding Files	491
Managing Packages	491
Viewing Installed Packages	492
Viewing all Packages (with Dependencies)	492
Showing Package Archive Contents	492
Creating Packages	492
Importing Bundles	494
Exporting Packages	495
Installing Packages	495
Uninstalling Packages	495
Editing Packages	496
Adding Resources to Packages	496
Removing Resources from Packages	496
Deleting Packages	496
Resolving Package Conflicts	497
Managing Pre-v4.x Content	498
Managing SmartConnectors	498
Selecting and Setting SmartConnector Parameters	498
Configuring the SmartConnector	498
Connector Editor Option Tabs	499
Connector Tab Configuration Fields	500
Default Content Tab Configuration Fields	501
SmartConnector Processing Categories	514
SmartConnector Time Interval Options	515
Managing SmartConnector Filter Conditions	515
Creating SmartConnector Filters	515
Adding SmartConnector Filter Conditions	516
Deleting SmartConnector Filter Conditions	516
Setting Special Severity Levels	516
Setting a Custom Severity Level	516

Configuring a Conditional Severity	517
Sending Model Mappings to SmartConnectors	517
Sending Model Mappings to a Connector	517
Sending Control Commands to SmartConnectors	517
Getting Status Reports	518
Sending Flow-Control Commands	518
Managing SmartConnector Groups	525
Creating SmartConnector Groups	526
Renaming SmartConnector Groups	526
Editing SmartConnector Groups	526
Moving or Copying SmartConnector Groups	526
Deleting SmartConnector Groups	526
Managing SmartConnector Resources	526
Moving or Copying a SmartConnector Group	526
Deleting a SmartConnector Group	527
Importing and Exporting SmartConnector Configurations	527
Importing a SmartConnector Configuration	527
Exporting a SmartConnector Configuration	528
SmartConnector Filters	529
Upgrading SmartConnectors	529
Overview of the Upgrade Process	529
Upgrading SmartConnectors	531
Rolling back to a Previous Version	532
Troubleshooting	532
Selecting Resources	533
Finding Resources	534
Searching for System Resources	534
Search Field on Console Tool Bar	534
Query Options	535
Result Columns	536
Locating Specific Resources	536
Visualizing Resources	537
Graphing Resources	537
Using Graphs	537
Configuring Resource Graphs	539
Viewing Resources in Grids	540
Validating Resources	540
Valid and Invalid Resources	541
Fixing and Validating Resources	541
Troubleshooting (Requirements for Valid Resources)	543
Automatic and Manual Validation	546
Resource Validation During Upgrade	546
Extending Audit Event Logging	547

Managing Partitions	547
Getting Partition Information	548
Seeing a Partition Schedule	548
Archiving Partitions	548
Reactivating Archived Partitions	549
Reactivating Zipped or Large Archived Partitions	549
Deactivating Archived Partitions	550
Running Scheduled Tasks Right Away	550
Partition Properties	550
Managing Customers	551
Creating Customers	551
Editing Customers	551
Deleting Customers	551
Saving Copies of Read-Only Resources	552
Using the Image Editor	552
Common Resource Attribute Fields	552
Common	552
Assign	553
Parent Groups	553
Creation Information	553
Last Update Information	554
Chapter 21: Personalizing the Console	555
Changing the Console Display	555
Resizing the Console	555
Showing or Hiding Menu Bars and Tools	555
Showing or Hiding the Status Bar	555
Showing or Hiding the Navigator Panel	555
Showing or Hiding the Viewer Panel	556
Showing or Hiding the Inspect/Edit Panel	556
Floating a Console Panel	556
Applying Translucency to a Console Panel	556
Docking a Console Panel	556
Closing a Console Panel	556
Changing User Preferences	556
Changing Your Password	557
Changing Other Users' Passwords	557
Setting Program Preferences	557
Changing Global Options Like Panel and Editor Characteristics	558
Setting Grid View Options	559
Setting Date and Time Formats	560
Configuring Event Graphs	561
Latitude and Longitude Options	561

Event Graph Options	562
Setting Notification Popups	563
Managing Hot Keys	563
Adding Shortcuts for Frequently Used Resources	563
Modifying a Custom Shortcut	565
Removing a Custom Shortcut	567
Activating a New Shortcut Schema	568
Sharing Custom Shortcut Schemas	569
Saving and Sending Settings	569
Saving a File	569
Saving a File to the ArcSight Manager	569
Loading a File From the ArcSight Manager	569
Sending a File by E-mail	570
Chapter 22: Reference Guide	571
Access Control Lists	571
Resource ACLs	571
Actions	572
Active Channels	572
Active Channel Views	573
Active Channel Headers	573
Comparisons	574
Active Channel Views for Assets and Cases	574
Active Lists	574
Uses of Active Lists	575
Active Lists for Long-term State Retention	575
Optimize Data with Hash-Based Active Lists	576
Active List Audit Events	576
Active List Monitor Events	576
Active Lists with Values	577
Variables	577
Example: Active List with Values to Store Directory Information	577
Create an Active List	577
Populate the Active List	578
Correlate Information Stored in UserRoles List	578
Working with Active Lists	580
Administrator	580
Aggregation	580
ArcSight Web	580
Assets	581
Assets Tab	581
Zones Tab	582
Networks Tab	582

Categories Tab	582
Vulnerabilities Tab	583
Locations Tab	583
Attack	583
Audit Events	583
Active Channel	584
Active List	585
Authentication	585
Authorization	586
Connectors	586
Dashboard	589
Data Monitors	589
Group Management	590
Manager Activation	591
Manager Database Error Conditions	591
Manager External Event Flow Interruption	591
Notifications	591
Partition Archiver	593
Partition Manager	593
Query Viewers	594
Reports	594
Resources (Configuration Events Common to All Resources)	594
Resource Quota	595
Rules	595
Scheduler	597
Stress	598
Trends	598
User Login	599
User Management	600
Batching	600
Case Editor Tab Fields	600
Case Editor Events Tab	601
Case Editor Attachments Tab	601
Case Editor Final - Attack Agent Tab	602
Case Editor Final - Attack Mechanism Tab	602
Case Editor Final - Incident Information Tab	602
Case Editor Final - Other Tab	603
Case Editor Final - Vulnerability Tab	603
Case Editor Follow-Up Tab	603
Case Editor Initial - Attributes Tab	604
Case Editor Initial - Description Tab	604
Case Editor Initial - Security Classification Tab	605
Case Editor Notes Tab	605

Cases	605
Case Groups	606
Categories	606
Object Category	607
Behavior Category	609
Outcome Category	610
Device Group Category	611
Technique Category	611
Significance Category	613
Custom Event Categorization	614
Collaboration	615
Common Conditions Editor	616
Editor Features	616
Condition Tree Command Buttons	618
Condition Tree Context Menu Commands	619
Adding Conditions	621
Field Comparisons with Variable or Static Values	622
Using Field Sets	623
Testing for Zone Relevance	624
How to Create a Matching or Join Rule	624
Conditional Statements	625
ArcSight Variables	626
Conditions	626
Parameterized Conditions	626
Console	628
Content	628
Content Packages	628
Custom Content	629
SmartConnector Content	629
Correlation	629
Correlation Rule	629
Customers	630
Dashboards	630
Dashboard Context Menu Options	630
Database	631
Schema Redesign	631
More Event Fields	631
More Efficient Field Usage	632
More Precise Event Categorization	632
Data Fields	633
Connector	633
Attacker	638
Category	643

Destination	644
Device	649
Device Custom	654
Event	656
Event Annotation	663
File	667
Final Device	668
Flex	672
Manager	673
Old File	673
Original Connector	674
Request	678
Source	680
Target	685
Threat	689
Resource Attributes	691
Geographical Attributes	691
Data Monitors	692
Asset Category Count Data Monitor	692
Event Correlation Data Monitor	693
Event Graph Data Monitor	694
Event Reconciliation Data Monitor	695
Correlation-Event-Generating Fields	697
Geographic Event Graph Data Monitor	698
Hierarchy Map Data Monitor	699
Enhancements for ESM v.4.5	699
Use Cases	699
Defining a Hierarchy Map Data Monitor	700
Adding Variables	701
Specifying the Source Node Identifiers	701
Specifying Group Attributes	703
Hierarchy Map Display and Visualization Controls	704
Hourly Counts Data Monitor	707
Last N Events Data Monitor	708
Last State Data Monitor	709
Moving Average Data Monitor	710
Rules Partial Match Data Monitor	713
Session Reconciliation Data Monitor	713
Statistics Data Monitor	715
System Monitor Data Monitor	717
System Monitor Attribute Data Monitor	718
Top Value Counts Data Monitor	718
Data Monitor Expressions	720

Supported Data Monitor Expression Operators	720
Supported Data Monitor Expression Functions	720
Device	721
Event Inspector	721
Field Sets	722
Events	722
Field Sets	723
Filters	724
Filtering Options	724
Grid View	725
iDefense	726
Inspect/Edit Panel	726
Job Scheduler	727
Knowledge Base	727
Logical Operators	727
Managed Security Service Providers (MSSPs)	728
Manager	728
Navigator Panel	729
Notifications	729
Notification Operation	729
Testing Notification Escalations	730
Notification Destinations	730
Notification Acknowledgements	731
Packages	731
Partitions	731
Pattern Discovery	732
Pattern Concepts	733
Discovering Patterns	733
Pattern Analysis	733
Initial Phase	734
Routine Pattern Processing	734
Workflow Management	734
Pattern Analysis	734
Pattern Disposition	734
Pattern Expertise	735
Workflow	735
Visualization	735
Applications	736
Payload	736
Prioritization Fields	736
Priority Calculations and Ratings	737
Priority Elements	739
Priority Operators	739

MaxValue Attribute	740
Weight Attribute	740
Priority Rating	740
Queries	741
Queries and Trends	741
Building and Running Queries	741
Query Viewers	742
Reference Pages	742
Reports	742
Working with Report Templates, Queries, and Trends	743
Viewing and Managing Reports	743
Archived Reports	743
Report Groups	743
Delta Reports	744
Report Parameters	744
Running Reports	745
ArcSight Provided Reports	745
Report Templates	745
Resources	746
Valid and Invalid Resources	746
Fixing and Validating Resources	747
Troubleshooting (Requirements for Valid Resources)	749
Automatic and Manual Validation	749
Resource Attributes	749
Rule Actions	751
Active List Rule Actions	751
Execute Connector Command Rule Actions	751
Rule Conditions	752
Rules	753
Rules Processing and Correlation	753
Rule Groups	755
Scheduled Rules	755
Rule-triggering Timing	755
Rule Chains	756
ArcSight Variables	756
Rules Editor	756
Scheduling Jobs	756
To schedule a job	757
To view all scheduled jobs	758
Troubleshooting Tips	758
Send Logs	758
Guidelines for Using the Send Logs Utility	758
Options for Running Diagnostics and Sending Logs	759

Starting the Send Logs Wizard on the Console	759
Session Correlation	760
Why Session Correlation Matters	761
Session Lists	761
SmartConnectors	762
Operational Status	762
Configuration	763
Zones	763
Upgrading	764
Filtering	764
SMTP	764
Sortable Field Sets	765
Using Sortable Columns in Grid Views	766
Status Monitor Events	766
Active Channel Statistics	766
Active List Statistics	767
Asset Statistics	768
Data Monitor Statistics	769
Event Broker Statistics	769
Filter Engine Statistics	770
Main Flow Statistics	770
Notification Statistics	770
Pattern Discovery Statistics	771
Report Statistics	771
Resource Framework Statistics	771
Rules Engine Statistics	772
Session List Statistics	773
Session Management Statistics	774
Side Table Statistics	774
SmartConnector Flow Statistics	775
Templates	777
Threat	777
Threat Evaluation	777
Evaluation Process	777
Evaluation Definitions	777
Maintaining Model Confidence	778
Using Threat Evaluation Information	778
Limitations and Workarounds	778
Thresholds	779
Time Error Correction	779
Timestamps	779
Security Events	780
Resources	780

General Information	780
Timestamp Variables	780
Inclusive Timestamps	781
Time Zone Correction	781
Trends	781
Understanding Trends and Queries	781
Building Trends	782
Upgrade SmartConnectors	782
User Groups	782
Users	783
User Types	783
Variables	784
Variables Fields	785
Timestamps	785
String Functions	786
Group Functions	787
Type Conversion Functions	788
Arithmetic Functions	790
IP Address Functions	792
List Functions	792
Conditional Functions	792
Velocity Templates	793
Velocity Application Points	793
Using Velocity Expressions in Rule Actions to Retrieve Values from Event Fields or Variables ..	794
Retrieving Values from Event Fields	794
Variables	794
Example of Rule Action that Uses Velocity Expressions to Retrieve Values	794
Examples	795
Usage Tips	795
Velocity References for Reports	796
Views	800
View Types	800
Other Views	801
Dashboards	801
Vulnerabilities	801
Vulnerability Groups	801
Standardized Vulnerability Tracking	802
Index	803

About this Guide

The Online Help delivered with the ArcSight Enterprise Security Management (ESM) Console is the ESM User and Reference Guides in a context-sensitive, online format.

The following topics describe how to use the Help system, list related documentation, and explain how to get more help from Customer Support or send us feedback on the documentation.

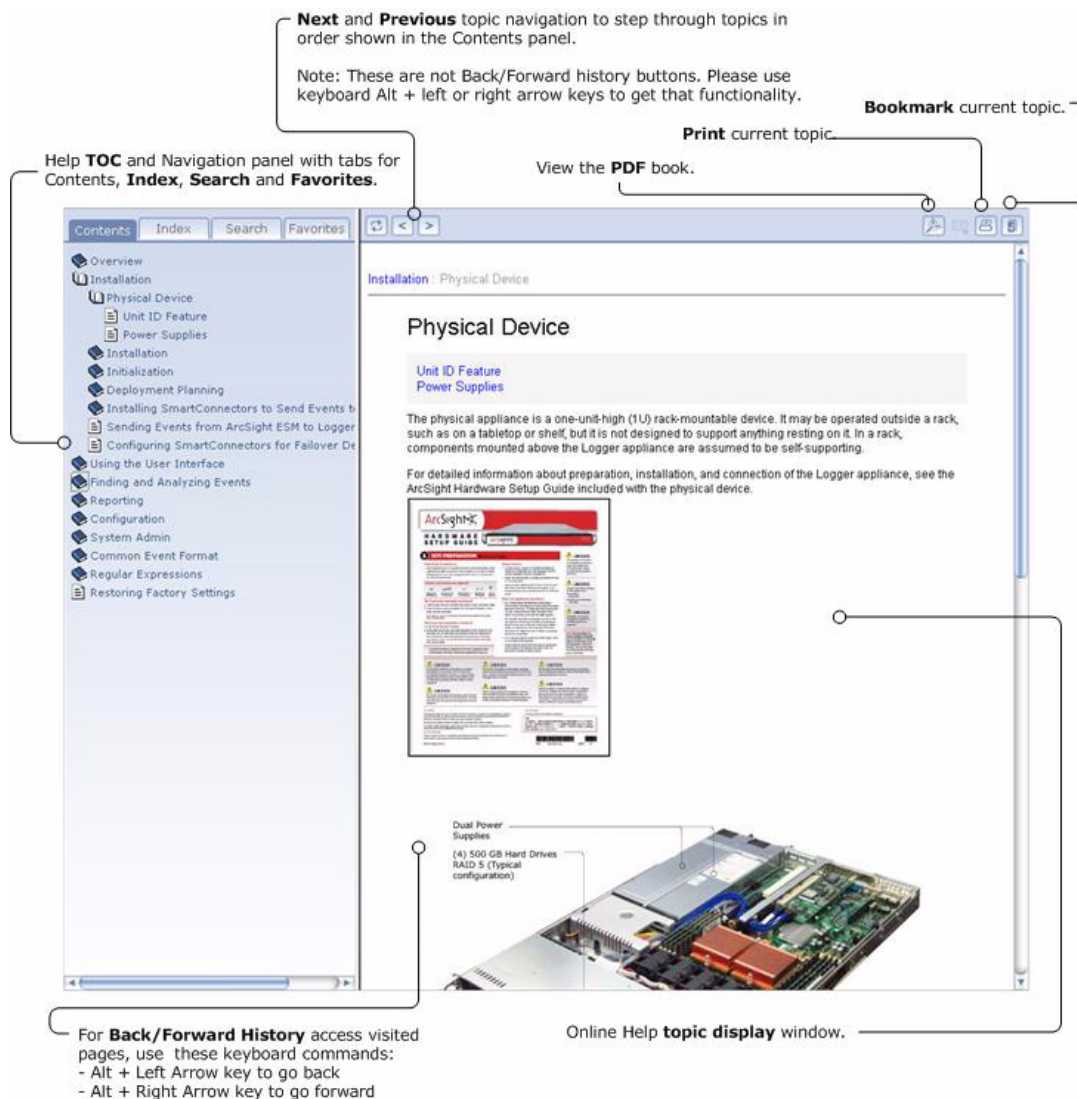
[“Power User Help Features” on page xxxvi](#)

[“Help Display Preferences” on page xxxviii](#)

[“Text Conventions” on page xxxviii](#)

[“Related Documentation” on page xxxix](#)

[“Feedback” on page xl](#)





Power User Help Features

Starting with ESM v.4.5, the ArcSight Console provides a feature-rich, Web-based Help display. Both HTML and PDF documentation is provided in the same display.

The Online Help includes the following features:

- Left panel Help navigation - Click a tab for **Contents (TOC)**, **Index**, **Search**, or **Favorites**.

The TOC tracks with your navigation of the Help topics in the main display, the Index gives you alphabetical "jump to" points, you can bookmark frequently referenced topics as "Favorites".


- **Next** and **Previous** sequential topic navigation to step through topics in order shown in the Contents (TOC) panel.- Click the Previous button  to view the preceding topic, or the Next button  to view the subsequent topic.




For **Back/Forward History** access to visited pages (like Back/Forward buttons on a Web browser), use these keyboard commands:

- **Alt + Left Arrow key** to go **Back**
- **Alt + Right Arrow key** to go **Forward**

- Topic display window - Click a topic in the Contents, Index, Search hit list, or saved Favorites to view it in the display window.
- Breadcrumbs - At the top of each HTML page on the main Help display shows your location in the topic list. Click on the "parent topic" to return to it. (The left panel TOC also tracks your location within the topics.)
- Access to the ESM Help and User's Guide as an Adobe Acrobat PDF document.

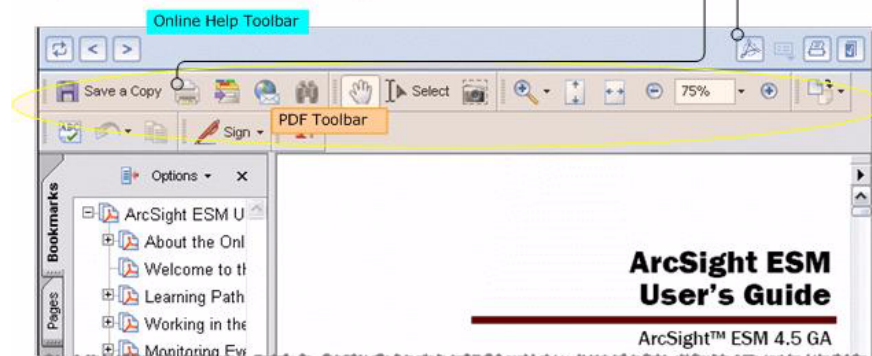
Click the **PDF** button  in the upper right of the Online Help toolbar to get PDF. The ArcSight ESM User Guide is displayed as a PDF within the Help window. (The User Guide is the entire ESM Help documentation set in print-friendly format.) All Adobe Acrobat PDF features (Bookmarks TOC, Hyperlinks, Search, Zoom, Comments, Print, Sign, E-mail, etc.) are available on the PDF from within the Console Help window.

To view the PDF outside of the Help display, click the Save button  to **download a copy of the PDF** to a selected location. Use the browser to navigate to the directory where you want to save the file, and click **Save**.



To **print the PDF**, click the Print button  on the PDF toolbar.


To view the Help in PDF format, first click the PDF button on the **Online Help toolbar**.

With the PDF displayed, use the save, print, and search buttons on the **PDF toolbar** to perform these operations on the PDF. (The Online Help toolbar above it is for operations on the browser style Help only.)



- Print capabilities - Click the **Print**  button to print a copy of the **current topic**.

To **print the PDF**, first click the **PDF** button  in the upper right of the main Web Online Help toolbar to get PDF click, then click the **Print** button  on the **PDF toolbar**. If you want to print out part of the book (e.g., just the Query Viewer topics or Rules topics) you'll need to provide the page range you want in the PDF print dialog.

- Bookmarks - Click the **Bookmark**  button and follow the instructions in the popup window to bookmark a topic.

Help Display Preferences

By default, the Help is displayed in the ESM Console “embedded Web browser”. You can also launch the default, external Web browser. See [related information on page 559](#).

Additionally, a preference is available for re-setting the default display size of the Help window. (To manually resize a currently displayed Help window, click and drag its corners.) See [related information on page 559](#).

For more information on setting these Help display preferences, see [Table 21-1, “Global Options,” on page 558](#) in [“Personalizing the Console” on page 555](#).

Text Conventions

The following table lists the syntax conventions used in this guide.

Text	Description and Example
Bold	<p>Bold is used to indicate an on-screen element that a user should click. Always use this character format rather than manually bolding the item with the format style menu or “bold” button.</p> <ul style="list-style-type: none">• Enter a value and click OK.
<code>Code</code>	<p>As described before, the code character tag is used for code elements discussed in-line in a paragraph.</p> <ul style="list-style-type: none">• If the name of your active list entries text file is “<code>AdministrativeUsers.txt</code>,” the script would look like this:
<i>Emphasis or BookName</i>	<p><i>Italics</i> indicates emphasis or a book name:</p> <ul style="list-style-type: none">• <i>Do not</i> perform this procedure until you have backed up your data.• For more information, see the <i>ArcSight Administrator’s Guide</i>.
menu > submenu	<p>Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences.</p> <ul style="list-style-type: none">• menu > submenu > submenu <p>For example:</p> <ul style="list-style-type: none">• Authoring > Rules > Rule Actions > Updating Session Lists
tab subtab	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none">• tab subtab subtab
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none">• All Reports/System Reports/Asset/All Assets

Text	Description and Example
<variable>	<p>A text string enclosed in angular brackets is a variable for which you need to supply a value. (The bracketed text may also be in italics to emphasize that it is a variable.)</p> <p>Example:</p> <p>In <code>--nsp_password=<password></code>, <password> is a variable for which you supply a value.</p>
{parameter1 parameter2 parameter3}	<p>Curly brackets enclose multiple parameters, at least one of which you must provide.</p> <p>Example:</p> <pre>{--user_id_seq=<user_id> -- user_login=<user_login>}</pre> <p>In the above example, either supply the user ID of a user or his/her login name.</p>
[optional_parameter]	<p>Square brackets enclose parameters, variables, or values that are optional.</p> <p>Example:</p> <pre>[--cli_restrict=1]</pre>

Related Documentation

ArcSight makes available the following ESM product documentation. Many of these documents are available from the ArcSight ESM Console by choosing the menu option **Help > Browse Documentation**. The latest and most complete set of documentation is always offered on the ArcSight Customer Support site (<https://support.arcsight.com>) through the Product Documentation link in the Knowledge Center section.

Document Title	Description
ESM 101: Concepts for ArcSight™ ESM	ESM 101 introduces the underlying concepts behind how ArcSight ESM works, and provides a roadmap to the tools available in ESM depending on your role in security operations.
ArcSight™ ESM Release Notes	Describes new product features, latest updates, known product issues and work-arounds, and technical support information.
ArcSight™ ESM Installation and Configuration Guide	Explains how to install and configure ArcSight Enterprise Security Management (ESM) components and tools including the ArcSight Database, Manager, Console, and Web applications. Also provides general information about how to plan for, install, and deploy ArcSight SmartConnectors.
ArcSight™ ESM Administrator's Guide	Describes how to configure ArcSight and its network interfaces, and maintain ArcSight for ongoing operations.
ArcSight™ ESM Reviewer's Guide	Introduces major new features in the current version of ArcSight ESM, including task walk-throughs and usage guidance. The same information is highlighted in the "What's New" Console Help topics.

Document Title	Description
ArcSight™ ESM User's Guide ArcSight™ ESM Reference Guide	Describes how to use the ArcSight Console. These are printable versions of the online Help topics and glossary.
ArcSight™ ESM Web User's Guide	Provides user and reference information from the ArcSight Web online Help system.
ArcSight™ SmartConnector Configuration Guides	Provides vendor-specific instructions for how to install individual SmartConnectors and configure their associated devices.
ArcSight FlexConnector Configuration Guide	Describes how to design, create, and install custom SmartConnectors.

Feedback

To submit feedback regarding ArcSight ESM or documentation, go to ArcSight's customer support web site at <https://support.arcsight.com>

Chapter 1

What's New

ArcSight™ Enterprise Security Management (ESM) consolidates and normalizes data from devices and applications across your enterprise network in a centralized view. ArcSight ESM provides a holistic view of the security status of all relevant IT systems, and integrates security into your existing management processes and workflows to provide “forensics on the fly”. ESM provides solutions for compliance automation, identity monitoring, event collection and management, multi-variable correlation and pattern-matching, historical reporting, alert and frequency threshold notification, and more.

This topic describes **new features and enhancements** added in this release, and explains where to find more information about them.

[“New Features” on page 1](#)

[“Correlation Enhancements” on page 2](#)

[“New Features of the ESM Console” on page 3](#)

[“New Features of ArcSight Web” on page 3](#)

[“ArcSight Express” on page 3](#)

New Features

The following features are new in ESM v.4.5. For a more thorough introduction to key features, along with example walk-throughs, please refer to the *ESM Reviewer's Guide* (choose **Browse ArcSight Documentation** on the Console's Help menu and click the link for “ESM Reviewer's Guide”).



Use Cases. ArcSight ESM resource collections that address common security issues and business requirements. When use cases are installed, a Use Case tab is displayed in the Navigator panel. A use case wizard is available to automate configuration of the resources involved in the use case. The wizard steps through questions on event sources to use, data sets to populate active lists, reports preferences, notifications, and so forth, then configures the use case accordingly. See [“Use Cases” on page 333](#).



Network Model Wizard. New in ArcSight ESM v.4.5, the Network Model wizard provides the ability to quickly populate the ESM network model by batch loading asset and zone information from Comma Separated Files (CSV) files. The following data can be imported into ArcSight ESM Manager from CSV files:

- The zones define functional parts of a network, such as a wireless LAN, a engineering network, a VPN or a DMZ.
- The assets representing individual nodes on the network, such as servers and routers
- The asset ranges representing a set of network nodes addressable as a contiguous block of IP addresses, such as laptops

For more information, see ["Populating the Network Model Using the Wizard" on page 459.](#)



Query Viewers. New in ArcSight ESM v.4.5, a *query viewer* is a new resource for defining and running SQL queries on various ESM data sources (trends, assets, cases, lists, events, etc.) Each query viewer contains an SQL query and other logic for establishing and comparing baseline results, analyzing against historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results.

Before ESM v.4.5, the only way to run SQL queries against ESM events and resources was to run reports, which use SQL queries and trend-queries. Starting with ESM v.4.5, you can use query viewers to run the same queries used for reports, and get quicker results.

See [Chapter 10, Query Viewers, on page 161.](#)



Integration Commands. Starting with ESM v.4.5, the Console offers better application integration capabilities to configure and launch commands, tools, and views in other applications, including other ArcSight products.

Provides the ability to configure custom scripts, URLs, and CounterACT SmartConnector commands, and integrate them into the Console UI in various contexts. Leverages velocity expressions and the UI contexts for pulling the content of event data, for example, as command parameter values.

Includes support for ArcSight Network Synergy Platform (NSP) Threat Response Manager (TRM) through the CounterACT SmartConnector. Role and access list (ACL) based use of the tools and commands can be configured and managed in the Console.

See [Chapter 18, Integration Commands, on page 405.](#)

Correlation Enhancements



CCE Field Comparison

The Common Conditions Editor (CCE) now provides the ability to define inner/within-event field comparisons as part of a rule condition. See ["Field Comparisons with Variable or Static Values" on page 622](#) in the topic on [Adding Conditions](#).

Filter Debugging

Starting with ESM v.4.5, a filter debugger is available as a right-click option on an event in an active channel. The filter debugger validates whether a selected filter matches a certain type of event and, if there are mis-matches, identifies which filter conditions are not matching the event details. See ["Debugging Filters to Match Events" on page 151.](#)

Cumulative Rule Chain

The **On Time Window Expiration** (TWE) Rule trigger now includes an option to show a ***cumulative rule chain*** (a summary of triggered rules) at the end of the triggered rules list. See [“On Time Window Expiration” on page 313](#) under [Creating Rule Actions, Threshold Triggering Options](#).

Permissions on Deploying Data Monitors

ESM v.4.5 features a redesigned, more user-friendly interface for editing Access Control Lists (ACLs), along with a new option to edit operations permissions on data monitors. See [“Editing Access Control Lists \(ACLs\)” on page 443](#) and [“Controlling Who Has Permissions to Deploy Data Monitors” on page 452](#).

Hierarchy Map Data Monitor

This Hierarchy Map Data Monitor draws an image made up of proportionally sized panels where each panel represents a group of events selected by group fields selected in the source node identifier. A source-node criteria could be a combination of fields.

As of ESM v.4.5, this data monitor includes several enhancements including a more refined view of grouped fields, more drill-downs, and enhanced visualization tools for controlling the map displays. See [“Hierarchy Map Data Monitor” on page 699](#).

New Features of the ESM Console



Console Preferences

New User Preference options on the Console are available:

- Latitude and Longitude Options. See [“Latitude and Longitude Options” on page 561](#).
 - Managing Hot Keys. See [“Managing Hot Keys” on page 563](#).
 - New Global Options for Console Help settings and default Web browser. See [“Launch Help in external Web browser” on page 559](#) and [“Set Help dialog size \(Width,Height\)” on page 559](#).
-

New Features of ArcSight Web



ArcSight Web: Views of New Features and Standard Content

ArcSight Web is ArcSight's next-generation Web server product. It includes views of new standard content (including ArcSight Express content in for those who have that product) along with operator views of new resources, such as deployed Query Viewers and Use Cases. See [“ArcSight Web” on page 580](#) for more information.

ArcSight Express



ArcSight Epress

ArcSight Express, a separate product offering from ArcSight ESM, is an enterprise security monitoring, response, and reporting system packaged as a suite of appliances. This is a streamlined, low maintenance, and easy-to-use solution. The ArcSight Express Security Information and Event Management (SIEM) appliance provides network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. See [Chapter 4, ArcSight Express Solution, on page 35](#) for more information.

Chapter 2

Getting Started

ArcSight™ Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

[“Quick Start Tools and Content” on page 5](#)

[“Network Model Wizard” on page 6](#)

[“Configuring ESM and Using Standard Content” on page 6](#)

[“ArcSight Express” on page 7](#)

Quick Start Tools and Content

The ESM Console serves as the control point for [ArcSight Express](#) and ESM administrators to configure content and resources, set up [ArcSight Web](#) access for Web users, and to manage, monitor, and respond to network security issues across the enterprise.



Use this information to better understand the Console's features, layout, tasks, and key-concept details.

To learn more about other ArcSight publications, choose **Browse ArcSight Documentation** on the Console's Help menu. If you are new to ESM, or would like to get hands-on experience with new and key features, please refer to the **ESM Reviewer's Guide**, which is also available on the Browse ArcSight Documentation page. The ESM Reviewer's Guide provides a thorough introduction to new and key features, along with example walk-throughs of common authoring and monitoring tasks.

A [Network Model Wizard](#) is provided (new in ESM v.4.5) to facilitate the process of describing network devices and assets in ESM.

Also, a set of coordinated *Resources* (filters, rules, dashboards, reports, and so on) is provided to address common security and management tasks. ESM [Standard Content](#) and [ArcSight Express Solutions](#) are designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box, with minimal configuration required on the Console.

- To get started using ESM, see [“Configuring ESM and Using Standard Content” on page 6](#).
- To get started using [ArcSight Express](#), see [“Getting Started Configuring ArcSight Express” on page 7](#).

Network Model Wizard

ESM v.4.5 provides a Network Model wizard that enables you to quickly populate the ESM network model by loading asset and zone information from Comma Separated Files (CSV) files. The following data can be imported into an ArcSight ESM Manager from CSV files:

- **Zones** define functional parts of a network, such as a wireless LAN, an engineering network, a VPN or a DMZ.
- **Assets** represent individual nodes on the network, such as servers and routers.
- **Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops.

For more about the Network Model wizard and instructions how to use it, see [“Populating the Network Model Using the Wizard” on page 459](#).

Configuring ESM and Using Standard Content

For a complete guide to ESM standard content (pre-packaged reports, rules, filters, channels, data monitors, etc.), please refer to [Chapter 3, Standard Content, on page 9](#).

Configuring ESM involves the following tasks:

- 1 [“Set Up Connectors and Model the Network” on page 14](#). Modeling the network includes establishing event feeds into ESM from SmartConnectors, setting up assets, zones, and networks for your key devices, and applying key asset categories used by ESM content.
- 2 [“Apply Standard Asset Categories to Assets” on page 16](#). Applying categories to assets provides more information to ESM about the criticality and business context of assets. Using categorization optimizes ESM monitoring to the specifics of your enterprise.
- 3 [“Configure Notification Destinations” on page 17](#). Add notification information for users, such as e-mail addresses, contact numbers, and hours of availability.
- 4 [“Configure Asset Auto-Creation Filters” on page 18](#)
- 5 [“Configure Rules to Send Notifications and Open Cases” on page 24](#). Configure key correlation rules that drive the notifications and case creation actions that communicate potential security risks to security operations personnel.
- 6 [“Schedule Reports” on page 26](#). Schedule reports that you want to make a central part of your regular reporting plan.
- 7 [“Default Trends Schedule” on page 26](#). Trends are special queries that can gather data over longer periods of time, which can be leveraged for reports. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources.
- 8 [“Getting Started Using Standard Content” on page 30](#). Executive summaries, operational summaries, and other types of content based are available as out-of-the-box, standard content in ESM. Using the tools and resources in ArcSight Foundation content, you can get started right away monitoring, analyzing, and investigating network activity.



ArcSight Express

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

ArcSight Express is made up of the following components:

ArcSight Manager	Provides correlation and analytics
ArcSight Logger	Provides long-term storage for historical search and investigation.
ArcSight Console	The interface through which an administrator sets up ArcSight Express user accounts, and configures and tunes the content.
ArcSight Web	The ArcSight Web client is the primary interface for ArcSight Express users, providing access to daily security operations.

The administrator adds the ArcSight [SmartConnectors](#) required for the devices in your network to gather [Events](#).

ArcSight Express also comes with a series of coordinated [Resources](#) (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. ArcSight Express content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration using the Console.

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

ArcSight Web

[ArcSight Web](#) provides full event monitoring and drill-down capabilities in a streamlined interface for ArcSight Express users. The ArcSight Express Web server is pre-installed on the ArcSight Express appliance.

The ArcSight Web interface can also be branded with your company logo.

Getting Started Configuring ArcSight Express

Configuring ArcSight Express involves the following tasks:

- 1 [Network Modeling](#). Modeling the network includes establishing event feeds into ArcSight Express from SmartConnectors, setting up assets, zones, and networks for your key devices, and applying key asset categories used by ArcSight Express content.
- 2 [Create ArcSight Express Users](#). Set up user accounts for the users who will access the ArcSight Express solution using the ArcSight Web.
- 3 [Configure Notification Destinations](#). Add notification information for users, such as e-mail addresses, contact numbers, and hours of availability.

- 4 [Configure Rules to Send Notifications and Open Cases](#). Configure key correlation rules that drive the notifications and case creation actions that communicate potential security risks to security operations personnel.
- 5 [Schedule Reports](#). Schedule reports that you want to make a central part of your regular reporting plan.
- 6 [Tuning ArcSight Express Content](#). After some use and testing, you may want to exclude certain devices or user scenarios from rule evaluation if they are part of a benign regular usage pattern in your environment.

ArcSight Express Documentation

- For complete instructions about how to configure the ArcSight Express content, see [“ArcSight Express Solution” on page 35](#).
- For instructions about installing and setting up the ArcSight Express appliance, see the *ArcSight Express Configuration Guide*.
- For instructions about administering the ArcSight Express solution, see the *ArcSight Express Administrator's Guide*.

Chapter 3

Standard Content

ArcSight Enterprise Security Management (ESM) comes with a series of coordinated resource systems that address common enterprise network security and ESM management tasks. These resource systems are referred to collectively as *standard content*.

With some basic configuration, standard content enables you to get started using ESM right away to effectively manage enterprise security operations without having to create additional resources. This topic describes the standard content and provides instructions for administrators about how to configure it using the ArcSight Console.

- ["What is Standard Content?" on page 9](#)
- ["Standard Content Foundations" on page 10](#)
- ["Standard Content Packages" on page 13](#)
- ["Navigating to Standard Content" on page 13](#)
- ["Set Up Connectors and Model the Network" on page 14](#)
- ["Apply Standard Asset Categories to Assets" on page 16](#)
- ["Configure Notification Destinations" on page 17](#)
- ["Configure Asset Auto-Creation Filters" on page 18](#)
- ["Configure Rules to Send Notifications and Open Cases" on page 24](#)
- ["Schedule Reports" on page 26](#)
- ["Default Trends Schedule" on page 26](#)
- ["Getting Started Using Standard Content" on page 30](#)

What is Standard Content?

Standard content is a series of coordinated [Resources](#) (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration.

The content that comes with ArcSight ESM provides a full spectrum of security, network and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the ESM system.

The standard content is organized into functional groups called foundations. For more about the foundations, see the next topic, ["Standard Content Foundations" on page 10](#).

The standard content is installed using a series of packages, some of which are installed automatically with the ESM Manager to provide essential system health and status




operations. The remaining packages are presented as install-time options organized by category.

Standard Content Foundations

Each foundation is a coordinated system of resources that provides real-time monitoring capabilities for its area of focus, as well as after-the-fact analysis in the form of reports, trends, and trend reports.

With ESM, you can extend these foundations with additional resources specific to your needs, or you can use them as a template for building your own resources and tasks.

Several of the foundations rely on a series of common resources that provide core functions for common security scenarios. Resources that manage core ESM functions are **locked** to protect them from unintended change or deletion.

Foundation	Description
Configuration Monitoring Foundation	 <p>The Configuration Monitoring foundation identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. Configuration monitoring is concerned mainly with monitoring hosts and user accounts for configuration-related activity, such as installing new applications, adding new systems to the network, anti-virus/network scanner/IDS engine and signature updates, and asset vulnerability postures.</p> <p>The configuration monitoring foundation helps you monitor how your networks change over time, measure daily statistics, understand the changes made, and know who's making them. Trends help you know what is normal and spot anomalies that should be investigated.</p>
Intrusion Monitoring Foundation	 <p>The focus of the Intrusion Monitoring foundation is to identify hostile activity and take appropriate action. This foundation provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting. As with previous releases, the essential security monitoring functions of the Intrusion Monitoring foundation make up the bulk of the ESM standard content.</p> <p>The Intrusion Monitoring foundation targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and so on.</p>
Network Monitoring Foundation	 <p>The Network Monitoring foundation monitors the status of network throughput and network infrastructure.</p> <p>This foundation provides statistics about traffic and bandwidth usage that helps you identify anomalies and areas of the network that need attention.</p>

Foundation	Description
ArcSight Workflow Foundation 	<p>The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking using the ESM incident response system.</p> <p>Qualifying events in the other ESM foundation packages trigger notifications and cases that get escalated through the ESM incident response stages.</p>
ArcSight Administration Foundation 	<p>The ArcSight Administration foundation provides statistics about the health and performance of ArcSight products. This foundation is installed automatically, and is essential for managing and tuning the performance of ESM content and components.</p>

ArcSight System Content



The ArcSight System content consists of resources that ESM requires for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.

System Function	Description
Internal ESM function	The system content contains sets of resources that manage ESM network modeling, vulnerability handling, and other internal ESM functions. These resources are leveraged by many basic systems and correlation tasks.
Correlation evaluation	System content rules, active lists, and filters help drive parts of the ESM correlation engine, such as priority formula calculations and basic out-of-the-box event processing.
Security center operations and monitoring	The system content provides standard field sets and active channels to provide basic operations and monitoring functions as soon as ESM is installed.
Benchmarking and analysis	ESM provides several benchmarking and analysis tools as add-on modules. As part of the system content, ESM includes two basic Pattern Discovery profiles. These profiles will be active only if you have Pattern Discovery installed.

This content is installed automatically with ArcSight ESM so that these functions and the infrastructure that supports them are immediately available. To safeguard against accidental damage or deletion, these resources are locked (read and write protected).

The core content infrastructure also serves the systems and solutions you deploy, and ESM content you create yourself.

The diagram below shows how ESM uses the system content.

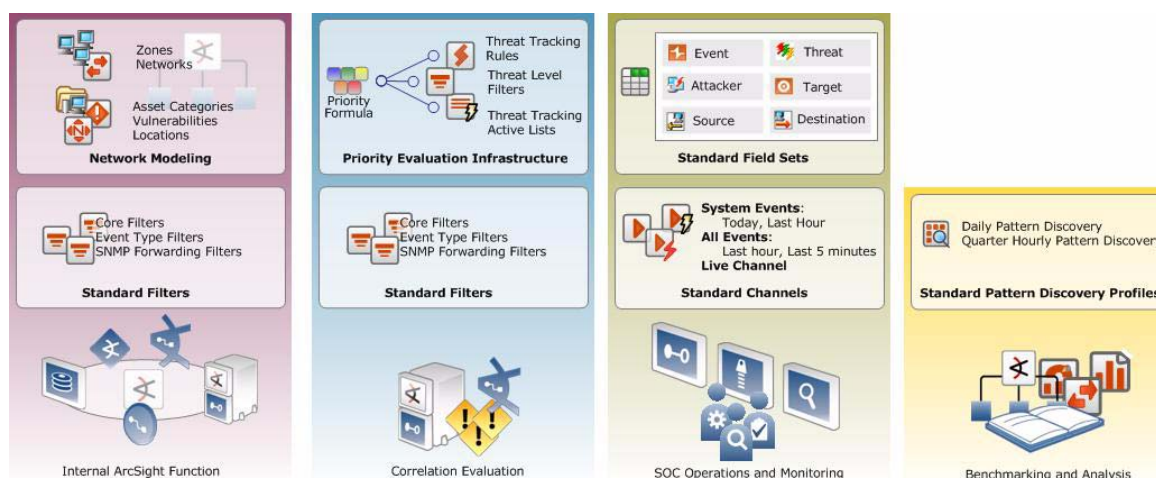


Figure 3-1 The standard features included in the core content support basic ESM functions, such as network modeling, correlation, basic monitoring, and benchmarking.

Shared Resources



ESM contains common resources that support the five foundations. These resources are delivered in their own packages. Dependencies between these resources and the foundation packages they support are managed by the Package resource.

Anti-Virus

The Anti-Virus content is a set of filters, reports, and report queries used by other foundations, such as Configuration Monitoring and Intrusion Monitoring.

Conditional Variable Filters

The Conditional Variable Filters are a library of filters used by variables in standard content report queries, filters, and rule definitions. They express conditions that can also be used by any content in any package.

The Conditional Variable Filters are used by other standard content foundations, such as Anti Virus, Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow foundations.

Network Filters

Network filters are a set of filters required by other standard content foundations, such as Intrusion Monitoring and Network Monitoring. The Network Filters package is installed automatically with ESM.

Standard Content Packages

ESM standard content comes in a series of packages that are either installed automatically with ESM or presented as an install-time option. The following graphic outlines the packages available with ESM, and demonstrates their interoperability.

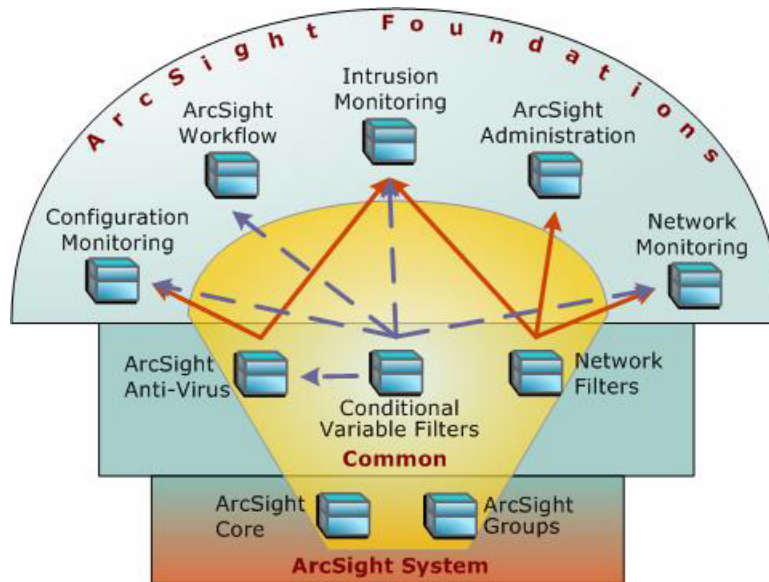


Figure 3-2 The ArcSight System packages at the base provide core content required for ArcSight operation. The Common packages in the center contain shared resources that support the foundation packages. The packages shown on top are ArcSight Foundations that address common network security and ESM management scenarios.

Depending on the options selected when ESM was installed, you will see the ArcSight System resources and some or all of the other package content.

Navigating to Standard Content

Standard content consists of just about every kind of resource available in ESM. If you look in any resource menu after installing ESM, you will find standard content. The example

below shows the Core filters in the ArcSight system tree, and describes the standard content groups that are present when all the standard content is installed.

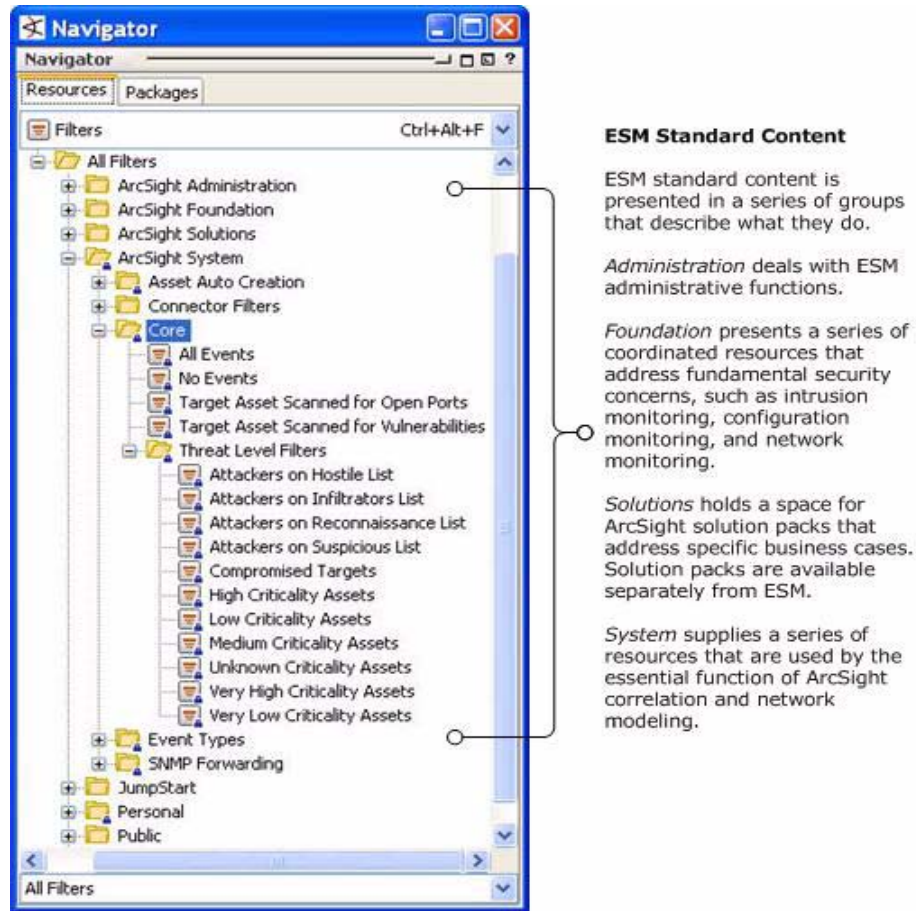


Figure 3-3 Every resource in the ESM resource menu contains standard content, a coordinated set of resources that address common security scenarios and facilitate basic ESM functions. This sample shows the Core filters in the ArcSight System group in the Filters branch.

Set Up Connectors and Model the Network

The graphic below outlines the process for establishing the feeds necessary to drive the standard content:

- 1 Establish relevant SmartConnector feeds
- 2 Model the network
- 3 Assign networks to the appropriate SmartConnectors

4 Test feeds and configure content

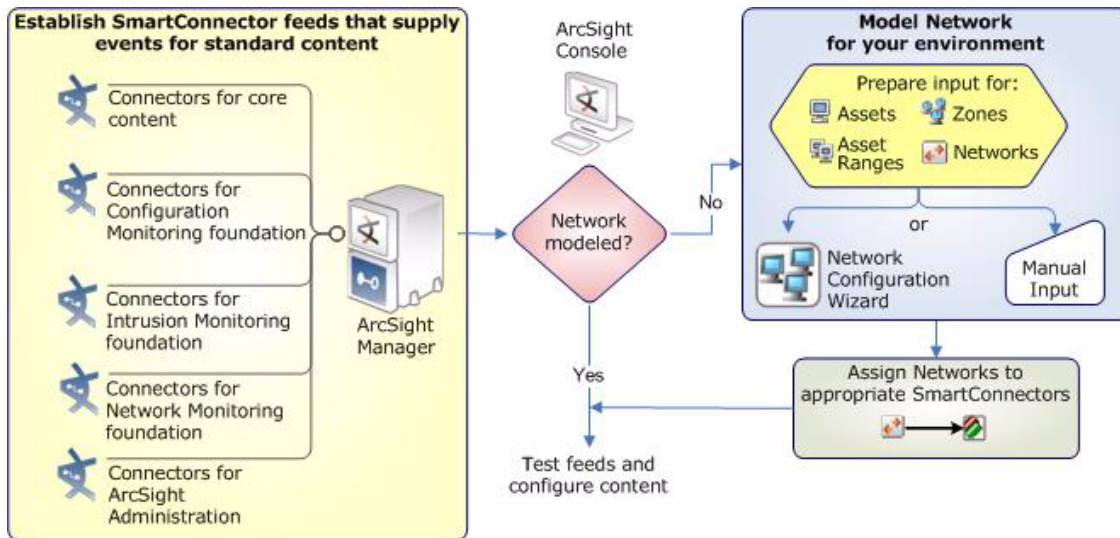


Figure 3-4 Configuring ESM standard content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM.

Standard Content-Related SmartConnectors

The standard content is designed to address event throughput, network health, and basic security-related scenarios. Depending on which packages you installed, verify that you have the minimum types of SmartConnectors reporting into ESM.

Package	Device Types
Anti-Virus (required by Configuration and Intrusion Monitoring foundations)	Anti-virus software, such as: <ul style="list-style-type: none"> • Symantec EndPoint Protection • TrendMicro • McAfee AV
Configuration Monitoring	<ul style="list-style-type: none"> • Operating systems • Security applications (Network and host-based IDS, anti-virus) • User management services (authentication, authorization, and accounting services) • Basic network devices (firewalls, routers, switches, VPN)
Intrusion Monitoring	<ul style="list-style-type: none"> • Network and host-based IDS • Intrusion Prevention Systems (IPS) • Anti-virus • Firewalls
Network Monitoring	<ul style="list-style-type: none"> • Routers • Firewalls • Switches • Real-time flow monitor

Network Modeling

ArcSight ESM uses a model of the network to keep track of the network nodes participating in the event traffic. Having your network modeled and critical assets categorized using the ESM standard asset categories is what activates much of the standard content and makes it effective.

There are several ways to model your network, including the ESM Network Modeling Wizard. If you are modeling the network using the Network Modeling wizard, review the next topic [“Apply Standard Asset Categories to Assets” on page 16](#) before creating the comma-separated values lists to load into the ESM network model.

For more about the network model and how to populate it, see [“Modeling Your Network and Managing Assets” on page 456](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 459](#).

To learn more about the architecture of the ESM network modeling tools, see Chapter 4, “ArcSight Network Model” in *ArcSight 101*.

Apply Standard Asset Categories to Assets

Once your network model is populated with assets, apply the standard asset categories to them to activate standard content that uses these categories to apply criticality and business context to events. Asset categories can be assigned individually using the Asset editor, or in a batch using the Network Modeling wizard.

The asset categories most essential for engaging ESM standard content are discussed in this topic.

For more about asset categories and instructions about how to apply them using the Console tools, see [“Asset Categories” on page 459](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 459](#).

Categorize Internal Assets

Internal Assets are considered to be assets inside the company network. Assets that are not categorized as specifically internal to the network are considered by ESM to be external. This includes assets with different asset categories, and those that are not categorized at all (such as external web sites, unknown external hosts, and so on).

For all assets that are internal to the network, classify them in the following asset category:

```
/All Asset Categories/Site Asset Categories/  
Address Spaces/Protected/
```

How ESM Determines the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

In general, assets do not inherit the categories applied to the zone it belongs to. However, any address contained in the Private Address Space Zones is categorized as *Protected*. For

example, an asset with an IP address of [192.168.0.1](#) is not automatically categorized as *Protected*, however, because it belongs to one of the Private Address Spaces zones, it is considered *Internal* because it belongs to a zone that is categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

Categorize Critical Assets

The asset categories most essential to basic event processing are those used by the Priority Formula to calculate an event's criticality. Asset criticality is one of the four factors used by the priority formula to generate an overall event priority rating.

Assets that are considered critical to protect, such as those that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations, should be classified as critical assets using the following criticality asset category:

[/All Asset Categories/System Asset Categories/Criticality/High](#)

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, see [“Priority Calculations and Ratings” on page 737](#).

Configure Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, the notifications are disabled in the standard content rules, so the admin user will need to configure the destinations AND enable the notification in the rules. For details about enabling the notifications in standard content rules, see [“Configure Rules to Send Notifications and Open Cases” on page 24](#).

The standard content rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center.

- 1** In the Navigator panel, go to **Notifications > Destinations > Shared > All Destinations > CERT Team**
- 2** Right-click Level 1 and select New Destination.
- 3** In the Destination Editor, enter the following values in the Attributes tab and click **OK**:

Field	Value
Name	Enter a name for the destination, such as the user name of the contact, or the role, such as Investigator or Manager.
Start/End Time	If applicable, enter the start and end times of the period this person is available, for example, Start: 08:00:00 AM; End: 04:59:59 PM.

Field	Value
Destination Type	<p>From the drop-down menu, select the method by which the notification will be delivered:</p> <ul style="list-style-type: none"> • Console — Notification popup in this user's ArcSight account • E-Mail — User's e-mail account • Pager — User's pager. Enter the pager's PIN number and service provider. • Cell Phone — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.
User/Group	<p>From the drop-down menu, select the individual user or user group who will receive the notification. This field is required if you selected Console as the destination type, or if you want to use the contacts specified in the User's profile.</p>

- 4 Repeat steps 1, 2, and 3 for each escalation level you want to add. Add more escalation levels as needed.
- 5 Repeat steps 1, 2, 3, and 4 for the SOC Operators destination (**Notifications > Destinations > Shared > All Destinations > SOC Operators**).

Configure Active Lists

The ArcSight System content includes active lists that are designed to be populated manually with data specific to your environment. Once populated with values, these lists are cross-referenced by active channels, filters, rules, reports, and data monitors to give ESM more information about the assets in your environment. For details about active lists and how they work, see *ESM 101* and the topic *Active Lists* in the Console Help.

The active lists that should be configured are:

- **Trusted/Untrusted** active lists in ArcSight System (Lists | Active Lists | [All Active Lists/Arcsight System/Attackers](#)). For more about the Trusted and Untrusted lists, see "Attackers Active Lists" in the ArcSight ESM Standard Content Guide.

The ArcSight System content also includes Active lists that are populated automatically during run-time by rules. These active lists do need not to have entries made to them manually before being used. You can, however, add manual entries to these lists.

You can manually add entries to active lists two ways:

- One by one using the Active List editor in the ArcSight Console. For instructions, see the topic *Editing Active List Entries* in the Console Help.
- In a batch by importing values from a CSV file. For instructions, see the topic *Importing an Active List* in the Console Help.

Configure Asset Auto-Creation Filters

A standard feature of ESM is that it automatically creates assets in the ArcSight asset model for events whose devices are not already modeled either manually or using an asset scanner.

Depending on what devices you have reporting to ArcSight and what devices report in to your network, however, this can cause more individual assets to be added to your asset

model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, ESM would model a new Connector, which falsely adds Connector nodes to the network model.

To limit how ESM automatically models assets in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

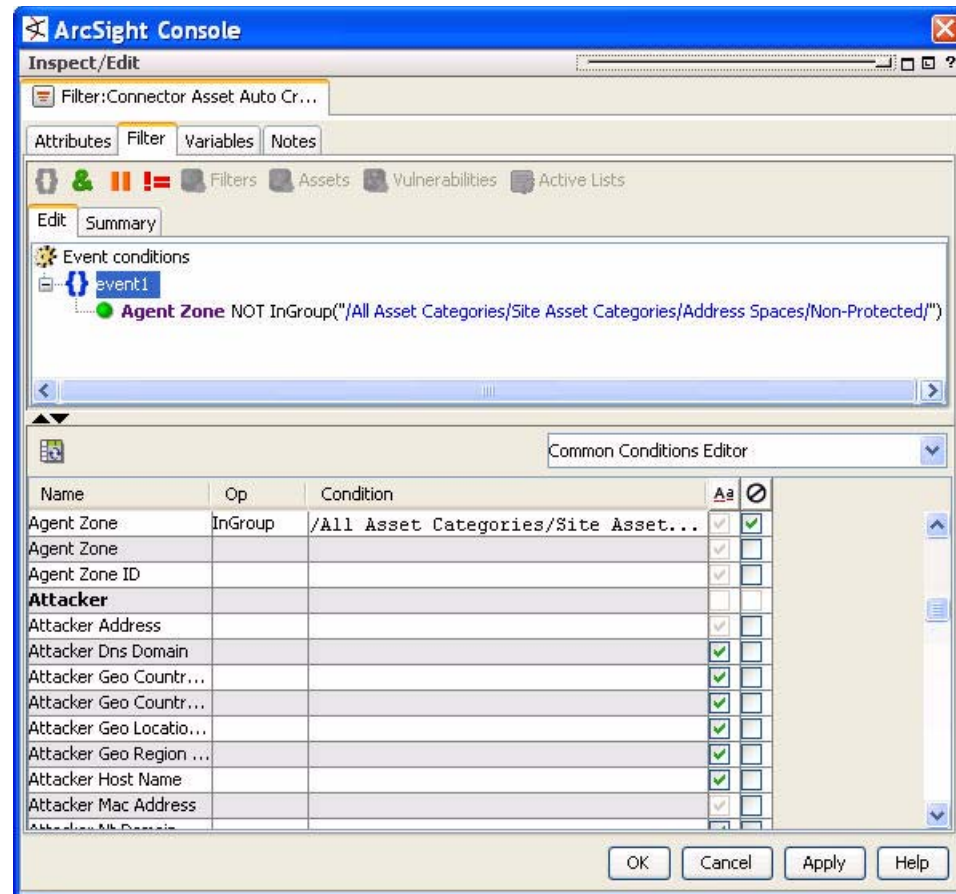
Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs ESM to create an asset for network nodes represented in the events received from the SmartConnectors present in your environment.

By default, the *Connector Asset Auto Creation Controller* filter is configured with the generic condition [True](#), which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to exclude connectors from a specific zone, such as a VPN zone, where the asset already exists, but traffic is coming into the network from an alternate VPN interface. You can also exclude traffic from different types of Connectors, such as from a particular device and vendor.

The example below shows the *Connector Asset Auto Creation Controller* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.

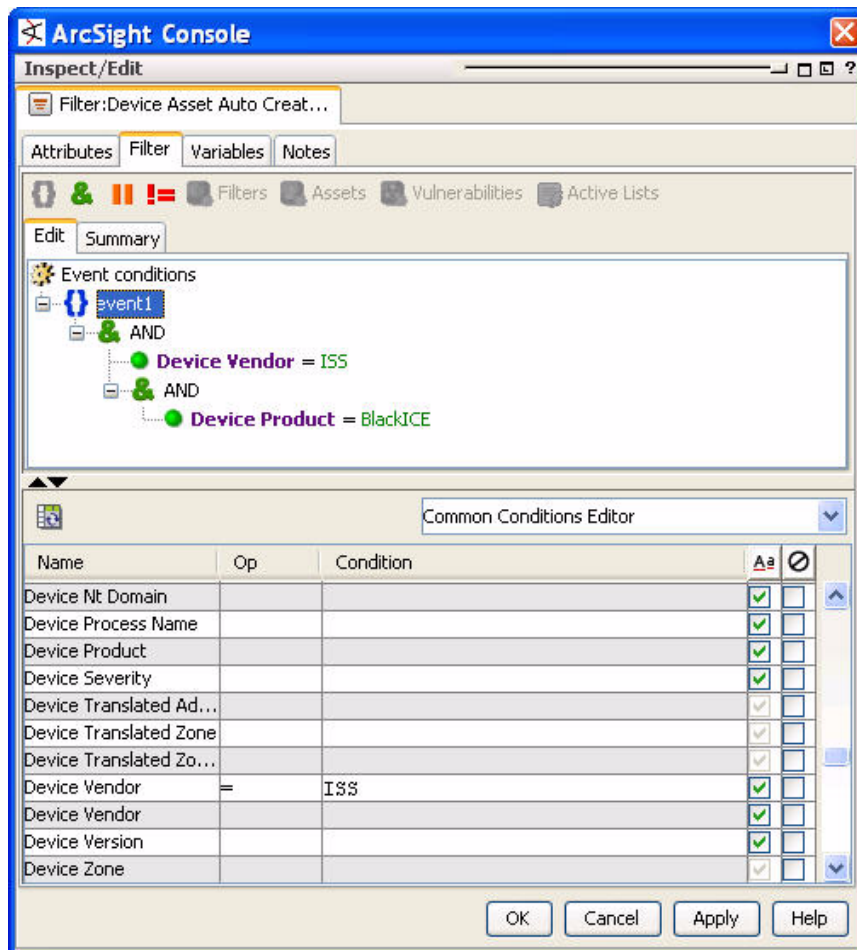



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition [True](#) (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.
- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊖).
- 7 Repeat steps 3 through 5 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.

Configure Device Asset Auto Creation Controller Filter

By default, the *Device Asset Auto Creation Controller* filter is configured with the generic condition `True`, which matches all events. As necessary, you can configure this filter to specify traffic from specific devices and device vendors, or event categories, such as `Hostile`. When you specify an event category, the filter directs the system to only create assets for events with this severity.

The example below shows the *Device Asset Auto Creation Controller* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition `True` (select the condition and press **Delete**).
- 3 Select `event1` and add an AND operator (click the AND icon .
- 4 Select `event1` and use the event fields grid to build the condition, or right-click `event1` and select **New Condition**. Navigate to `Device > Device Vendor`. In the Condition field, enter the vendor name, in this case `ISS`.
- 5 Add the device vendor and product you wish to include.

- a If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to Device > Device Product. In the Condition field, enter the device name, in this case **BlackICE**.
- b If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to Device > Device Product. In the Condition field, enter the device name.

For example, the condition would look like this:

```

OR
    AND
        Device Vendor A
        Device Product 1
    AND
        Device Vendor B
        Device Product 2
    AND
        Device Vendor C
        Device Product 3

```

- 6 Repeat steps 3 through 6 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7 Click **OK** to apply changes and close the Filter editor.

Configure SNMP Trap Forwarding Filter

If you do not have SNMP traps enabled, you can skip this section and move on to “Configure Rules to Send Notifications and Open Cases” on page 24.

The System filters group contains an SNMP Trap Sender filter ([All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#)). The SNMP Trap Sender filter only needs to be configured if you have the SNMP Trap Sender enabled to forward events via SNMP to a network management system, such as HP Openview.

By default, this filter is configured with the filter [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#). If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events will be trapped and forwarded to the network management system.

To configure this filter to forward certain events as an SNMP trap, you can do either of the following:

- Change the default condition in the SNMP Trap Sender filter so it expresses which events should be forwarded as traps. You can express this condition directly in the SNMP Trap Forwarding filter, or you can create another filter that expresses these parameters and point to it in the SNMP Trap Sender filter.
- Change the server configuration (via [server.properties](#)) to point the SNMP trap sender to another filter, and set that filter up as per your convenience.

Change Default Condition in SNMP Trap Forwarding Filter

- 1 In the Navigator panel, navigate to [All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#). Double-click the filter or right-click and select **Edit** to open it in the Filter editor in the Inspect/Edit panel.
- 2 At the Filter tab, change the default condition [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#) to list the type(s) of

events you want forwarded, or to point to another filter that expresses these parameters.

For example, you can create a filter that specifies all events with a priority greater than 8, or events from all Top Secret systems.

Change SNMP Trap Sender in `server.properties`

If you wish to use a filter other than the default `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender`, you must point the SNMP trap sender to the new filter in the ESM Manager `server.properties` file.



These instructions apply **only** if you have SNMP forwarding already enabled at the Manager, *and* if you are using a filter other than the default SNMP Trap Sender filter to forward events.

If the SNMP forwarding feature is not already enabled at the Manager, the `server.properties` file will not contain the string that needs to be modified.

- 1 On the ArcSight ESM Manager machine at a command line, stop the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager stop`
 - ◆ Windows: Stop the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu
- 2 Make a backup copy of the file `$ARCSIGHT_HOME/config/server.properties`.
- 3 In a text editor, open the file `$ARCSIGHT_HOME/config/server.properties` and look for the following lines:

```
# -----
# SNMP Trap Sender configuration.
# -----
# Configuration for the SNMP trapsender. Copy these properties into
# your server.properties file and remove the '#'s (comments). By
# default, the SNMP trap sender is disabled.
#
# set the following property to true to enable trap sending
snmp.trapsender.enabled=false

# Filter that determines what arcsight events will be sent out as
traps
snmp.trapsender.uri=/All Filters/ArcSight System/SNMP
Forwarding/SNMP Trap Sender
```

- 4 Change the `snmp.trapsender.uri` from `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender` to the URI for the filter you want to use.
- 5 Save and close the `server.properties` file.
- 6 Restart the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager start`
 - ◆ Windows: Start the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu

To enable the SNMP trap sender, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.

Configure Rules to Send Notifications and Open Cases

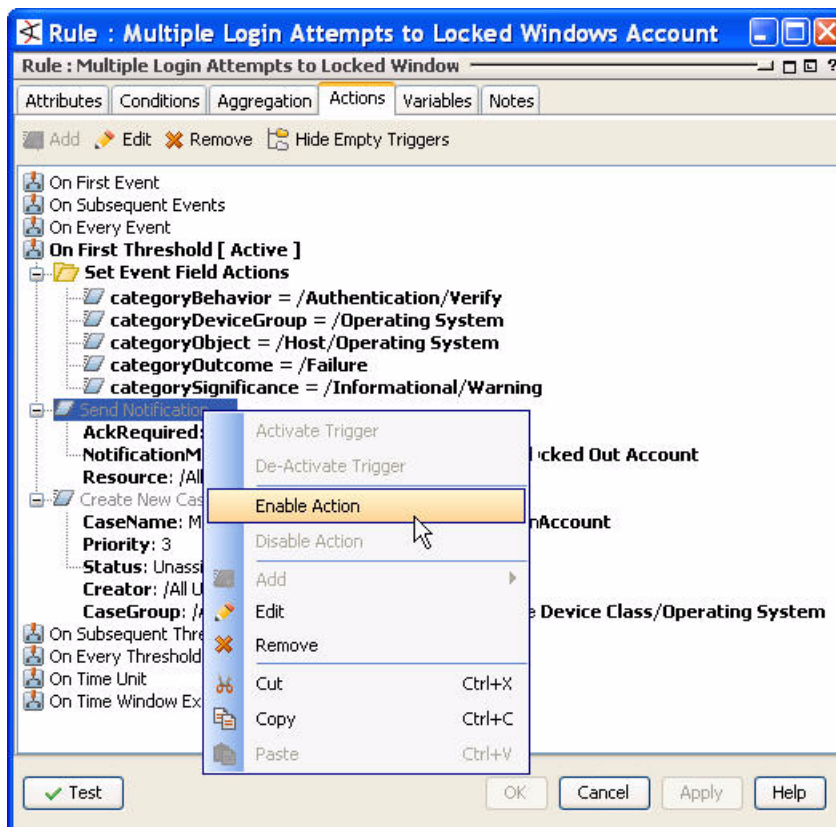
Standard content depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that the standard content is designed to find.

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group. For ESM administration scenarios, notifications are enabled, but case creation is disabled.

To enable standard content rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 17](#), then enable the notification and case actions in the rules.

- 1 In the Navigator panel, navigate to each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 25](#) and [“Configure Rules with Notifications to the SOC Operators” on page 26](#).
- 2 Open the rule for editing in the Inspect/Edit panel (double-click the rule or right-click it and select **Edit**).
- 3 In the Rule Editor in the Inspect/Edit panel, click the **Action** tab.
- 4 Find the *Send Notification* action. The disabled action will appear in grey text. To enable it, select the **Send Notification** action name, right-click it, and select **Enable**.

The example below shows the Action tab for the rule *Multiple Login Attempts to Locked Windows Account*.



- 5 To also create a case when the rule conditions are met, edit the action to give it an owner and enable the action.
 - a Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
 - b In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate ESM user. Click **OK**.
 - c Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.
- 6 Repeat steps 1 through 6 for each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 25](#) and [“Configure Rules with Notifications to the SOC Operators” on page 26](#).

For more about working with Rule actions in the Rules Editor, see [“Creating Rule Actions” on page 310](#) and [“Applying Rule Actions” on page 315](#).

Configure Rules with Notifications to the Cert Team

The following security-related rules send notifications to the **CERT Team** notification group. In these rules, both the notification and case creation actions are disabled by default.

Cases created by these rules should be assigned to the appropriate user or user group in your organization.

Rule URI (File Path)	Rule Name
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Windows Account Locked Out Multiple Times
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Insecure Configuration
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Vulnerable Software
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/	Notify on Successful Attack

Configure Rules with Notifications to the SOC Operators

The following ArcSight Administration rules send notifications to the **SOC Operators** notification group. For these rules, the notification is enabled, and the case creation is disabled by default. Cases created by these rules are assigned to the ESM Admin user.

Rule URI	Rule Name
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Excessive Rule Recursion
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Rule Matching Too Many Events
/All Rules/ArcSight Administration/ESM/System Health/Storage/	ASM Database Free Space - Critical

Schedule Reports

Reports can be run on demand, automatically on a regular schedule, or both. By default, the reports that come with ESM are not scheduled to run automatically.

Evaluate the reports that come with the foundations you have installed, and schedule the reports that are of interest to your organization and business objectives.

For instructions about how to schedule reports, see [“Archiving Reports” on page 294](#).

Default Trends Schedule

Trends are a type of report query that can gather data over longer periods of time, which can be leveraged for reports. Trends streamline data gathering to the specific pieces of data you want to track over a long range, and breaks the data gathering up into periodic updates. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources. Trends can also provide a snapshot of which devices report on the network over a series of days.

The standard content contains trends that monitor long-term conditions among the ArcSight foundations.

Based on the volume of data generated by some of these queries, only some of the trends are enabled by default at installation; the rest are disabled by default.

The enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually slower than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the Console.

ESM standard trends are listed below with their status on installation, and the time at which they are scheduled to run.

ArcSight Administration Trends

Both ArcSight Administration trends are enabled by default.

ArcSight Administration Trends	Status	Schedule
Trend Queries	Enabled	4:00 a.m.
ASM Database Free Space	Enabled	4:30 a.m.
ArcSight User Login Trends – Hourly	Enabled	5:00 a.m.

Configuration Monitoring Trends

Seven of the 13 Configuration Monitoring trends are enabled by default.

Configuration Monitoring Trends	Status	Schedule
Assets with Recent Configuration Modifications - Daily Trend	Enabled	12:40 a.m.
Host Configuration Modifications	Enabled	1:35 a.m.
Asset Startup and Shutdown Events - Daily Trend	Enabled	2:40 a.m.
Critical System Startup and Shutdown Events - Daily Trend	Disabled	N/A
Most Common Account Login Attempts - Daily Trend	Enabled	3:40 a.m.
User Account Login Failures	Enabled	4:40 a.m.
AAA User Account Creation	Disabled	N/A
AAA User Account Deletions	Disabled	N/A
Account Creation by Host	Disabled	N/A
Accounts Deleted by Host	Disabled	N/A
Local Windows User Creation - Disallowed Systems	Disabled	N/A
Password Modifications	Disabled	N/A
User Account Creation	Enabled	5:40 a.m.
User Account Modifications	Enabled	6:20 a.m.
User Removals	Enabled	1:15 a.m.
VPN User Account Creation	Disabled	N/A
Top Vulnerability Exposure of Critical Assets	Enabled	5:10 a.m.
Vulnerability Exposure by Asset Criticality (Snapshot)	Enabled	1:50 a.m. once a week
Vulnerability Exposure of Critical Assets (snapshot)	Enabled	3:30 a.m.
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend (Snapshot)	Disabled	N/A

Intrusion Monitoring Trends

Eight of the 16 Intrusion Monitoring trends are enabled by default.

Intrusion Monitoring (8/16)	Status	Schedule
SANS Top 20 (v6.01) Attacked Systems	Disabled	N/A
Prioritized Attack Counts by Service	Disabled	N/A
Prioritized Attack Counts by Target Zone	Disabled	N/A
Inbound DoS Events	Disabled	N/A
Environment Status Events	Disabled	N/A
Port Scanning	Enabled	1:20 a.m.
Port Scanning Daily Top 20	Enabled	2:20 a.m.
Reconnaissance Activity	Disabled	N/A
Reconnaissance Types Detected	Disabled	N/A
Top 10 Reconnaissance Types Detected	Disabled	N/A
Zone Scanning Events by Priority	Enabled	4:20 a.m.
Brute Force Access Session Trends	Enabled	1:40 a.m.
Daily Top 10 Resource Access Trends	Disabled	N/A
Resource Access	Disabled	N/A
Asset Counts by Vulnerability (Snapshot)	Enabled	12:20 a.m. once a week
Prioritized Vulnerability Events by Zone	Enabled	5:20 a.m.
Top 10 Daily Vulnerability Events	Enabled	6:25 a.m.
Failed Logins per Hour	Enabled	6:00 a.m.
Top Users with Failed Logins per Day	Enabled	6:40 a.m.
Number of Vulnerabilities per Asset (Snapshot)	Enabled	3:20 a.m. once a week

Network Monitoring Trends

All three Network Monitoring trends are disabled by default.

Network Monitoring	Status	Schedule
Inbound Traffic by Application Protocol	Disabled	N/A
Outbound Traffic by Application Protocol	Disabled	N/A
Overall Traffic	Disabled	N/A

Workflow Trends

One Workflow trend is enabled by default, and the other is disabled by default.

Network Monitoring	Status	Schedule
Notification Events	Disabled	N/A
Notifications	Enabled	6:00 a.m.

How to Enable/Disable Trends



If you wish to enable a disabled trend, you must first **change the default start date** in the Trend editor, then enable it.

If the start date is not changed, the trend will take the default start date (which is derived from when the trend was first installed), and backfill the data from that time. For example, if you enable the trend 6 months after the first install, these trends will try to get all the data for the last 6 months, which would cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

To enable a disabled trend:

- 1 Edit the trend to change the default start date.
 - a Double-click the trend, or right-click it and select **Edit Trend** to open it in the Trend Editor in the Inspect/Edit panel.
 - b In the Trend editor, click the **Parameters** tab. In the *Query Parameters* section, find Start Time and uncheck the **Use Default** checkbox.
 - c In the *Value* drop-down menu, select a start date appropriate for the frequency at which the trend is scheduled to run. For example, if the trend is scheduled to run daily, select a start date of a week or less earlier than today. Keep in mind the data partitioning schedule your Manager uses to make sure the time frame you have specified provides adequate online access to the events. Click **Apply**.
- 2 Enable the trend.
 - ◆ If the Trend editor is still open, click the **Attributes** tab and check the **Enabled** checkbox. Click **OK** to apply changes and close the Trend editor.
 - ◆ If the Trend editor is closed, right-click the trend in the Navigator panel and select **Enable Trend**.

To disable an enabled trend:

- In the Navigator panel, right-click the trend you want to enable and select **Disable Trend**.

How to Monitor Trend Performance

The ArcSight Administration foundation contains resources that enable you to monitor the performance of your enabled trends. The Trends Status dashboard shows the run-time status for all enabled trends. The Trend reports show statistics about trend performance for all enabled trends.

Getting Started Using Standard Content

Whatever your role in the security operations center, you can get started right away using the ESM standard content.

Each foundation is organized with content for different types of users.

- **Executive Summaries.** Executive summaries provide high-level analysis of event activity for management reports. These views show overall trends and long-term summaries.
- **Operational Summaries.** The operational summaries are intended for SOC operators and analysts for daily event monitoring and triage-level investigation.
- **Details.** The detailed content is intended for incident responders and analysts who need access to relevant event details in order to investigate situations that arise from monitoring reports in the operational summaries.
- **SANS Top 5 Reports.** Each foundation contains a set of reports that address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports.

Monitoring with Standard Content

You can use standard content to begin monitoring your network immediately when SmartConnectors are added and basic configuration is complete.

Active Channels

Each foundation provides high-level channels for observing general activity for its area of focus.

Foundation	Channel	Description
ArcSight System	System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	Today	Channel showing events received today since midnight. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	All Events / Last 5 Minutes and Last Hour	Channel showing events received during the last five minutes or the last hour. The channel includes a sliding window that always displays exactly the last five minutes of event data.
	Core / Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing correlation events.

Foundation	Channel	Description
Configuration Monitoring	Operational Summaries / High-Priority Scan Events Directed Toward High-Criticality Assets	This channel shows scan results in real time to give you a view into any high-priority vulnerabilities detected on highly critical assets.
Intrusion Monitoring	Intrusion Monitoring - Significant Events	<p>This channel provides an overview of hostile, compromise or high priority events. It continuously monitors events matching:</p> <ul style="list-style-type: none"> • Not ArcSight Internal Events • Priority greater than 8 or Category Significance Starts With /Compromise or /Hostile <p>Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).</p>
Network Monitoring	Argus Events	This active channel shows all the events coming from Argus SmartConnectors for the past 24 hours.
Workflow	Assigned Events	This channel shows events assigned today. The channel always displays events occurring since midnight of the current day up to the current time. A filter prevents the channel from showing correlated events. It shows only events that are not in closed stage and are assigned to a user.

Each foundation contains more channels that focus on events of different types. Explore the active channels to monitor the activity you are interested in.

For more about using active channels, see [“Monitoring Active Channels” on page 91](#).

Dashboards

Each foundation also includes general dashboards that provide a high-level view of activity for its area of focus.

Foundation	Dashboard	Description
Configuration Monitoring	Operational Summaries	This group contains four dashboards that provide an overview of configuration changes, database errors, host configuration modifications, and an overview of hosts with problems.

Foundation	Dashboard	Description
Intrusion Monitoring	Operational Summaries / Security Activity Statistics	<p>This dashboard is a window into the health of common avenues for security threats on the network, including transport protocols, address spaces, application protocols, and statistics involving the top target and attacker IPs, among others.</p> <p>The Intrusion Monitoring foundation contains many other dashboards that provide general executive-level summaries, and more detailed views on different focus areas for operations and investigations.</p>
Network Monitoring	General	<p>The dashboards in the General group provide an overview of the top traffic to mail and web servers, and moving average statistics for TCP, UDP, ICMP, and SYN transport protocols.</p> <p>The Network Monitoring foundation contains many more dashboards that provide more detail about network health, including bandwidth usage, inbound and outbound traffic, and activity from firewalls, network devices, and VPNs.</p>

Investigating with Standard Content

Each foundation contains resources that enable operators to view detailed activity and drill down, investigate, track, graph, map, and export, just to name a few.

Use **active channels** to view and sort event flows, investigate blocks of events, and drill down into single event details. For more about using active channels to investigate event activity, see [“Monitoring Active Channels” on page 91](#).

Use **dashboards** to view activity from many perspectives in a single screen. Dashboards are also fully drill-down enabled. For more about investigating using dashboards, see [“Using Dashboards” on page 113](#).

Use the Daily and Quarter Hourly **Pattern Discovery** profiles to find traffic patterns that are not easily detected using other methods. For more about investigating using Pattern Discovery, see [“Pattern Discovery” on page 127](#).

Reporting with Standard Content

ESM standard content supplies a robust set of reports for each ESM foundation. The reports for each foundation are organized into different levels of detail depending on who the reports are for as outlined in [“Getting Started Using Standard Content” on page 30](#).

Foundation	Reports
Common	The Common group contains a set of anti-virus reports that apply to all the foundations.

Foundation	Reports
Configuration Monitoring	<ul style="list-style-type: none"> • Detailed reports concentrate on configuration changes by device and by user, inventories of applications and assets by role, and vulnerabilities by asset, asset type, asset criticality, and so on. • Executive Summary reports focus on overall host configurations by zone, role, criticality, data role, and operating system. • Operational Summaries provide summaries of host configuration modifications by Customer, OS, and over the last 30 days; top user login successes and failures over recent time periods; and asset restarts over recent time periods. • SANS Top 5 Reports focus on SANS section 3: Unauthorized Changes to Users, Groups, and Services.
Intrusion Monitoring	<ul style="list-style-type: none"> • Detailed reports are organized into types of activity: anti-virus; attack monitoring; environment state for applications, operating systems, and services; reconnaissance attempts; access events; user activity through device type; vulnerability activity by asset and by vulnerability; and worm outbreak activity. • Executive Summary reports provide an overall Security Intelligence Status Report, and summary views by business role and systems that are subject to regulations, such as the Sarbanes-Oxley Act. • Operational Summaries provide mid-level summaries organized into device types, such as anti-virus, attack monitoring, and reconnaissance. • SANS Top 5 Reports focus on SANS sections 1, 4, and 5: Attempts to Gain Access, Through Existing Accounts, Systems Most Vulnerable to Attack, and Suspicious or Unauthorized Network Traffic Patterns.
Network Monitoring	<ul style="list-style-type: none"> • Detailed reports provide views into traffic by host, by protocol, and by target, and activity over network devices and VPNs. • Executive Summary reports provide traffic summaries over daily, monthly, quarterly, and weekly time intervals. • Operational Summaries provide an overall traffic snapshot; bandwidth utilization statistics by device and by time interval; and statistics for inbound and outbound traffic by protocol and by host. • SANS Top 5 Reports focus on SANS section 5: Suspicious or Unauthorized Network Traffic Patterns.
Workflow	<ul style="list-style-type: none"> • Detailed reports provide statistics for all cases, notifications, and notification action events. • Executive Summary reports provide overall case statistics, such as average time to case resolution, number of cases at each escalation stage, and cases as they affect operations. • Operational Summaries provide detailed case statistics, including trends over time, notifications that reach level 3, the status of notifications by user, and so on.

Chapter 4

ArcSight Express Solution

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

The ESM portion of the ArcSight Express solution comes with a series of coordinated resource systems that address common enterprise network security and ArcSight administration tasks. These resource systems are referred to collectively as *ArcSight Express content*.

With some basic configuration done using the ESM Console, ArcSight Express content enables you to get started using ArcSight Express right away to effectively manage enterprise security operations without having to create additional resources.

The Logger storage portion of the ArcSight Express solution comes with basic system-level filters and foundation reports. For more information about the standard Logger filters and reports, see the *Logger Administrator's Guide*.

["What is ArcSight Express Content?" on page 35](#)
["How ArcSight Express Is Organized" on page 36](#)
["Set Up Connectors and Model the Network" on page 36](#)
["Apply Standard Asset Categories to Assets" on page 39](#)
["Create ArcSight Express Users" on page 39](#)
["Configure Notification Destinations" on page 40](#)
["Configure Asset Auto-Creation Filters" on page 41](#)
["Configure Rules to Send Notifications and Open Cases" on page 44](#)
["Schedule Reports" on page 47](#)
["Tuning ArcSight Express Content" on page 48](#)

What is ArcSight Express Content?

ArcSight Express content is a series of coordinated [Resources](#) (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. ArcSight Express content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration using the ArcSight Console.

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

The instructions in this topic describe how Administrators can configure the ArcSight Express content for the users of the ArcSight Web interface.

How ArcSight Express Is Organized

ArcSight Express content monitors and reports on activity relevant to the types of devices reporting into ESM. The content is organized into the following device-specific groups:

Function	Description
Cross-Device	Functions that apply to multiple kinds of devices, such as login attempts, bandwidth usage, and configuration changes.
Anti-Virus	Activity involving anti-virus devices, such as update status, virus activity, and configuration changes.
Case Management	Activity and notifications involving cases opened in ArcSight as a result of events that warrant investigation.
Database	Database activity, such as configuration changes, database logins, errors and warnings.
Firewall	Firewall activity, such as network logins and logouts, denied connections, bandwidth usage, and configuration changes.
Identity Management	User activity, such as logins, user session durations, and configuration changes in order to identify who is doing what activity on the network.
IDS-IPS	Activity involving Intrusion Detection and Prevention Systems, such as signature updates, alerts, and statistics.
Network	Activity involving network infrastructure, including system up/down status, configuration changes, bandwidth usage, and login events.
Operating System	Activity involving operating systems, such as user logins, and user modification events.
VPN	Activity involving VPN connections, including authentication errors, logins, and connection status.
Vulnerabilities	Resources that monitor and report on exposed vulnerabilities by asset.

Set Up Connectors and Model the Network

The graphic below outlines the process for establishing the feeds necessary to drive the ArcSight Express content:

- 1 Establish relevant SmartConnector feeds
- 2 Model the network
- 3 Assign networks to the appropriate SmartConnectors

4 Test feeds and configure content

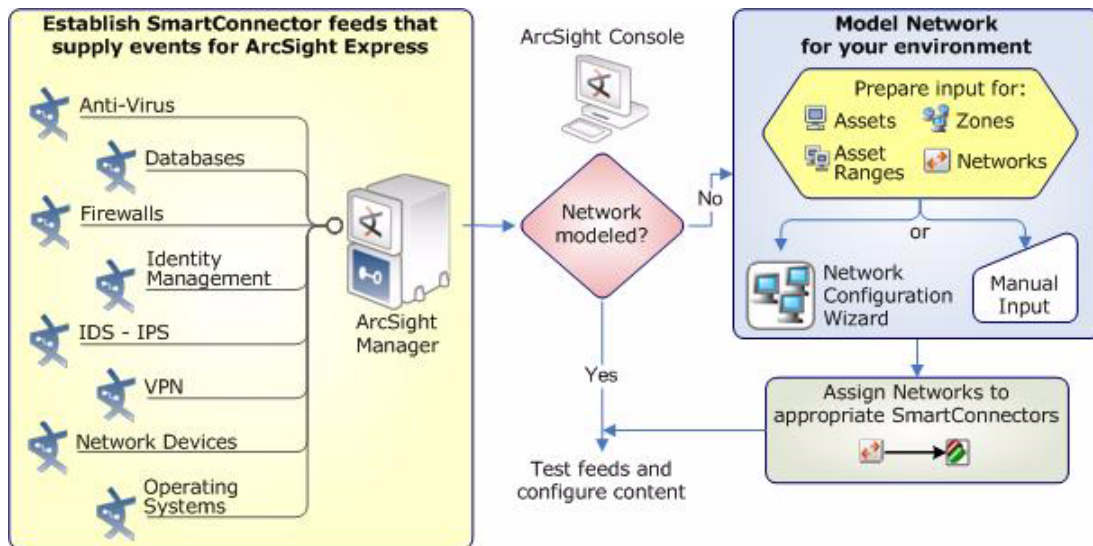


Figure 4-1 Configuring ArcSight Express content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM.

ArcSight Express-Related SmartConnectors

The ArcSight Express content is designed to address event throughput, network health, and basic security-related scenarios. The ArcSight Express content supports feeds from the following types of SmartConnectors.

Device Group	Related Connectors
Anti-Virus	Most major anti-virus products, such as: <ul style="list-style-type: none"> • Symantec EndPoint Protection • TrendMicro • McAfee AV
Database	The database content for basic error reporting and user info that comes from most database connectors, such as: <ul style="list-style-type: none"> • Oracle 10g • MSSQL Server
Firewall	Firewall content picks up parsed and categorized events from specific firewalls, all-in-one devices, and client-side firewalls, such as those found on Windows. Examples include: <ul style="list-style-type: none"> • Juniper Netscreen • CheckPoint • Cisco PIX
Identity Management	Identity management content picks up from identity management systems, such as: <ul style="list-style-type: none"> • Juniper Steel-Belted Radius • Cisco Secure ACS • Windows AD

Device Group	Related Connectors
IDS - IPS	<p>This content picks up events from any IDS/IPS system for which ArcSight supplies a Connector, including combination devices that may generate events of these types. For example:</p> <ul style="list-style-type: none"> • ISS Site Protector • Symantec Network Security • Cisco IPS
Network	<p>This content works on events from networking devices, such as:</p> <ul style="list-style-type: none"> • Cisco IOS Devices • Juniper JunOS Devices
Operating System	<p>This content picks up events from Windows and Unix-based systems that generate relevant events and for which ArcSight supplies supported connectors, such as:</p> <ul style="list-style-type: none"> • Linux OS Events (All major Versions) • MS Windows (2003/XP)
VPN	<p>This content works on events from most VPN devices that report on errors, sessions established, and so on. For example:</p> <ul style="list-style-type: none"> • Juniper/Netscreen VPN • Cisco VPN • CheckPoint VPN-1
Vulnerabilities	<p>Vulnerability content relies on the ESM device model, which can be populated one by one, or by a vulnerability scanner for which ArcSight supplies a Connector.</p>

Network Modeling

ArcSight ESM uses a model of the network to keep track of the network nodes participating in the event traffic. Having your network modeled and critical assets categorized using ESM standard asset categories is what activates much of the ArcSight Express content and makes it effective.

There are several ways to model your network, including the ESM Network Modeling Wizard. If you are modeling the network using the Network Modeling wizard, review the topic [“Apply Standard Asset Categories to Assets” on page 39](#) before creating the comma-separated values lists to load into the ESM network model.

For more about the network model and how to populate it, see [“Modeling Your Network and Managing Assets” on page 456](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 459](#).

To learn more about the architecture of ESM's network modeling tools, see Chapter 4, “ArcSight Network Model” in *ArcSight 101*.

Apply Standard Asset Categories to Assets

Once assets are added to the network model, or if you are adding them in bulk using the Network Modeling wizard, categorize relevant assets as internal to the network, and/or as critical assets.

Assets can be categorized individually using the Assets Editor, or in bulk using the Network Modeling wizard. Asset categories can also be applied to zones.

For more about asset categories and instructions about how to apply them using the Assets Editor, see [“Asset Categories” on page 459](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 459](#).

Categorize Internal Assets

Internal Assets are considered to be assets inside the company network. Assets that are not categorized as specifically internal to the network are considered by ESM to be external. This includes assets with different asset categories, and those that are not categorized at all (such as external web sites, unknown external hosts, and so on).

For all assets that are internal to the network, classify them in the following asset category:

```
/All Asset Categories/Site Asset Categories/Address Spaces/Protected/
```

How ESM Determines the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

By default, the Private Address Space Zones are categorized as *Protected*. Assets within a zone that has been categorized do not inherit categories from the zone. For example, an asset with an IP address of 192.168.0.1 is not automatically categorized as *Protected*, but it belongs to one of the Private Address Spaces zones, so it is considered *Internal* because it belongs to a zone categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

Categorize Critical Assets

Assets that are considered critical to protect, such as those that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations, should be classified as critical assets using the following asset category:

```
/All Asset Categories/System Asset Categories/Criticality/High
```

Create ArcSight Express Users

ArcSight Express comes configured with a custom user group called ArcSight Express. Add users to this group with ArcSight Web privileges.

- 1 In the Navigator panel, go to **Users > Shared > Custom User Groups**
- 2 Right click on ArcSight Express and select **New User**

- 3 For each user you add, provide a User ID and Password, and set the User Type to **Web User** and click **OK**.

For more about creating users, see [“Managing Users” on page 438](#).

Configure Notification Destinations

Configure notification destinations if you want to be notified when some of the ArcSight Express rules are triggered. By default, the notifications are disabled in the ArcSight Express rules, so the admin user will need to configure the destinations AND enable the notification in the rules. For details about enabling the notifications in ArcSight Express rules, see [“Configure Rules to Send Notifications and Open Cases” on page 44](#).

The ArcSight Express rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center.

- 1 In the Navigator panel, go to **Notifications > Destinations > Shared > All Destinations > CERT Team**
- 2 Right-click Level 1 and select New Destination.
- 3 In the Destination Editor, enter the following values in the Attributes tab and click **OK**:

Field	Value
Name	Enter a name for the destination, such as the user name of the contact, or the role, such as Investigator or Manager.
Start/End Time	If applicable, enter the start and end times of the period this person is available, for example, Start: 08:00:00 AM; End: 04:59:59 PM.
Destination Type	From the drop-down menu, select the method by which the notification will be delivered: <ul style="list-style-type: none"> • Console — Notification popup in this user's ArcSight account • E-Mail — User's e-mail account • Pager — User's pager. Enter the pager's PIN number and service provider. • Cell Phone — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.
User/Group	From the drop-down menu, select the individual user or user group who will receive the notification. This field is required if you selected Console as the destination type, or if you want to use the contacts specified in the User's profile.

- 4 Repeat steps 1, 2, and 3 for each escalation level you want to add. Add more escalation levels as needed.
- 5 Repeat steps 1, 2, 3, and 4 for the SOC Operators destination (**Notifications > Destinations > Shared > All Destinations > SOC Operators**).

Configure Asset Auto-Creation Filters

A standard feature of ESM is that it automatically creates assets in the ArcSight asset model for events whose devices are not already modeled either manually or using an asset scanner.

Depending on what devices you have reporting to ArcSight and what devices report in to your network, however, this can potentially cause a lot of unnecessary individual assets to be added to your asset model. For example, laptops with the intrusion detection system BlackICE from ISS can generate a new asset ID for that device every time the laptop logs onto the network. This situation also applies to VPN and wireless networks every time a device logs onto a new subnet.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, ESM would model a new Connector, which falsely clutters the network model with Connector nodes.

To limit how ESM automatically models assets in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

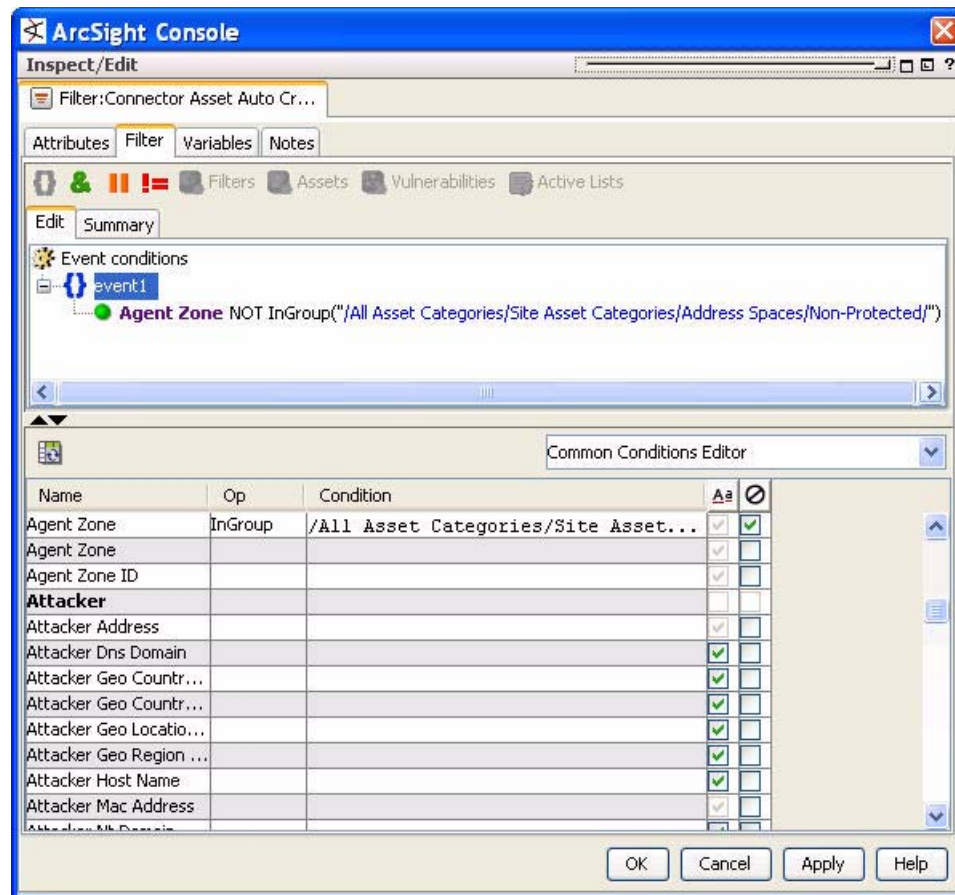
Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs ESM to create an asset for network nodes represented in the events received from the SmartConnectors present in your environment.

By default, the *Connector Asset Auto Creation Controller* filter is configured with the generic condition `True`, which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to exclude connectors from a specific zone, such as a VPN zone, where the asset already exists, but traffic is coming into the network from an alternate VPN interface. You can also exclude traffic from different types of Connectors, such as from a particular device and vendor.

The example below shows the *Connector Asset Auto Creation Controller* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.



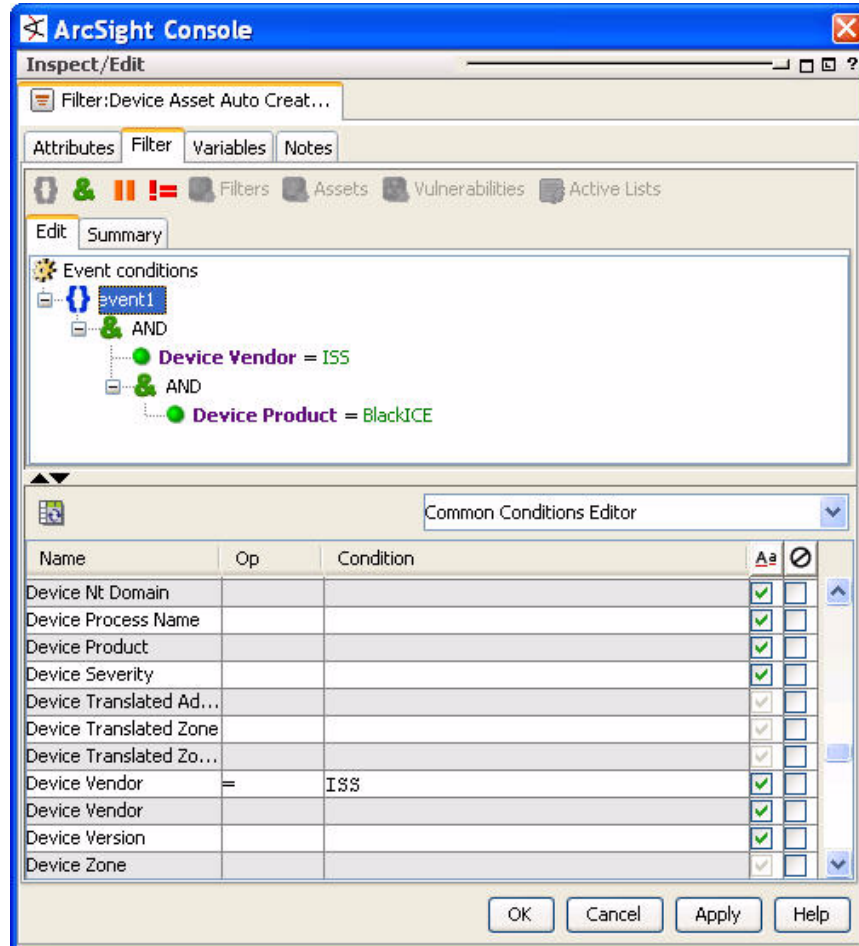
- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.
- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊖).
- 7 Repeat steps 3 through 5 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.


Configure Device Asset Auto Creation Controller Filter

By default, the *Device Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to

specify traffic from specific devices and device vendors, or event categories, such as [Hostile](#). When you specify an event category, the filter directs the system to only create assets for events with this severity.

The example below shows the *Device Asset Auto Creation Controller* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 Select **event1** and add an AND operator (click the AND icon .
- 4 Select **event1** and use the event fields grid to build the condition, or right-click event1 and select **New Condition**. Navigate to [Device > Device Vendor](#). In the Condition field, enter the vendor name, in this case **ISS**.
- 5 Add the device vendor and product you wish to include.
 - a If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to [Device > Device Product](#). In the Condition field, enter the device name, in this case **BlackICE**.

- b** If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to Device > Device Product. In the Condition field, enter the device name.

For example, the condition would look like this:

```
OR
  AND
    Device Vendor A
    Device Product 1
  AND
    Device Vendor B
    Device Product 2
  AND
    Device Vendor C
    Device Product 3
```

- 6** Repeat steps 3 through 6 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7** Click **OK** to apply changes and close the Filter editor.

Configure Rules to Send Notifications and Open Cases

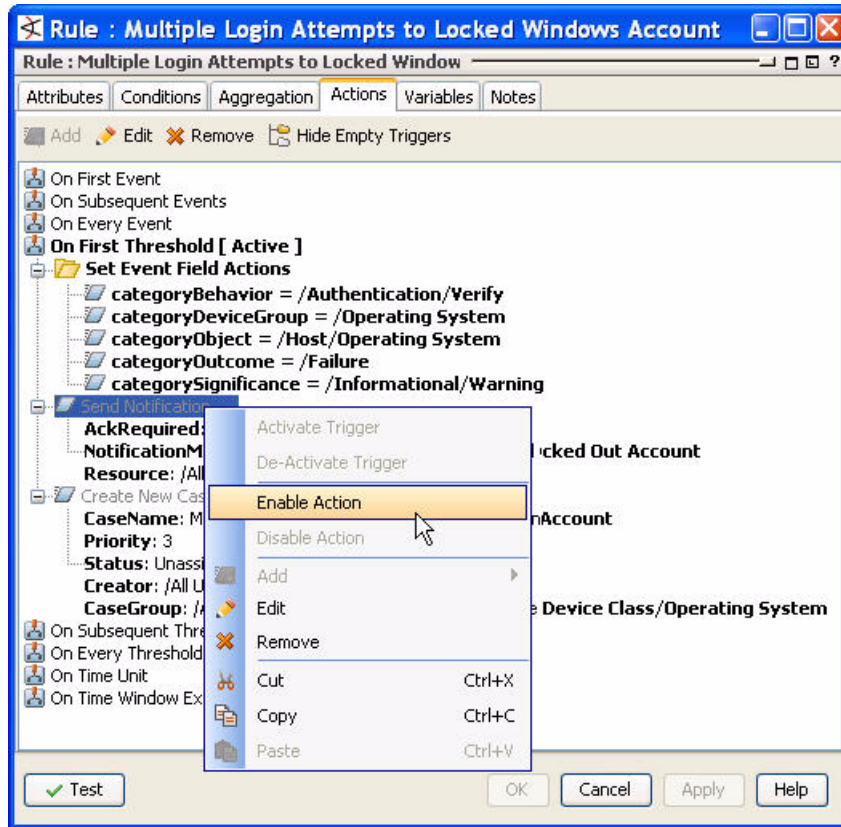
ArcSight Express depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that ArcSight Express is designed to find.

By default, the notifications and create case actions are disabled in the ArcSight Express rules that send notifications about security-related events to the Cert Team notification group. For ESM administration scenarios, notifications are enabled, but case creation is disabled.

To enable ArcSight Express rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 40](#), then enable the notification and case actions in the rules.

- 1** In the Navigator panel, navigate to each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 45](#) and [“Configure Rules with Notifications to the SOC Operators” on page 46](#).
- 2** Open the rule for editing in the Inspect/Edit panel (double-click the rule or right-click it and select **Edit**).
- 3** In the Rule Editor in the Inspect/Edit panel, click the **Action** tab.
- 4** Find the *Send Notification* action. The disabled action will appear in grey text. To enable it, select the **Send Notification** action name, right-click it, and select **Enable**.

The example below shows the Action tab for the rule *Multiple Login Attempts to Locked Windows Account*.



- 5 To also create a case when the rule conditions are met, edit the action to give it an owner and enable the action.
 - a Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
 - b In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate ArcSight Express user. Click **OK**.
 - c Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.
- 6 Repeat steps 1 through 6 for each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 45](#) and [“Configure Rules with Notifications to the SOC Operators” on page 46](#).

For more about working with Rule actions in the Rules Editor, see [“Creating Rule Actions” on page 310](#) and [“Applying Rule Actions” on page 315](#).

Configure Rules with Notifications to the Cert Team

The following security-related rules send notifications to the **CERT Team** notification group. In these rules, both the notification and case creation actions are disabled by default.

Cases created by these rules should be assigned to the appropriate user or user group in your organization.

Rule URI (File Path)	Rule Name
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Windows Account Locked Out Multiple Times
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Insecure Configuration
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Vulnerable Software
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/	Notify on Successful Attack

Configure Rules with Notifications to the SOC Operators

The following ArcSight Administration rules send notifications to the **SOC Operators** notification group. For these rules, the notification is enabled, and the case creation is disabled by default. Cases created by these rules are assigned to the ArcSight Express Admin user.

Rule URI	Rule Name
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Excessive Rule Recursion
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Rule Matching Too Many Events
/All Rules/ArcSight Administration/ESM/System Health/Storage/	ASM Database Free Space - Critical

Schedule Reports

Reports can be run on demand, automatically on a regular schedule, or both. By default, the reports that come with ArcSight Express are not scheduled to run automatically.

You may want to schedule certain reports that are based on cases, notifications, assets (not based on events). These non-event-based reports cannot be run for the previous day or the previous week, which means that their output is always the “current” state.

An example of an asset-based report that you may want to schedule would be *Exposed Vulnerability Count by Critical Asset*.

Reports on cases

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases by Operational Impact
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Case Stage Counts
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	All Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases per Target
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Open Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Today's Cases

Reports on notifications

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Statistics Summary
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	All Level 3 Notifications
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Status Report
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notifications By Acknowledgement Status
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Unacknowledged Level 3 Notifications

Reports on assets

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerabilities by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Critical Asset

For instructions about how to schedule reports, see [“Archiving Reports” on page 294](#).

Tuning ArcSight Express Content

ArcSight Express content is designed to find activity of concern that the staff of your security operations center should be notified about so they can follow up. There may be times, however, that a situation is actually a benign or routine condition in your environment.

In such a case, ArcSight Express provides the following active lists where you can store specific event and user situations that are determined to be low or no risk:

- /All Active Lists/ArcSight System/Tuning/**Event-based Rule Exclusions**
- /All Active Lists/ArcSight System/Tuning/**User-based Rule Exclusions**

The entries in these active lists are ignored by the rules that reference them. The *Event-based Rule Exclusions* active list is referenced by the event-based rules, and the *User-based Rule Exclusions* are referenced by the user-based rules:

Event-Based Rules	User-Based Rules
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ High Number of IDS Alerts for DoS	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Logout
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ SYN Flood Detected by IDS and Firewall	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Login
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/ High Number of IDS Alerts for Backdoor	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/ Multiple Windows Logins by Same User

These active lists store the following fields for the events and users:

Event-based Rule Exclusions	User-based Rule Exclusions
The following fields limit the rule exclusions to very specific events between two specific systems. <ul style="list-style-type: none"> • Device Event Class ID • Event Name • Attacker Zone Name • Attacker Address • Target Zone Name • Target Address 	The following fields limit the rule exclusions to user account activity that can be safely ignored. <ul style="list-style-type: none"> • Target NT Domain • Target User ID • Target User Name

There are three ways to add entries to these active lists:

- From an active channel
- Manually from the Active List editor
- In a batch from a CSV file

To add entries from an active channel:

- 1 In the active channel where the event appears, select and then right-click the event and select **Active List > Add to > Other...**
- 2 In the *Add to Active List* dialog box in the drop-down field, navigate to **/All Active Lists/ArcSight System/Tuning/Event-based Rule Exclusions** or **/All Active Lists/ArcSight System/Tuning/User-based Rule Exclusions** and click **OK**.
- 3 The *Add to Active List* dialog box will display the list of fields the active list will save from the selected event. If the selected event does not have a value for one or more of the fields, those fields will remain empty.

To add entries to these active lists manually:

- 1** In the Navigator panel, go to **Lists > Active Lists > All Active Lists > ArcSight System > Tuning**.
- 2** Right-click the active list you want to populate and select **Edit Active List**.
- 3** In the Active List Editor in the Inspect/Edit panel, click **Add Entry**.
- 4** In the ActiveList Entry Editor, enter the appropriate event or user details and click **Add**.
- 5** Repeat steps 3 and 4 for every event or user situation you want to exclude from the event or user-based rules.

To populate Active Lists from an imported CSV file:

- 1** In the Navigator panel, navigate to the active list you want to configure ([Lists > Active Lists](#)).
- 2** Generate a CSV file with the values with which you wish to populate the active list, and save it to a directory on the Console system.
- 3** Right-click the active list you wish to import the values into and select **Import CSV File...**
- 4** In the Open dialog box, navigate to and select the CSV file and click **Open**.

For more about working with active lists, see [“Managing Active Lists” on page 385](#).

Chapter 5

Learning Paths

ArcSight ESM involves many different security functions, as presented through the ESM Console. Some of these functions are subjects of a certification process under various standards specified in the Common Criteria for Information Technology Security.

These topics are provided as a guide to help you locate and understand the ESM security functions related to certification. The User category applies to persons who, after logging in, would have only basic access to the system. The Author category applies to persons with analytic authoring privileges. The Administrator category applies to persons with both administrative and analytic authoring privileges in addition to basic access.

Table 5-1 Roles Mapped to Related Topics and Tasks

ArcSight ESM Roles	Topics and Tasks
Administrator	<p>ArcSight Administration: See Chapter 20, Managing Resources (for Administrators), on page 437.</p> <ul style="list-style-type: none">• Manages ArcSight groups and users creating, editing, and deleting• user accounts, creating access control lists, and setting permissions• Establishes escalation procedures for automated notifications sent by e-mail, pager or cell phone

ArcSight ESM Roles	Topics and Tasks
Author	<p>Analysis Authoring: See “Rules Authoring” on page 301, “Identity Correlation” on page 357, “List Authoring” on page 385, “Case Management and Queries” on page 397, “Knowledge Base Authoring” on page 433, and topics on creating and editing dashboards and data monitors in “Monitoring Events” on page 91. See also, reference topics on “Categories” on page 606, “Common Conditions Editor” on page 616, “Data Fields” on page 633, and “Prioritization Fields” on page 736.</p> <ul style="list-style-type: none">• Creates rules that are cross-correlated with incoming events to automatically generate responses with automated actions• Creates and generates custom reports that are viewed by Operators to summarize enterprise security activity or display detailed information on particular devices, events, or users• Creates cases that are used by Operators as a tracking system to monitor specific suspicious events or situations that occur in the enterprise• Creates Knowledge Base content that provides Operators with solutions and possible actions to security threats• Customizes Views that are used by Operators to capture enterprise network infrastructure displaying real-time events
Operator	<p>Analysis Operations: See “Monitoring Events” on page 91, “Filtering Events” on page 147, “Building Reports” on page 205, “Running and Managing Reports” on page 287.</p> <ul style="list-style-type: none">• Monitors, investigates, and analyzes events using Views, Event Inspector, Replay Controls, and other monitoring tools• Acknowledges notifications and responds to security threats• Views reports, cases, and Knowledge Base articles in order to proactively approach security issues

[“For the User” on page 53](#)
[“For the Administrator” on page 53](#)

For the User

ESM users with an interest in certification issues can use the following subject matter list as a guide to relevant documentation topics.

ArcSight ESM User Certification Subjects

Active Channels

- [“Monitoring Active Channels” on page 91](#)
- Reference topic: [“Active Channels” on page 572](#)
- Related topic: [“Viewing and Using Channels” on page 92](#).

Login Process

- Reference topic: [“Access Control Lists” on page 571](#)
- Related topics: [“Filters” on page 724](#), [“Users” on page 783](#), and [“User Groups” on page 782](#).

For the Administrator

ArcSight ESM users with administrative privileges and an interest in certification issues can use the following subject matter list as a guide to relevant documentation topics. See also, [Chapter 20, Managing Resources \(for Administrators\), on page 437](#).

ArcSight Administrative Certification Subjects

Access Control Lists (ACLs)

- Reference topic: [“Access Control Lists” on page 571](#)
- Related topics: [“Filters” on page 724](#), [“Users” on page 783](#), and [“User Groups” on page 782](#).

Active List Resources

- Reference topic: [“Active Lists” on page 574](#)
- Related topics: [“Rule Actions” on page 751](#) and [“Creating Filters” on page 147](#).

Dashboards

- Reference topic: [“Dashboards” on page 630](#)
- Related topics: [“Data Monitors” on page 692](#), [“Using Dashboards” on page 113](#), and [“Viewing and Using Channels” on page 92](#).

Data Monitor Resources (statistical)

- Reference topic: [“Data Monitors” on page 692](#)
- Related topics: [“Dashboards” on page 630](#), [“Data Monitor Types” on page 692](#), and [“Viewing and Using Channels” on page 92](#).

Database Full Response

- Reference topic: [“Database” on page 631](#)
- Related topics: [“Data Fields” on page 633](#), [“SmartConnectors” on page 762](#), and [“Sending Control Commands to SmartConnectors” on page 517](#).

Filters

- Reference topic: [“Filters” on page 724](#)

- Related topics: [“Using Grids” on page 105](#), [“Creating Filters” on page 147](#), and [“Applying Filters” on page 155](#).

Firewalls, Ports, Switchover Database Cable, Security Domain

Information on these topics is provided in a separate Security Domain document.

Reports

- Reference topic: [“Reports” on page 742](#)
- Related topics: [Chapter 11, Building Reports, on page 205](#), [“Understanding Reporting Workflow” on page 205](#), [“Using Report Templates” on page 209](#), [“Building Queries” on page 228](#), [“Building Trends” on page 241](#), [“Creating Reports” on page 251](#), [“End-to-End Reporting Examples” on page 272](#), and [Chapter 12, Running and Managing Reports, on page 287](#).

Resource Editors

The ArcSight ESM Console offers one or more specialized editors for each resource or significant resource component. Consequently, there are many usage descriptions to support these editors, and numerous related informational topics. Since listing these topics would in effect reiterate a large part of the Console's documentation, the more practical guidance is to summarize the resource groups and allow the reader to explore resource editing from that perspective.

- Navigating
- Help system file: `helpgu18.htm`
- Help topic: Navigating

Resources

As with Resource Editors, the direct and relevant supporting topics for security analysis resources constitutes most of the Console's documentation. Again, the more practical guidance is to summarize the resources being documented and allow the reader to explore further from that perspective

- [“Navigating” on page 58](#)
- Reference topic: [“Navigator Panel” on page 729](#)

Rules

- Reference topic: [“Rules” on page 753](#)
- Related topics: [Chapter 13, Rules Authoring, on page 301](#), [“Rule Actions” on page 751](#), [“Rule Conditions” on page 752](#), and [“Rules Editor” on page 756](#).

Rule Actions

- [“Rule Actions” on page 751](#)
- Reference topic: [“Rule Actions” on page 751](#)
- Related topics: [Chapter 13, Rules Authoring, on page 301](#), [“Rule Actions” on page 751](#), [“Rule Conditions” on page 752](#), and [“Rules Editor” on page 756](#).

Shell Commands

Documentation for using operating system shell commands (command line commands) is included in the appropriate appendixes of the ArcSight ESM Administrator's Guide.

Secure Sockets Layer (SSL) Communications Encryption

- Secure Sockets Layer
- Reference topic: Secure Sockets Layer

Threat Level Formula

- Reference topics: ["Threat Evaluation" on page 777](#)
- Related topics: ["Priority Calculations and Ratings" on page 737](#), ["Prioritization Fields" on page 736](#), and ["Threat" on page 777](#).

User Groups (Administrator, Author, Operator)

- Reference topic: ["User Groups" on page 782](#)
- Related topic: ["Users" on page 783](#).

Users

- Reference topic: ["Users" on page 783](#)
- Related topic: ["User Groups" on page 782](#).

Working in the Console

In addition to all the security analysis, forensic, response, and reporting capabilities built into the ArcSight Console, the Console itself is a tool with its own characteristics and specialized controls. The Help topics in this section describe the basics of using Console tools and controls to make the most of its features.

[“Navigating” on page 58](#)

[“Viewing” on page 63](#)

[“Inspecting and Editing” on page 66](#)

[“Controlling the Console” on page 70](#)

[“Using the Network Tools” on page 72](#)

[“Staying Informed” on page 75](#)

[“Using the Menus” on page 77](#)

[“Keyboard Shortcuts \(Hot Keys\)” on page 82](#)

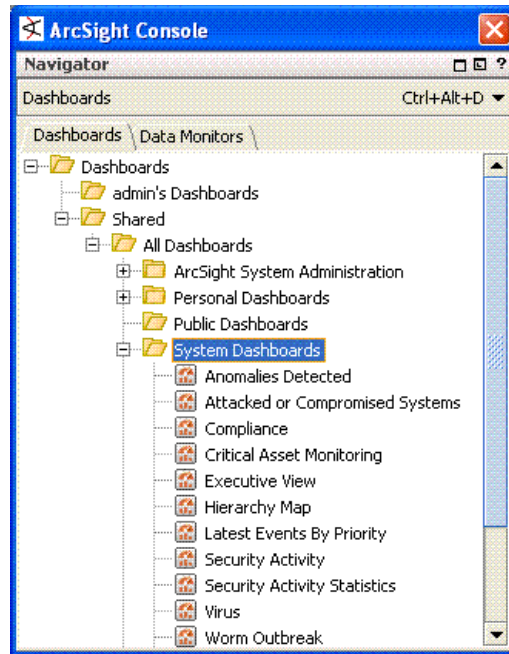
[“Moving Copying, Linking, and Deleting Resources” on page 83](#)

[“Printing from the Console” on page 83](#)

Navigating

The primary principle of navigating in the ArcSight Console is to use the Navigator panel to locate and manage security resources, and the Viewer and Inspect/Edit panels to analyze resource data and view or adjust the attributes of the resources producing the data.

Figure 6-1 The Navigator panel showing the Dashboards resource tree













Using the Navigator panel consists of:











- Choosing a resource tree from the drop-down list.
- Expanding (+) and collapsing (-) resource groups to locate particular subgroups or individual resources. (You can also use the keyboard **right arrow key to expand** and **left arrow key to collapse** the **Navigator resource trees**.)
- Right-clicking groups or individual resources to choose from their context menus.
- Using the Viewer or Inspect/Edit panels to see or act on the results of the context menu commands.

The resources available to you in the Navigator panel can be affected by your user type.

As a suggestion, browsing the resource trees established for your enterprise is a very good way to become familiar with both your environment and the ArcSight Console's capabilities.

Navigator Panel Resource Tree

Tree	Icon	Resource
Active Channels		Create, modify, and delete security-event views that actively and continuously evaluate the events they display, on the basis of time and other filter conditions. This view also includes the Field Sets resource tree for managing named field sets. See Chapter 7, Monitoring Events, on page 91 .
Assets		Security-sensitive devices and device groups installed in your enterprise, and the known exposures to potential threats those devices may represent. Assets also includes the related network, zone, location, category, and vulnerability information you use to manage network devices. See Chapter 20, Modeling Your Network and Managing Assets, on page 456 .
Cases		Enterprise security incident cases, by status and priority. See Chapter 17, Case Management and Queries, on page 397 .
Connectors		The SmartConnectors currently installed at your enterprise. See "Managing SmartConnectors" on page 498 .
Customers		Manage resources that represent the security concerns of particular MSSP (Managed Security Services Provider) clients. See "Managing Customers" on page 551 .
Dashboards		Various event data monitors and their containing dashboards. See "Using Dashboards" on page 113 .
Files		The Files resource tree, when populated, lists files saved as resources on the Manager. This makes them accessible to all users of the system who are authorized for such access. File resources include Case file attachments, templates, and general-purpose shared files. See "Managing File Resources" on page 488 .
Filters		Event filtering definitions, organized in groups. See Chapter 9, Filtering Events, on page 147 and "Managing Filters" on page 480 .
Knowledge Base		A database of articles and groups of articles that aid problem-solving, analysis, and operation. See "Getting Knowledge Base Articles" on page 146 and Chapter 19, Knowledge Base Authoring, on page 433 .
Integrations		Application integration resources used to configure and launch commands, tools, and views in custom and third party applications and other ArcSight products from within the ESM Console. Provides the ability to configure custom scripts, URLs, and CounterACT SmartConnector commands, and integrate them into the Console UI in various contexts. Leverages velocity expressions and the UI contexts for pulling the content of event data, for example, as command parameter values. Provides support for ArcSight Network Synergy Platform (NSP) and Threat Response Manager (TRM). See Chapter 18, Integration Commands, on page 405 .

Tree	Icon	Resource
Lists		<p>Active Lists are lists of active source and target IP addresses of interest, as defined by enterprise rules. See “Managing Active Lists” on page 385 for more information.</p> <p>Session Lists are similar to active lists, but are optimized for time-based queries and monitoring of rule-driven combinations of event attributes or custom fields. See Chapter 15, Identity Correlation, on page 357 for more information.</p>
Notifications		Destinations and settings for the automatic messages that alert you to pre-defined situations or events. See “Using Notifications” on page 76 and “Managing Notifications” on page 482 .
Partitions		ArcSight Database archiving management. See “Managing Partitions” on page 547 .
Pattern Discovery		Profiles to capture, and snapshots of, potentially threatening event patterns. See “Pattern Discovery” on page 127 .
Query Viewers		A resource for defining and running SQL queries on other ESM resources (independent of reports), including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results. Query viewers can use the same queries as reports do, but can be run independently of them. See Chapter 10, Query Viewers, on page 161 .
Reports		Definitions for, and archived output from, various activity reports. See Chapter 12, Running and Managing Reports, on page 287 and Chapter 11, Building Reports, on page 205 .
Rules		Rules, and groups of rules, created for isolating, analyzing, and responding to events. See Chapter 13, Rules Authoring, on page 301 .
Stages		Workflow and annotation features for real-time analyst collaboration on security events.
Use Cases		ArcSight ESM resource collections that address common security issues and business requirements. When use cases are installed, a Use Case tab is displayed in the Navigator panel. A wizard is available to automate configuration of the resources involved in the use case. The wizard steps through questions on event sources to use, data sets to populate active lists, reports preferences, notifications, and so forth, then configures the use case accordingly. See “Use Cases” on page 333 .
Users		ArcSight users and user groups. See “Managing Users” on page 438 .

Using SmartFolders

ArcSight has special, automatically maintained folders to track the results of your case searches or to track your currently selected replay rules and currently running reports.

When you create them, these folders appear just below the root of each resource type in the Navigator, prefixed with your ArcSight user name.

Creating a Case-Search SmartFolder

To create a case-search SmartFolder:

- 1 Right-click a folder in the Cases tree and choose **New Search Group** in the context menu to open the Search Group Editor.
- 2 Use the Editor to define a search that updates dynamically (runs automatically) each time a change occurs to one of your cases.

A given group contains the result of this search when it is applied to those cases.

Creating a Reports SmartFolder

The Reports tree in the Navigator panel now shows each user a folder with their user name and the suffix "Reports." In this folder the Console automatically lists all the reports that user is applying, and the right-click context menu offers the commands available for those reports. This folder is maintained automatically and not subject to change by the user.

You can use this feature to conveniently control report runs. For example, if a report is running too long and you would like to end it, right-click it and choose **Stop Report**.



Reports you run using the **Run** button in the Report Editor are initiated outside the usual Console processes and do not appear in, and are not controllable from, the Reports tree in the Navigator.

Editing Groups

All resource types in the Navigator panel can be grouped to assist in organizing and managing them. Groups can also be hierarchical, resulting in "trees" of resources. Apart from the characteristics of the resources involved, such as assets or vulnerabilities, each group identity has certain properties you can edit in the Group Editor.

Editing a Group

To edit a group:

- 1 In the Navigator panel, right-click a resource group and choose **Edit Group**.
- 2 In the Group Editor, click the **Value** fields for the group attributes you want to change.
- 3 Click **Apply** to put your changes into effect but leave the editor open. Click **OK** to apply your changes and also close the editor.

Note that fields containing system information (like Creation Time) are not subject to editing.

See ["Reference Pages" on page 742](#) for more about using the **Group Page** and **Member's Page** fields.

See ["Scheduling Jobs" on page 756](#) for information about scheduling tasks or "jobs" for reports (individually or by group), rules, or pattern discovery snapshots.

Categories Tab

The Group Editor for groups in the Assets tab of the Assets resource tree has an additional Categories tab. This Categories tab has two subpanels: Local Asset Categories and Inherited Asset Categories. "Local" shows assets that are explicitly assigned to categories.

"Inherited" shows assets whose category connections are presumptions based on a parent's group or a simple asset-range association.

Viewing Group Cases in a Grid View

When you right-click a case group in the Cases resource tree in the Navigator panel, and choose **View in Grid**, you see that group's cases listed in a Case Details view in the Viewer panel. Click any case in the grid to work with it individually. You can also:

- Right-click any column heading to get a menu of column configuration options.
- Right-click any individual case's fields to get a menu of case handling options, described below.

Table 6-1 Case Grid Right-click Menu Options

Option	Description
New	Create a new case.
Edit	Open a case in the Inspect/Edit panel for editing.
Delete	Delete the selected case.
Export to external system	Export the case to an external tracking system.
Edit case by ID	Find a case by its Display ID value.
Select rows with matching cell	Select cases where all values in a particular column have the same value or entry.
Invert selection	Reverse selection and highlighting of a previous selected group of cases.
Close	Clear the Case Details view.
Refresh	Refresh the Case Details view to reflect new or deleted cases and information updated in existing cases.
Knowledge Base	Show Knowledge Base information associated with cases.

Batch Editing

You can make common edits to multiple case or SmartConnector resources by selecting a set of either type in the Navigator panel and changing their common fields in the Case or Connector Editor.

Batch-Editing Cases or Connectors

To batch-edit cases or connectors:

- 1 **Ctrl+click** or **Shift+click** to select a set of individual cases or SmartConnectors in their respective resource trees in the Navigator panel.
- 2 **Right-click** the selected items and choose **Edit**.
- 3 Make changes to the appropriate common fields, such as **Description** or **Owner**.
- 4 Click **Apply** to record your changes and leave the editor open, or click **OK** to save and close. Saving affects only the fields you have changed, in each of the selected resources.

Cases Reminder

You can also lock and unlock cases in batches, using the **Lock Case** check box.

SmartConnector Reminders

Batch changes affect only default configurations, not alternates. However, you can add new alternate configurations by batch editing.

Note that if you make changes under the **Filters** tab, the entire tab's contents are saved to the selected SmartConnectors.

Only connectors of the same version can be batch-edited. Version is indicated by the color of the connector icons in the resource tree: blue for pre-v2.5 and green for v2.5 or later.

Reconnecting to the Manager

If your ArcSight Console loses its connection to the ArcSight Manager, a dialog box will offer you the option to **Retry** the connection, **Relogin** to log in again, or to **Cancel** the connection attempt. You should attempt to use these options in this order.

An existing connection to the ArcSight Manager can't be re-established when the ArcSight Manager has to be restarted or when a network problem prevents communication with the same Manager. In such cases you need to click **Cancel** and start the Console again, using an appropriate ArcSight Manager host name.

Viewing

Topics in this section provide information on using the Console "Viewer Panel" and choosing "look-and-feel" options (skins) for the Console.

Viewer Panel

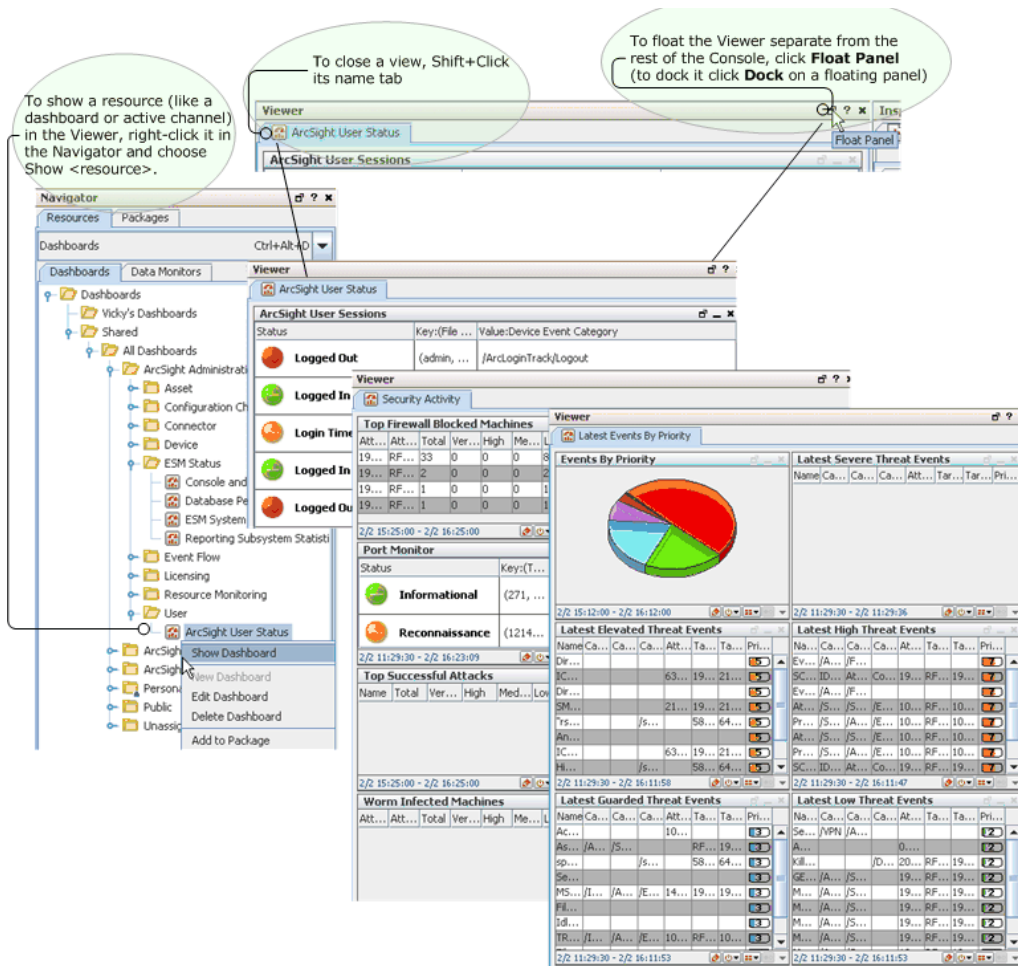
You see the products of security-event analyses in the Viewer panel, which can display several different types of views. (See also, ["Using Views" on page 91.](#))

Although there are some views that display information about resources, most views are active channels, which are continuously evaluated collections of security-event data. (See also, ["Monitoring Active Channels" on page 91.](#))



Tips:

- To show a resource (like a particular dashboard or active channels) in the viewer, right-click it in the Navigator tree and choose Show <resource>.
- To close individual views quickly, Shift+Click their name tabs. (You can also right-click a view name tab and choose Close from the popup menu.)
- To float the Viewer panel, click the Float icon at the top left of the Viewer.



The Viewer panel can also internally render basic HTML, meaning that it automatically shows HTML-based reports, reference pages, results for the Web Search tool, and notification acknowledgements. More complex HTML that might include JavaScript, plugins, or other embedded objects is, for security reasons, still rendered in the external browser you specify through the Preferences dialog box. The external browser is also used by PDF document files.

The **Web Viewer** tabs in the Viewer panel have a live link at the top. You can click these links to open the contents in an external, fully functional browser window. You can also right-click the contents of a Web Viewer and use the standard browser commands to do basic functions such as going back or forward or reloading.

If your Console is not already displaying a default set of pre-defined views, or you want to change the views displayed, you can use these options:

- Choose **Window>Viewer Panel** to open the panel if it isn't open.
- Choose the **Active Channels**, **Dashboards**, or **Pattern Discovery** resource trees in the Navigator panel to find analysis tools or results to view.
- Right-click a resource in a tree and choose **Show <resource>** to open it in the Viewer panel.

- When multiple tabbed views are open in the panel, click the tabs at the **top** of the panel to choose the active channel you want to see, and the tabs at the **bottom** of the panel to choose which view of that active channel should be foremost.

To close an individual view, **Shift+click** its name tab. (You can also right-click a view name tab and choose **Close** from the popup menu.)

Using active channels and the many types of views they offer is fully covered in the topics under these headings:

- Monitoring Events
- Selecting and Investigating Events
- Using Dashboards

Console Look-and-Feel

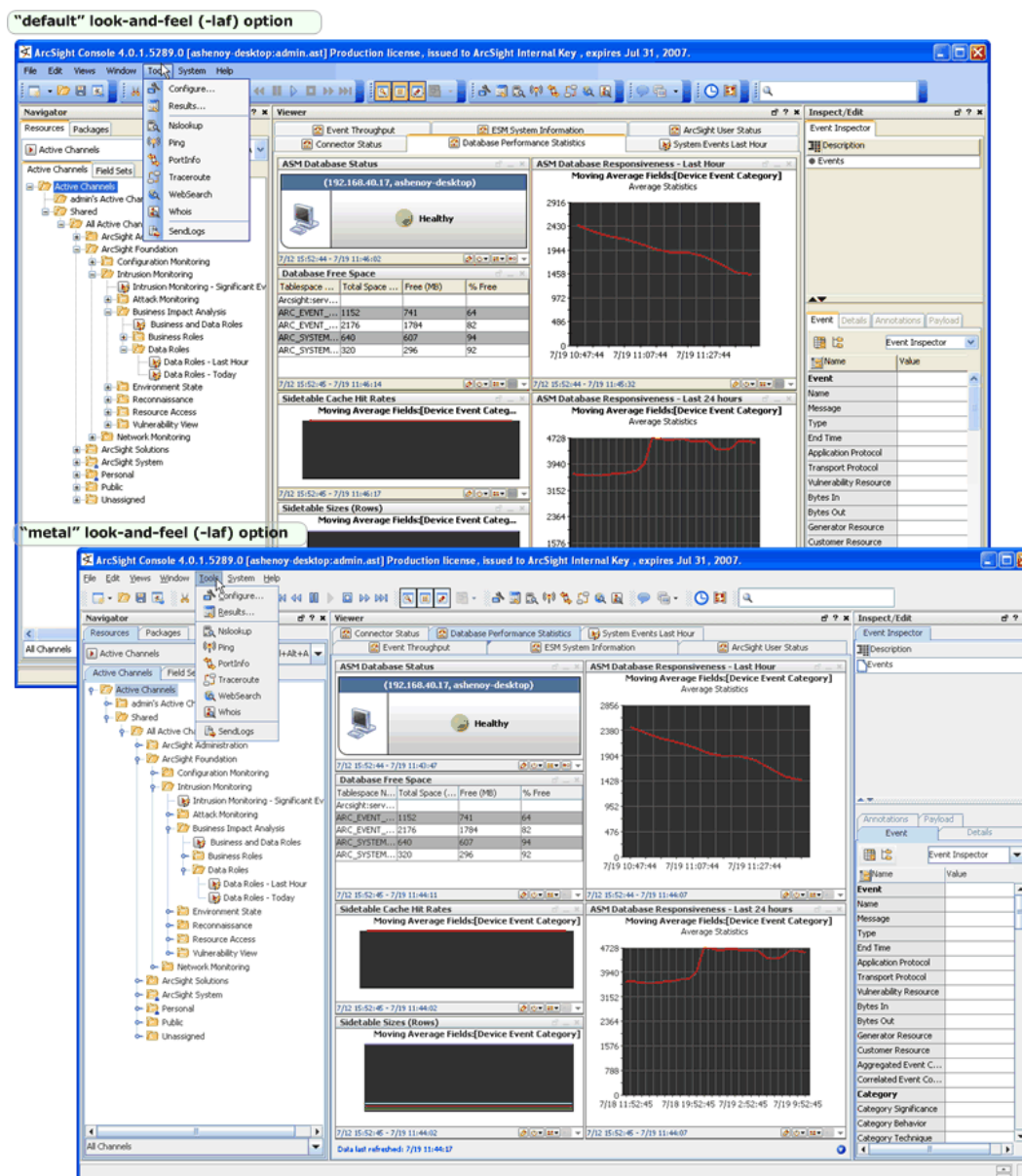
If you start the Console from the command line with the **arcsight console** command (in [ARCSIGHT_HOME/current/bin](#)), you can use the **-laf <style>** flag to specify a look-and-feel style. For example, the following command starts the Console with a "metal" look-and-feel:

```
arcsight console -laf metal
```

The different look-and-feel styles modify the colors and styles of the Console display and associated Online Help. The following styles are available:

- metal
- plastic
- plastic3d

If you do not specify a look-and-feel style, a default style is used. The figure below shows examples of what a Console looks like when started with the default and metal styles.



The screen snaps and illustrations used throughout the Console Online Help show various look-and-feel styles. For more information about **arcsight console** command options, including **-laf**, see the "ArcSight Commands" appendix in the ArcSight ESM Administrator's Guide.

Inspecting and Editing

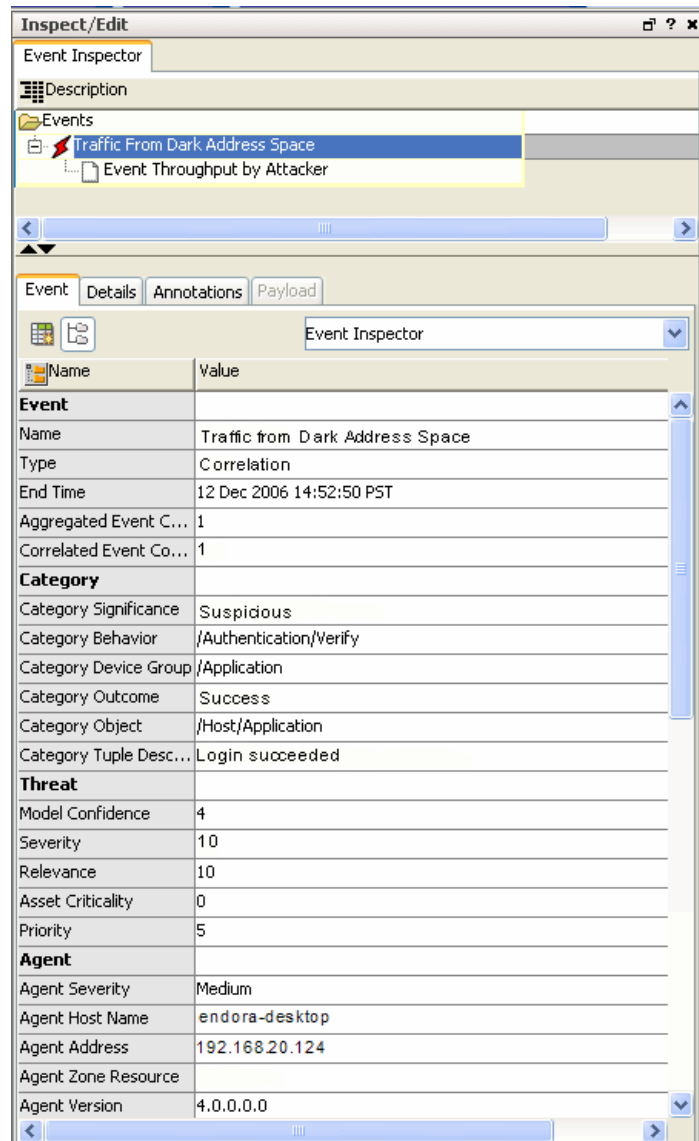
You use the Inspect/Edit panel to examine the details of events that appear in active channels in the Viewer panel, or to modify the attributes of resources you find in the Navigator panel.

You examine security events through the Inspect/Edit panel's Event Inspector, and handle resources through many specialized editors, one for each specific resource type.

See also: [“Hiding Empty Rows in the Event Inspector” on page 141](#), [“Displaying Articles from the Event Inspector” on page 146](#), [“Retrieving Payloads” on page 145](#), and [“Event Inspector” on page 721](#).




Overview of Inspect/Edit Features and Utilities

Each editor has its own particular controls and attributes that are described in the Help topics connected with its resource.



You don't usually need to open the Inspect/Edit panel manually. It opens automatically when you double-click an event in a grid view or choose to edit a resource in the Navigator panel. Another way to get this display is to right-click on an event in a grid view and choose **Show Event Details**. If you want to explore the Inspect/Edit panel, you can:

- Choose **Window>Inspect/Edit Panel** to open or restore the panel, if it already has inspectors or editors in it. If no inspectors or editors are currently open, the panel isn't available.

- When there are no editors or inspectors open, or you want to work with different ones, double-click an event in a grid view or right-click an item in a Navigator panel resource tree and choose **Show <resource>**.
- When you want to clear some editors out of the Inspect/Edit panel, right-click each one's tab and choose **Close**.
- Click the **Hide Empty Rows** button () beside the **Select a Field Set** menu to see only populated fields.
- Click the New Field Set button () to create a new field set.
- Click the icon toggle button () to show/hide icons next to each field entry.

Searching for Fields in Event Inspector, Resource Editors or CCE

To find an item in a list of fields on the Event Inspector, any Resource Editor, or the [Common Conditions Editor](#) (CCE), click on any field Name (on the left side of the field list) and start typing. A Search popup is displayed when you start typing, and shows the term as you type it. The search is "predictive" in that it will navigate to and select matching fields as you type. The Search utility works essentially the same way in the Event Inspector and in resource editors that use field sets and filters (and, by association, the CCE).

To search for a field, select any entry in the Field "Name" side of the Event Inspector and start typing.

The **Search for:** popup field is displayed and navigates to matching items as you type a search term.

The screenshot shows the 'Event Inspector' window with tabs for 'Event', 'Details', 'Annotations', and 'Payload'. The 'Event' tab is active. A search bar labeled 'Search for: Event' is at the top. Below it is a table with two columns: 'Name' and 'Value'.

Name	Value
Event ID	30000147689
Name	ScheduledTask updated
Type	Base
Start Time	12 Dec 2006 16:15:03 PST
End Time	12 Dec 2006 16:15:03 PST

The popup Search on fields is available in all resource editors with Field tabs. To activate the Search, select the any field in the list and start typing.

The screenshot shows the 'Inspect/Edit' window with tabs for 'Event Inspector', 'Report:test', and 'Query:Attacker Counts by Agent...'. The 'Fields' tab is active. The 'Query Structure' section shows a SQL query:

```
SELECT
  Agent Type
  Attacker Zone URI
  Attacker Address
  Count COUNT
ORDER BY
  Agent Type ASC
```

The 'Data Options' section has tabs for 'Select', 'Order By', and 'Group By'. The 'Select' tab is active. A search bar labeled 'Search for: End' is at the top. Below it is a list of fields with checkboxes:

- ☐ Aggregated Event Count
- ☐ Application Protocol
- ☐ Bytes In
- ☐ Bytes Out
- ☐ Concentrator Agents
- ☐ Concentrator Devices
- ☐ Correlated Event Count
- ☐ Crypto Signature
- ☐ Customer
- ☐ Customer External ID
- ☐ Customer ID
- ☐ Customer Name
- ☐ Customer Resource
- ☐ Customer URI
- ☒ End Time
- ☐ Event ID
- ☐ External ID
- ☐ Generator

The 'Query Columns' section shows a list of columns:

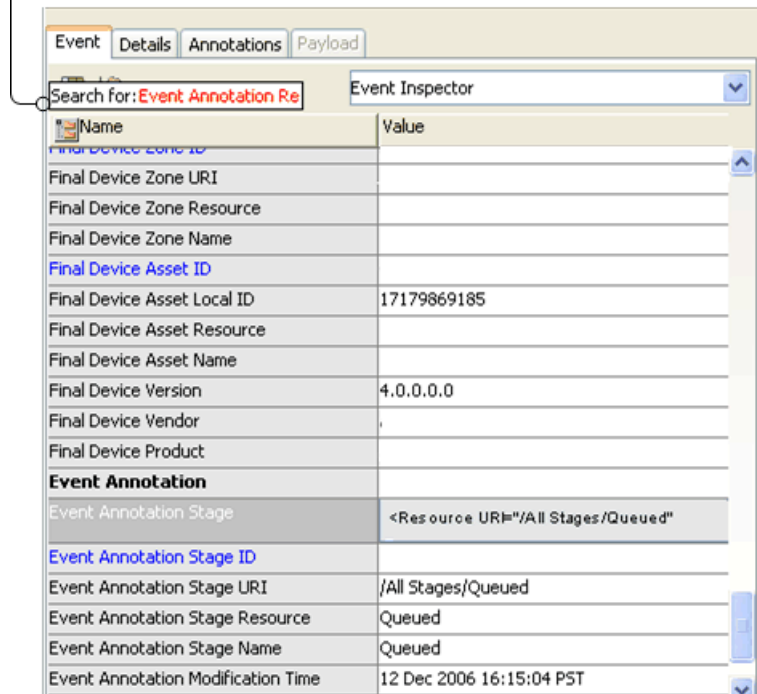
- Agent Type
- Attacker Zone URI
- Attacker Address
- Event ID COUNT

The 'Column Function' section shows a dropdown menu with 'None' selected and a checkbox for 'Unique'.

If you start to type a term that is not in the field list, the Search popup text turns red. If you backspace out, the popup text will change from red to black when a matching field is found. Resume typing to find another matching term.

Predictive search updates as you type. If you start typing a term that is not in the list, your entry is highlighted in red.

You can backspace to erase letters in your search term. Your entry will show up in black again when it finds a match, and the Search utility will continue to jump to the first matching entry as you re-type.



To exit the Search, hit the **Return** key.

To start a new Search, click into any entry in the "Name" list on the left side of the list again.

Getting More Help

The best way to learn more about the Event Inspector and each of the many resource editors is to click the question mark button (?) in the upper-right corner of the







Inspect/Edit panel or **Help** button () in the lower right of a resource editor.

Controlling the Console

The ArcSight Console has certain common controls that you might use at any time to do basic tasks like copying and pasting, and showing or hiding panels or the status bar.

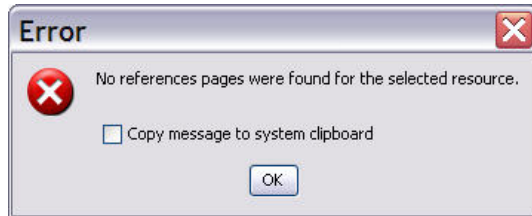
The controls you may find yourself using most often are the toolbar buttons. There are four toolbars under the menus at the top of the Console. Each button has an identifying tooltip, but the full descriptions are as follows.

To show or hide toolbar components, right-click the toolbar and select or deselect the sections you want to change.

Tree	Icons	Resource
Standard application functions		The Save , Open , Cut , Copy , and Paste buttons operate as they do in any application. Saving and opening applies to ArcSight Console settings (.ast) files. Cutting, copying, and pasting applies to text and resources. (There is also a File > Save to Manager option available from the menus.)
Show or hide UI elements		Click the Show/Hide buttons to open/close the Navigator, Viewer, and Inspect/Edit panels and status or menu bars. Click the Floating button to bring floating windows forward.
Replay controls		The Replay buttons have essentially the same functions in certain views in the Viewer panel as their counterparts do on VCRs or CD players. From left to right, the buttons are: Rewind to Start , Rewind Incrementally , Pause , Play , Stop , Go Forward Incrementally , and Go Forward to End . You use the Replay buttons when working with channels configured for this mode.
Network tools		These buttons run standard IP-based network analysis tools as described in “Using the Network Tools” on page 72 .
Notifications		The Acknowledge Notifications button in the toolbar line tells you when you have messages to acknowledge. Click the button to open the Notifications manager in the Viewer panel so you can acknowledge the notification and resolve the issue.
Status Bar		<p>You can show or hide the status bar at the bottom of the Console window with this toolbar button, or use the Window>Status Bar menu command. When the status bar is showing, it displays specific Console operation messages. Normal status messages appear in blue and error messages are red.</p> <p>To view details on a message, click the message in the status bar. The ArcSight Messages dialog is displayed with the current message highlighted. From this dialog, you can access console messages, system messages and user notifications.</p> <p>To copy any message from the Messages dialog, highlight it and click Copy. The message is copied to the clipboard along with associated date and time. You can then paste the message into any other window, mail program, or editor that accepts ASCII text.</p>
Menu Bar		You use the menus in the menu bar as described in “Using the Menus” on page 77 .

Error and Warning Messages

Certain error messages, warnings, and notifications may be displayed in a small dialog. These messages often contain specific information. To capture the error message and supporting data, click the Copy button or check Copy message to system clipboard to copy the entire message to the Clipboard. You can then paste the error message in text fields in the ArcSight Console, into the body of an e-mail message, or other applications.



Using the Network Tools

The network tools are the rightmost set of buttons on the toolbar and are also available from the Tools menu. ArcSight provides **Ping**, **Traceroute**, **Nslookup**, **PortInfo**, **Whois**, **WebSearch**, and **SendLogs** as default utilities. Most of these tools are utilities you use to investigate events in grid views. In a grid view, you right-click an event to access these tools from a context menu. A new wizard-based utility called **SendLogs** gathers logs and diagnostic information for in-house review or sending to ArcSight.

You can add, copy, edit, or delete network tools using the Tools menu in the menu bar. The toolbar buttons and menu commands adjust automatically to such changes.



As of ESM v.4.5, the Network Tools are also available as *integration commands* (see [“Network Tools as Integration Commands” on page 431 in Integration Commands](#)).

For this release, these tools are available in both places on the Console UI, but for future releases the legacy “network tools” feature described here will be phased out in favor of the integrations commands. The same, customizable tools and commands will be available (**ping**, **whois**, and so on), along with other new commands and a full set of application integration features.

For ESM v.4.5, the legacy network tools are available for use through right-click menus in various contexts as before, by choosing **Tools > <Command>**.








To configure these tools, choose menu option **Tools > Local Commands > Configure**, as described in the following topics.

Running a Tools Command

To run a tools command:

- 1 In a grid view, select an IP address.
- 2 Right-click and select **Tools**, then one of the tool options described below.
- 3 Based on the tool selected, a window appears with the information.
- 4 In the window, click **Close**.

Network Tool Default Options

Tree	Icon	Resource
Nslookup		Resolves an IP address to a host or domain name or vice versa.
Ping		Determines whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response.
PortInfo		Lists standard usage, for example, WWW, FTP, and so on for a specified port number.
Traceroute		Shows the path from the ArcSight Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between.
WebSearch		Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells.
Whois		Looks up who is behind a given domain name; information might include addresses and telephone numbers.
SendLogs		Starts the Send Logs wizard to gather logs and diagnostic information and, optionally, sends them to ArcSight. Logs and diagnostics can be collected for all or a selected set of ArcSight components. (See “Send Logs” on page 758.)

Adding a Tool

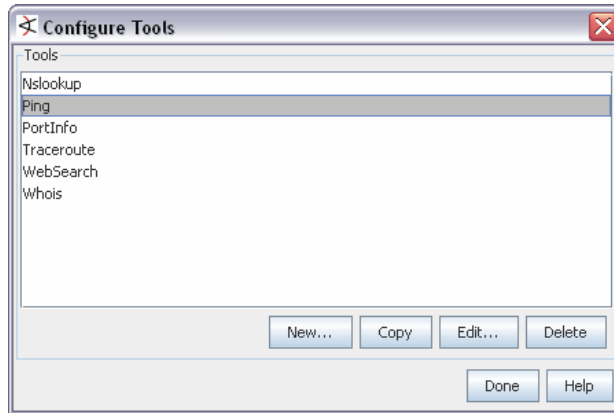
To add a tool:

- 1 Choose **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, click **New**.
- 3 In the Tool window, edit the Name, Program, Working Directory, Icon, and Program Parameters (command line parameters to be used for the program) text fields.
- 4 Click **OK**.
- 5 Click **Done**.

Configure (Edit) a Tool

To configure (edit) a tool:

- 1 Choose menu command **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, select an existing tool and click **Edit**.



- 3 In the Tool window, set these parameters and options:

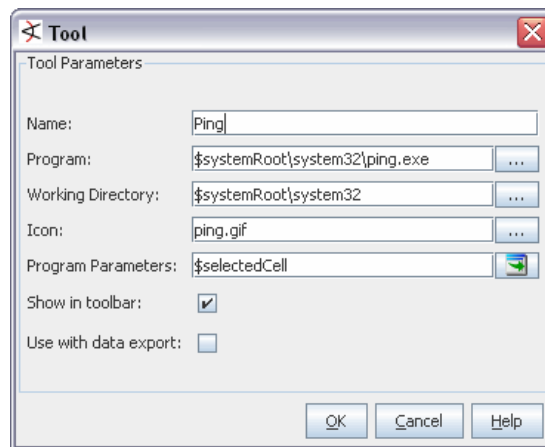



Table 6-2 Tool Configuration Parameters

Option	Description
Name	User-friendly name for this tool.
Program	Path to the executable file.
Working Directory	Default location assumed for arguments to the command. For example, to create a command (e.g., " delete <file>.ast") that acts on a file type that always resides in the same directory, specify the location here to save users from having to provide the full path to the file each time they use the command.
Icon	Path to the icon image file used to represent the tool.

Option	Description
Program Parameters	Provide any parameters needed for the command. You can type parameters in the field, or click the  button to get a pull-out menu where you can select Event Attributes to use as parameters, or add the "selected cell" or "selected row" as parameters to the command.
Show in toolbar	When "Show in toolbar" is on, the tool icon is shown in the Console toolbar. By default, this option is selected.
Use with data export	The purpose of this option is to separate tools that are run against events in channels and tools used as a destinations for event export. By default this option is not selected (off). If this tool is to be used as a destination for event export, select (checkmark) "Use with data export". If this tool contains a command that will run against events in a channel, leave "Use with data export" off.

- 4 **Name, Program, Working Directory, Icon, and Program Parameters** (command line parameters to be used for the program) text fields. Also select whether you want the tool to show in the toolbar
- 5 Click **OK**.
- 6 Click **Done**.

Deleting a Tool

To delete a tool:

- 1 Choose menu command **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, select an existing tool and click **Delete**.
- 3 In the dialog box, click **Yes**.
- 4 Click **Done**.

Staying Informed

In addition to the security-event information ArcSight collects and analyzes, you can get, record, and pass other types of working information. This additional information falls into these categories:

- **Notifications:** To be informed when certain defined events or circumstances occur. You might receive notifications by pager, or e-mail or similar means, but you can be sure to see an indicator in the **Notifications** button in the toolbar line of the Console.
- **Notes:** When you work with any ArcSight resource you use an editor in the Inspect/Edit panel and that editor will include a Notes tab in which you can record extra information about that resource. Cases are a good example of a resource that benefits from recording accumulated information.

Using Notifications

Using notifications means acknowledging them. Apart from acknowledging, you may need to take other action, but this will depend on the circumstances of the event.

Acknowledgements are described briefly here, but for full detail please see [“Managing Notifications” on page 482](#).

Acknowledging a Page

You can acknowledge a page by replying to it through your pager. All pagers must be configured to send replies. Your reply is sent to the pager service provider and then to ArcSight.

Acknowledge a Cell Phone Message

You can acknowledge a call by replying to the e-mail sent through your cell phone. You must have an e-mail enabled cell phone in order to receive notifications and reply to them.

Acknowledge an E-mail Message

You can acknowledge an e-mail by replying to the message. You must reply to the e-mail address that sent you the notification.

Acknowledge Notifications at the Console

The ArcSight Console automatically alerts you of pending acknowledgements. The **Acknowledge Notifications** button is automatically enabled when you have one or more notification messages that need to be acknowledged. When you click the **Acknowledge Notifications** button, the Notifications manager opens in the Viewer panel so you can acknowledge and resolve the notification.

Using Notes

Each individual resource and resource group in the trees of the Navigator panel has an editor, and each of these editors has a Notes tab. These Notes tabs retain all the text that you and other users add to the resource in the course of using it.

Notes tabs have Table and List sub-tabs to show you tabular or text layouts of the notes accumulated for a resource. Notes are stored chronologically and you can sort them by clicking the **Date**, **Owner**, and **Text** headers.

Adding a Note

To add a note:

- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose **Edit Group**. If it is a resource, choose **Edit <resource>**.
- 4 In the Inspect/Edit panel, click the editor's **Notes** tab.
- 5 In the Notes space, type a note.
- 6 Click **Save**.
- 7 Click **OK**.

Viewing a Note

To view a note:

- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose **Edit Group**. If it is a resource, choose **Edit <resource>**.
- 4 In the Inspect/Edit panel, click the editor's **Notes** tab.
- 5 Right-click a note and choose **View**.

Deleting a Note

To delete a note:






- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose Edit Group. If it is a resource, choose Edit <resource>
- 4 In the Inspect/Edit panel, click the editor's Notes tab.
- 5 Right-click a note and choose Delete.


Using the Menus

This section briefly describes the Console's menus and sub-menus.

File Menu








Keyboard shortcut **Alt+F** brings up the **File** menu. Keyboard shortcuts for File menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).

Option	Icon	Resource	Keyboard Shortcut
New		Create a new resource from the available submenu.	
Open		Open an existing Console settings file to use that configuration.	Ctrl-O
Save		Save your latest Console settings in the current configuration file.	Ctrl-S
Save As	None	Save your current Console settings in a different configuration file.	
Save to Manager		Save your current Console settings at the ArcSight Manager rather than locally, so you can get these settings at a different Console.	
Load From Manager		Load a preferred Console configuration file from the ArcSight Manager, so you can use it at this Console.	

Option	Icon	Resource	Keyboard Shortcut
Send To		Send a local Console configuration (.ast) file to an e-mail address so another user can save and use it at their Console.	
Log Out	None	Log out of the Console with your current user ID, without exiting, so someone else can log in.	
Exit	None	Log out of the Console and exit.	Alt-F4


Edit Menu





Keyboard shortcut **Alt+E** brings up the **Edit** menu. Keyboard shortcuts for Edit menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).

Option	Icon	Resource	Keyboard Shortcut
Cut		Cut selected text.	Ctrl-X
Copy		Copy selected text or resources.	Ctrl-C
Paste		Paste text or resources from the clipboard.	Ctrl-V
Delete		Delete selected text or resources.	Delete
Select All		Select all text.	Ctrl-A
Preferences		Open the Preferences dialog box to make personal configuration changes.	
Find Resource		Use the Find Resource query editor to search for resources and review their details.	Ctrl-F

View Menu





Keyboard shortcut **Alt+V** brings up the **View** menu. Keyboard shortcuts for View menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).


Option	Icon	Resource	Keyboard Shortcut
New Active Channel		Open the New Active Channel dialog box so you can set up and start a new active channel in the Viewer panel.	Ctrl+Shift-D

Option	Icon	Resource	Keyboard Shortcut
Show Active Channel		Open the Active Channel Selector dialog box so you can choose an active channel to display in the Viewer panel.	Ctrl+Shift-S
Recent Active Channels	None	Choose a recently opened active channel to display in the Viewer panel again, if available.	
New Dashboard		Create a new, untitled and empty dashboard to populate with data monitors.	Ctrl+Shift-B
Show Dashboard		Open the Load Dashboards dialog box so you can select dashboards to open in the Viewer panel.	Ctrl+Shift-W
Recent Dashboards		Choose a recently opened dashboard to display in the Viewer panel again, if available.	
Notification Acknowledgement		Shows all Notifications for the current user (pending, undeliverable, not acknowledged, acknowledged, and resolved)	Ctrl-N
Show Messages		Shows all console messages, system messages, and user notifications in the ArcSight Messages dialog.	Ctrl-M
Next View		Takes you to the next open view or tab in the Viewer.	Ctrl+Shift-N
Previous View		Takes you to the previous open view in the Viewer.	Ctrl+Shift-P
Close All Views	None	Close all views that are open in the Viewer panel.	

Window Menu









Keyboard shortcut **Alt+W** brings up the **Window** menu. Keyboard shortcuts for Window menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).

Option	Icon	Resource	Keyboard Shortcut
Navigator Panel		Show or hide the Navigator panel.	Ctrl-1
Viewer Panel		Show or hide the Viewer panel.	Ctrl-2
Inspect/Edit Panel		Show or hide the Inspect/Edit panel.	Ctrl-3
Status Bar		Show or hide the status bar.	Ctrl-4

Option	Icon	Resource	Keyboard Shortcut
Floating		Bring to the front one of the listed floating (undocked) windows, if available.	



Tools Menu

Keyboard shortcut **Alt+T** brings up the **Tools** menu. Keyboard shortcuts for Tools menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)”](#) on page 82.

Option	Sub-menu	Icon	Resource	Keyboard Shortcut
Local Commands	Configure		Add, copy, edit, or delete Network Tools.	Alt-C
	Results		Display the Tool Results dialog box.	Ctrl+Shift-R
	Nslookup		Resolve an IP address to a host name.	
	Ping		Determine whether an IP address is online.	
	PortInfo		List the default protocol usage for a specified port number (e.g., WWW, FTP, SMTP).	
	Traceroute		Show the path to an IP address.	
	WebSearch		Use Google to search the web for event-related keywords.	
	Whois		Find the registered owner of a given domain name.	
Network Model			Brings up the Network Model wizard. See “Populating the Network Model Using the Wizard” on page 459.	
Use Case			Brings up the Use Case wizard. See “Configuring Use Cases” on page 338.	
Send Logs			Brings up the Send Logs wizard. See “Send Logs” on page 758.	






System Menu

Keyboard shortcut **Alt+S** brings up the **System** menu. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).

Option	Icon	Resource
Scheduled Jobs		Open the Job Scheduler. For more information, see “Scheduling Jobs” on page 756 .
Categorize Event		Select a non ArcSight event in the grid, then select System > Categorize Event menu option to apply a category. For more information, see “Apply Standard Asset Categories to Assets” on page 16 and “Categories” on page 606 .

Help Menu

See also [“About this Guide” on page xxxv](#). Keyboard shortcut **Alt+H** brings up the **Help** menu. Keyboard shortcuts for Help menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 82](#).

Option	Icon	Resource	Keyboard Shortcut
Help Contents		Open the ArcSight Console Online Help. This is the Help system shown when you click a context-sensitive Help button in the Console. See “About this Guide” on page xxxv for details about using the Help, including navigating, printing, getting PDFs, and more.	F1
Browse ArcSight Documentation		Open an index page that offers pointers and links to other PDF-formatted documents concerning subjects such as SmartConnectors or upgrading.	
Knowledge Base		Switch to the Knowledge Base resource tree in the Navigator panel.	
ArcSight Support		Open a browser window that displays the ArcSight Support login page, so you can sign in and use the ArcSight Support Center's User Forum and other features.	
About		Show your ArcSight installation's legal notices and version information.	

Keyboard Shortcuts (Hot Keys)

You can accomplish many actions on the Console by using the default keyboard shortcuts or *hot keys*, instead of menus and mouse navigation. The standard keyboard shortcuts and their associated actions is listed in the table below. Keyboard shortcuts associated with menu options are included here and also shown in [“Using the Menus” on page 77](#).



You can view the default keyboard shortcut schemas and set up custom shortcuts on the Hot Key tab in the Console Preferences dialog (Console menu option **Edit > Preferences**, click **Manage Hot Keys**). For information on how to view or configure Console keyboard shortcuts, see [“Managing Hot Keys” on page 563 in Chapter 21, Personalizing the Console, on page 555](#).

Task	Keyboard Shortcut	Description
Annotate event (s)	Ctrl-T	Select one or more events in any grid view, and use Ctrl-T keyboard command (as an alternative to the right-click Annotate Events menu option). See “Annotating an Event” on page 142 .
Mark events reviewed	Ctrl-R	Select one or more events in any grid view, and use Ctrl-R keyboard command (as an alternative to right-click Mark as reviewed menu option). See “Collaborating on Events” on page 141 .
Copy	Ctrl-C	See “Edit Menu” on page 78
Cut	Ctrl-X	See “Edit Menu” on page 78
Delete	Delete key	See “Edit Menu” on page 78
Find	Ctrl-F	See “Edit Menu” on page 78
Open the Edit menu	Alt-E	See “Edit Menu” on page 78
Paste	Ctrl-V	See “Edit Menu” on page 78
Redo	Ctrl-Y	Re-do any text edit operation.
Select All	Ctrl-A	See “Edit Menu” on page 78
Undo	Ctrl-Z	Undo any text edit operation.
Exit/shut down the Console	Alt-F4	See “File Menu” on page 77
Open the File menu	Alt-F	See “File Menu” on page 77
Open the Edit menu	Alt-E	See “Edit Menu” on page 78
Open the View menu	Alt-V	See “View Menu” on page 78
Open the Window menu	Alt-W	See “Window Menu” on page 79
Open the Tools menu	Alt-T	See “Tools Menu” on page 80
Open the System menu	Alt-S	See “System Menu” on page 81
Open the Help menu	Alt-H	See “Help Menu” on page 81 and “About this Guide” on page xxxv .
Open the Help directly	F1	See See “Help Menu” on page 81 and “About this Guide” on page xxxv .

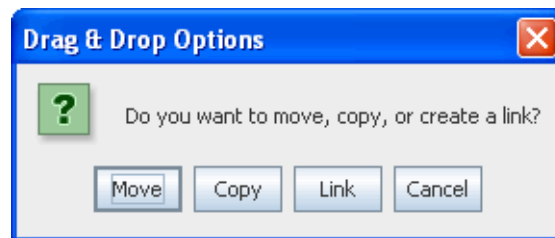
Moving Copying, Linking, and Deleting Resources

You may need to move or duplicate a resource to better organize your work or to make editable copies. You may also need to delete resource definitions you no longer need. These tasks are described here. For more information, see all topics in [Chapter 6, Working in the Console, on page 57](#).

Move, Copy, or Link a Resource

To move, copy, or link a resource:

- 1 Choose the resource type you want to work with in the Navigator (Active Channels, Filters, Rules, and so on).
- 2 Navigate to and select a resource instance in the tree, and drag and drop it into another group of the same resource type. The system displays a dialog that provides options to move, copy, or link the resource.



Select **Move** to move the resource, **Copy** to make a separate copy of it, or **Link** to create a copy of the resource that is linked to the original.

If you select **Copy**, you create a separate copy of the resource definition that will not be affected when the original is edited. If you select **Link**, you create a copy of the resource definition that is linked to the original. Therefore, if you edit a linked resource definition, whether it be the original or the copy, all links are edited as well. When deleting linked resource definitions, you can either delete only the selected one or the selected one and all linked copies.

Delete a Resource

To delete a resource:

- 1 Navigate to the resource type you want to work with.
- 2 Select a resource instance in the tree, right-click and choose **Delete <Resource>** from the context menu.

Printing from the Console

Starting with ArcSight ESM version 4.0, you can print Navigator trees for all resources. You can print resource definitions for rules, filters, and cases, as well as conditions from the [Common Conditions Editor](#) (for all resources with filters). You can print from all grid or channel views.



As you would expect, you can also print any item for which the Console calls a Web browser, such as graphs, charts, and reports. This topic deals specifically with printing directly from the Console those resources or elements of resources that are not displayed in a web browser by default.

Printing Navigation Tree Views of Resources

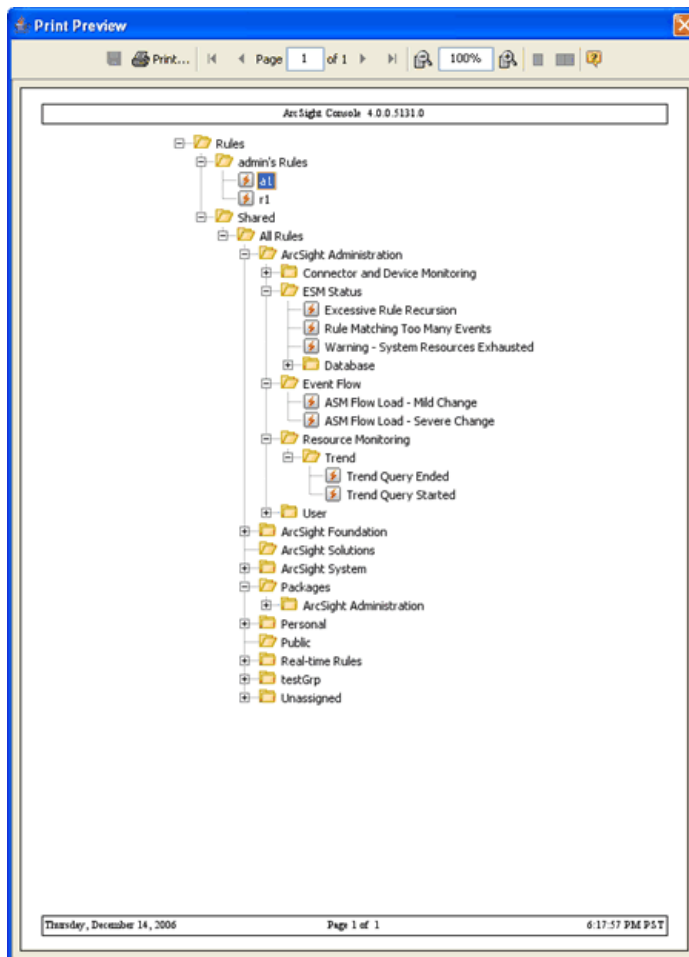
To print the Navigation tree for a resource:

- 1 In the Navigator, choose the resource you want to print.
- 2 Click items in the tree to expand or collapse folders in the tree depending on what you want to see in the printout.



A printout of the Navigation tree for a resource will show the tree exactly as it is displayed on the Console. Folders that are expanded or collapsed on the Console will show the same way in the printout. To print the tree showing the items contained in a particular folder, expand the folder in the Navigation tree before selecting the Print option.

- 3 Right-click any element in the Navigation tree for that resource and choose **Print <ResourceName> Tree**. (For example, Print Rule Tree.) Regardless of which item you select to access the right-click menu, the whole tree prints.
- 4 The system displays a preview of the printout. For example, here is a Print Preview of a Rules tree.



- 5 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 6 Click **OK** to print.

Printing Resource Definitions

You can print resource definitions for rules, filters, and cases. You can print a resource definition from the Navigator tree or from within the resource editor.

To print a resource definition:

- 1 In the Navigator, choose the type of resource you want to print.
- 2 Do either of the following:
 - ◆ "Right-click a particular instance of that resource (a rule, filter, or case), and choose **Print <ResourceName> Definition**. (For example, Print Rule Definition.)
 - Or
 - ◆ "Double-click a resource instance in a tree to open its editor in the Inspect/Edit panel, then right-click the topmost tab in the resource editor and choose **Print <ResourceName> Definition**. (For example, Print Rule Definition.)
- 3 The system displays a preview of the printout. For example, here is a Print Preview of a Rules definition.

From the Print Preview of a resource definition you can:
Export and save as an HTML file,
Or


Print.

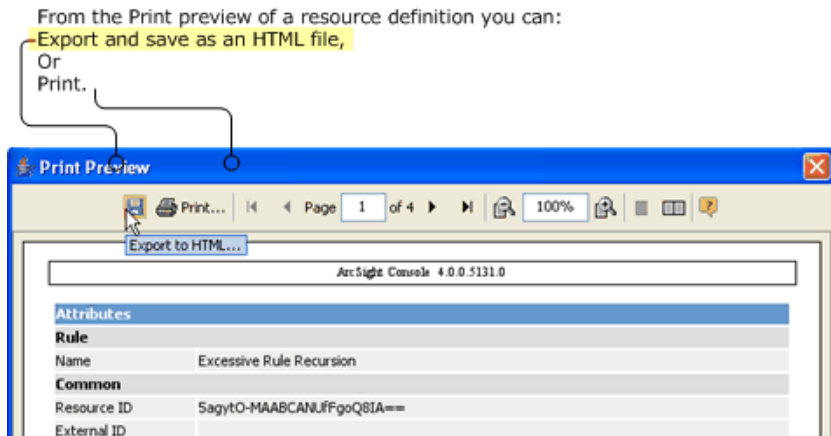


- 4 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 5 Click **OK** to print.

Saving as an HTML File

From the Print Preview dialog for a Resource Definition, you can also save the definition as an HTML file.

- 1 On the Print Preview dialog, click the **Export to HTML** () tool button.



- 2 In the file browser, navigate to the location where you want to save the HTML file.
- 3 Enter a name for the file in the File Name field. The File Type is "Web Page (*.html)" by default.
- 4 Click **Save**.

Printing Grid Views

To print items from a grid view, (such as an active channel or active list):

- 1 Select one or more items in the grid. (To select multiple, adjacent items, use the **Shift** key and mouse click, or simply click and drag. To select non-adjacent items, use the **Alt** key in combination with mouse clicks.)
- 2 Right-click and choose **Print Selected Rows**.
- 3 The system displays a preview of the printout. (For examples, see ["Using Column Flip Limit to the Control Format of Grid View Printouts"](#) on page 88.)
- 4 Click **Print** to bring up the Print dialog, and set these properties (which printer, page layout, and so on).
- 5 Click **OK** to print.



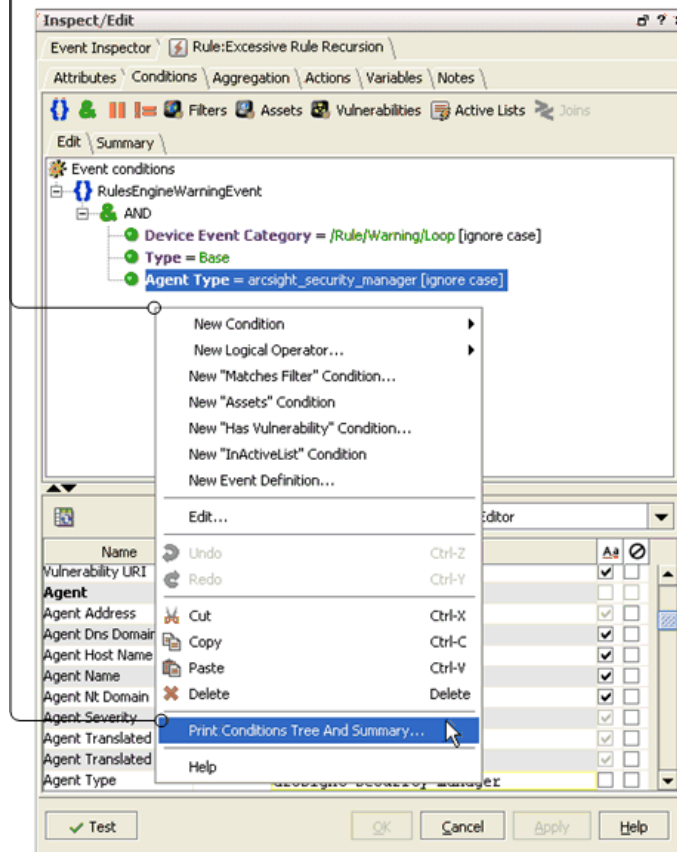
The format of a grid view printout is determined by the number of columns in the table and the configuration of the Column Flip Limit, which is set in the Console Preferences dialog. For more information, see ["Using Column Flip Limit to the Control Format of Grid View Printouts"](#) on page 88.

Printing Conditions Tree Summary

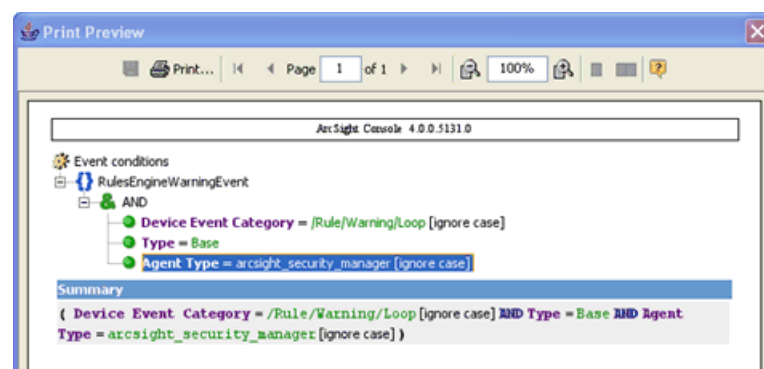
You can print Conditions for any resource with filters.

- 1 Open the resource in the Editor.
- 2 Click the Conditions tab.
- 3 Right-click anywhere on the Edit tab in the [Common Conditions Editor](#) (CCE).
- 4 Choose **Print Conditions Tree and Summary** from the context menu.

To print Conditions for any resource with filters, open the resource in the Editor, click the **Conditions** tab, and right-click anywhere on the **Edit** tab of the **Common Conditions Editor**. From the context menu, choose **Print Conditions Tree and Summary**.



- 5 The system displays a preview of the printout. For example, here is a Print Preview of the filter for a stock rule called Excessive Rule Recursion.

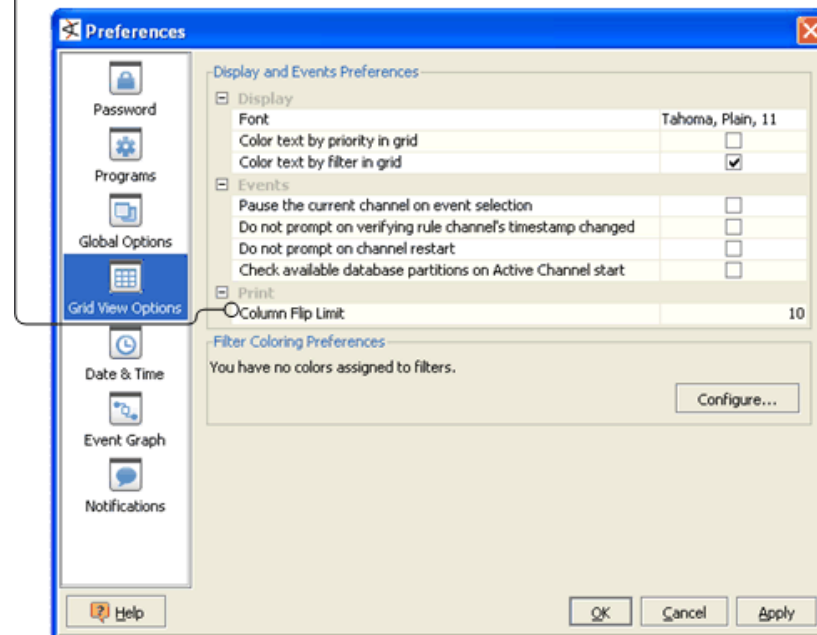


- 6 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 7 Click **OK** to print.

Using Column Flip Limit to the Control Format of Grid View Printouts

For printing tables from Grid Views (channels, lists, and so forth), you can configure the **Column Flip Limit** in the Console Preferences. (Choose **Edit > Preferences**, and click **Grid View Options**.) The default setting is 10 columns.

For printing tables from Grid Views (channels, lists, and so forth), you can configure the **Column Flip Limit**. (Choose **Edit > Preferences** and click **Grid View Options**.) A grid view will print as a table or with details per row, depending on the number of columns it has and how the Column Flip Limit is configured.



Grid views with the same or fewer columns than the Column Flip Limit print as a table, the same as that shown in the UI on the Console grid view.

Grid views with the same or fewer columns than the Column Flip Limit print as tables, in the same format shown in the UI on the Console grid views.

Print Preview

Print... Page 1 of 2 100%

ArcSight Console 4.0.0.5131.0

End Time	Name	Device Receipt Time	Event ID	Type	Target Address	Priority	Device Vendor	Device Severity	Aggregated Event Count
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280345	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280346	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280347	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280348	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280349	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280350	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280351	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280352	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280353	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280354	Base	192.168.40.235	3	ArcSight	Warning	1

Thursday, December 14, 2006 Page 1 of 2 4:53:19 PM PST

Grid views with more columns than the Column Flip Limit print details per-row rather in a normal table like that shown on the Console grid view.

Grid views with more columns than the Column Flip Limit print as detail per row. The bracketed section shown here represents the first row of this table.

ArcSight Console 4.0.0.5131.0											
1	End Time	14 Dec 2006 15:35:00 PST									
	Name	Monitor Event									
	Device Receipt Time	14 Dec 2006 15:35:00 PST									
	Event ID	50000280346									
	Type	Base									
	Target Address	192.168.40.235									
	Priority	3									
	Device Vendor	ArcSight									
	Device Severity	Warning									
	Aggregated Event Count	1									
	Device Product	ArcSight									
2	End Time	14 Dec 2006 15:35:00 PST									
	Name	Monitor Event									
	Device Receipt Time	14 Dec 2006 15:35:00 PST									
	Event ID	50000280347									
	Type	Base									
	Target Address	192.168.40.235									
	Priority	3									
	Device Vendor	ArcSight									
	Device Severity	Warning									
	Aggregated Event Count	1									
	Device Product	ArcSight									
3	End Time	14 Dec 2006 15:35:00 PST									
	Name	Monitor Event									
	Device Receipt Time	14 Dec 2006 15:35:00 PST									
	Event ID	50000280348									
	Type	Base									
	Target Address	192.168.40.235									
	Priority	3									
	Device Vendor	ArcSight									
	Device Severity	Warning									
	Aggregated Event Count	1									
	Device Product	ArcSight									
4	End Time	14 Dec 2006 15:35:00 PST									
	Name	Monitor Event									

Thursday, December 14, 2006 Page 1 of 4 3:58:25 PM PST

Instructions for setting the Column Flip Limit for grid views is also summarized in Setting Grid View Options in the [“Changing User Preferences”](#) on page 556, along with information about how to set other Console preferences.

Chapter 7

Monitoring Events

This topic describes how you use ArcSight to monitor enterprise security.

[“Monitoring Active Channels” on page 91](#)

[“Using Dashboards” on page 113](#)

[“Using Data Monitors” on page 117](#)

[“Monitoring Active Lists” on page 124](#)

[“Graphing Attacks” on page 125](#)

[“Pattern Discovery” on page 127](#)

You can monitor events on active channels through a rich set of views, field sets, charts, and grids, as described in the following topics.

Monitoring Active Channels

Monitoring events in the Viewer panel is described in these topics.

Using Views

Views can vary in scope and scale, from broad to narrow, and from graphic to detailed, depending on how your enterprise is organized and monitored.

Selecting a View

In the Viewer panel, click a tab at the **top** to choose an active channel by name. When you've chosen a channel, you can select various instances of that channel (e.g., a grid view and bar chart of the same data) by clicking its tile, or its tab at the **bottom** of the panel.

Alternately, to quickly advance through each of the tabs in the Viewer panel, press **Ctrl+Shift+N** (next) or **Ctrl+Shift+P** (previous) to jump forward or backward. This applies to any type of view in the Viewer panel.

Changing View Layouts

You change individual view layouts with the **Layout** menu available from the blue icon at the lower-right corner of the Viewer panel. Click this icon to choose:

Table 7-1 View Layout Options

Option	Result
Tab	Fill the active channel display with the current view and make other open views selectable by tabs at the lower border.
Tile Best Fit	Display all views in the active channel as variously shaped tiles, giving each a proportional amount of space.
Tile Horizontally	Display all views in the active channel horizontally, giving each a proportional amount of space.
Tile Vertically	Display all views in the active channel vertically, giving each a proportional amount of space.

Floating a View

In the active channel's name tab, right-click and choose **Float**.

Closing one View or All Views

In the active channel's name tab, right-click and choose **Close** or **Close All**.

To close an individual view **Shift+click** its name tab. (You can also right-click a view name tab and choose **Close** from the popup menu.)

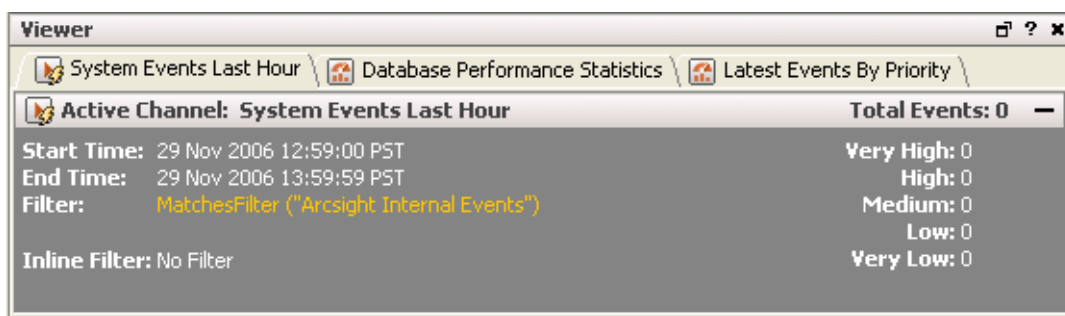
Closing all Views Except the Current One

In the active channel's name tab, right-click and choose **Close All But Current**.

Viewing and Using Channels

Viewing and using active channels includes creating them, filtering them, customizing contents, changing presentation formats or layouts, and deleting them.

Using active channels begins with reading and understanding their headers. Beginning in ArcSight v3.0, some information that was displayed in the Console's framework has moved to active channel headers.

**Figure 7-1 Example of an Active Channel Header**

Also, you can create new active channels from rules.

Viewing an Active Channel


- 1 Choose **Active Channels** in the Navigator.



- 2 Right-click on a channel and choose **Show Active Channel**. The selected channel is displayed in the Viewer.



If a channel is open when Daylight Savings Time goes into or out of effect, the live channel will not reflect the correct start and end times until it is stopped and re-started.

Sorting Events in an Active Channel

The names of sortable fields in column headers are indicated with a double arrow icon .

If a field is already sorted, an up  or down  arrow indicates the direction of the sort.

- To sort the list by a column, right-click over the column and select **Sort Column**.
- To reverse the sort order, select **Sort Column** again on an already-sorted column.
- To remove a sort, right-click over a sorted column and select **Remove Sort**.

For more information, see [“Applying a Field Set to an Active Channel” on page 94](#) and [“Using Sortable Columns in Grid Views” on page 766](#). For information on how to create field sets that use sortable field sets, see [“Using Field Sets” on page 101](#).

Creating an Active Channel

- 1 Choose the **File>New>Active Channel** menu command to open the **New Active Channel** dialog box, or right-click a group in the Active Channel resource tree and choose New Active Channel.
- 2 In the dialog box, name the channel and choose from the [Active Channel Options](#) described below.
- 3 Click the **Examples** button to see how to specify commonly used channel values.
- 4 Click **OK** to save the new channel in your group in the Active Channels resource tree, and to open and run it in the Viewer panel.



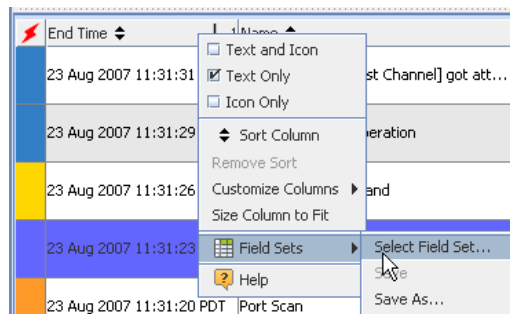
Starting with ArcSight ESM v4.0, you can view most resources (in addition to events) in active channels, including Assets, Vulnerabilities, Asset Categories, Scanner Reports, Cases, and Stages. In the Navigator, right-click on a resource or group, and choose **Show <ResourceName>**. The resource(s) are displayed in an active channel view.

Using slightly different menu options, you can view the results of triggered Rules in channels as well. (For information on creating active channels for Rules, see [“Verifying Rule\(s\) with Events” on page 326](#).)

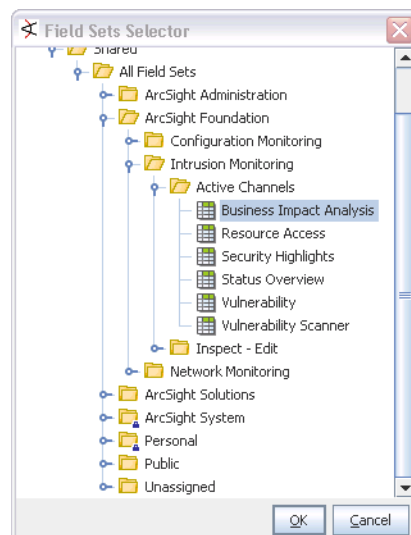
You can also create active channels from filters. In the Filters resource tree, right-click a filter and choose **Create Channel with Filter**. Many resources that have filters also provide this option. For example, you can right-click on Connectors in the Navigator, and choose Create Channel with Filter to create a channel with the filter used by that connector. You can do the same with Assets (Assets, Vulnerabilities, Zones, Categories), Cases, and Stages. (For Cases, choose Case Details Channel as described in [“Creating a Channel for a Case” on page 401](#). The case must include some events.)

Applying a Field Set to an Active Channel

- 1 Right-click over any field header and choose **Field Set > Select a Field Set** to open the Field Sets Selector dialog.



- 2 In the Field Sets Selector dialog, select a field set and click **OK**.



The active channel is displayed with the selected field set.



The "Sortable Field Sets" under ArcSight System are not available for selecting in this mode. Other field sets available for use are, in effect, sortable. The ArcSight System sortable field sets are a special set marked for internal, system use to provide the sortable functionality and maintain consistency between the Console user interface, field sets, and database indexes.

For more information on sorting, see ["Sorting Events in an Active Channel" on page 93](#).

Using an Active Channel Header

Each active channel has a header section with several features you can use to understand and manipulate what the channel displays.

Table 7-2 Active Channel Header Features

Feature	Usage
Name and Total	The top line of the header shows the channel's name and the total number of events it contains. You can also use the Plus (+) and Minus (-) buttons at the right end to open and close the header.
Priority Indicators	On the right-hand border of the header is a column of event-priority statistic indicators. The numbers beside the Priority categories show the number of events in those categories. You can click these indicators to instantly filter the channel to show only the selected priority.
Time Span	The Start Time and End Time show the chronological range of the channel.
Filter status	This describes the filter that limits what the channel shows. Click a filter status name, such as <No Filter> , to open the Active Channel Editor and its Filters tab, where you can add, edit, or delete contents as described in "Creating Filters" on page 147 . You can also right-click the current filter status and choose to edit, save, or remove it.
Radar display button	Open and close the display with the Plus (+) and Minus (-) button at the right end of the Filter line.
Radar display operation	Click , Shift+click , Ctrl+click , or drag to select bars in the display. You can also drag a selection's borders left or right. The grid then shows just the events the selection represents. The display shows "This channel is active but temporarily empty" at any time, no matter how briefly, if there are no qualifying events. This also might show when a channel first opens.

Filtering an Active Channel

You can filter active channels through the Filter tab of the Active Channel Editor or inline using the blank fields in the top row of each grid view. Right-click the filter name in the header and choose **Edit Filter** to open the editor and create a filter as described in ["Creating Filters" on page 147](#). To use inline filters, see ["Using Grids" on page 105](#).



Understanding how to use the Common Conditions Editor (CCE) is integral to creating and editing filters. Please ["Common Conditions Editor" on page 616](#) for more information.

Saving Copies of Active Channels and Filters

You may want to save copies of active channels or their filters so that you can modify them later. This is particularly useful when you want to retain an original channel or filter as is, but use a copy of it as a basis for a new resource.

You can save a copy of an active channel under a new name. Right-click the filter name in the header, and choose **Save Active Channel As**. This brings up the Active Channels

Selector dialog which shows the Active Channels resource tree. Navigate to the location where you want to save the channel, enter a new name for it, and click **OK**.

You can save a copy of the filter associated with an active channel and use it independently, or as a basis for other filters. Right-click the filter name in the header, and choose **Save Filter**. This brings up the Filter Selector dialog which shows the Filters resource tree. Navigate to the location where you want to save the filter, enter a new name for it, and click **OK**.

Editing an Active Channel

- 1 Right-click a channel in the Navigator panel's Active Channel resource tree and choose **Edit Active Channel**.
- 2 To change an active channel's operating parameters. Click the **Attributes** tab. The attributes are described in [Active Channel Options](#).

Active Channel Options

Feature	Usage
Start Time	<p>The relative or absolute time reference that begins the period in which to actively track events in the channel. Edit the time expression, choose a common expression from the drop-down menu, or click the Selector button to choose an absolute date and time value. See "Timestamp Variables" on page 780 for more expression options.</p> <p>Note: If a channel is open when Daylight Savings Time goes into or out of effect, the live channel will not reflect the correct start time until it is stopped and re-started.</p>
End Time	<p>The relative or absolute time reference that ends the period in which to actively track the events in the channel. Edit the time expression, choose a common expression from the drop-down menu, or click the Selector button to choose an absolute date and time value. See "Timestamp Variables" on page 780 for more expression options.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If a channel is open when Daylight Savings Time goes into or out of effect, the live channel will not reflect the correct start time until it is stopped and re-started. • If setting the End Time results in the message "Invalid end date for sliding channel", this is because the channel is set to "Continuously Evaluate" instead of "Evaluate once at attach time". Either re-set the End Time or change the Time Parameters for the channel to "Continuously evaluate".
Use as Timestamp	<p>Choose the event-timing phase that best supports your analysis. End Time represents the time the event ended, as reported by the device. Manager Receipt Time is the event's recorded arrival time at the ArcSight Manager.</p>
Time Parameters	<p>Choose whether the channel will Continuously evaluate to show events that are qualified by Start and End times which are re-evaluated constantly while the channel is running, or Evaluate once at attach time to show only the events that qualify when the channel is first run.</p> <p>A channel set to "Continuously evaluate" is also known as a <i>sliding channel</i>, and typically has its End Time set to \$Now.</p>

Feature	Usage
Default Field Set	Choose an existing event field set for the events processed through the channel.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

- 3 Click the **Filter** tab to edit the channel's filter condition as described in [“Creating Filters” on page 147](#).
- 4 Click the **Sort Fields** tab to explicitly set which fields you want to sort the channel on in grid views, the sort order for those fields, and whether sorting for each field is ascending (A to Z) or descending (Z to A).
- 5 Click the **Variables** tab to use ArcSight variables with the active channel's filters.
- 6 Click **Apply** or **OK** to save the updated channel.

Defining Grid Fields Options

In the New Active Channel dialog box you can choose from the **Select a Field Set** menu, or you can click the **Define** button to open the Define Grid Fields dialog box. See [“Using Field Sets” on page 101](#) for more information. To change these choices after creating a channel, use the steps described in [“Customizing Grid Columns” on page 111](#).

Table 7-3 Grid Field Options

Feature	Usage
Fields	A name for the set.
Available Fields	Select the event fields (also called data fields or attributes) that you want the channel to process. As you make selections, they appear in the Fields to Show list at the right. Remember that not all fields are readily sortable.
Fields to Show	This list shows the selections you have made in the Available Fields list. The order you give to the fields in this list becomes their default presentation order in grid views. Once populated, you can select one or more fields (Shift+click and Ctrl+click apply) to rearrange with the Move Up , Move Down , and Remove buttons.
Move Up, Move Down, Remove	These buttons move or remove the fields you select in the Fields to Show list. The order you set becomes the presentation order in grid views.
Sort First By	After selecting and ordering fields, you establish their sorting order (also called their "group by" order). Use Sort First By to set the ascending (A to Z) or descending (Z to A) order of the first or most-significant column.
Then By	Use the first Then By sort-order field to set the second sorting order. Use the second Then By sort-order field to set the third sorting order.
More, Less	Click More if you need an additional Then By field. Click Less to remove one.

Discovering Patterns in an Active Channel

Right-click the channel in the Navigator panel's Active Channels resource tree and choose **Discover Patterns**. ArcSight takes a snapshot of the channel's current contents and examines it for patterns. You see the snapshot in the Viewer panel and the profile that generated the pattern appears in your personal folder in the Navigator panel's Pattern Discovery resource tree.

Deleting an Active Channel

Right-click the channel in the Navigator panel's Active Channels resource tree and choose **Delete Active Channel**.

Adding a View Format

To add another type of presentation (view) for the data in an active channel, click the **View Type** icon in the lower-right corner of the Viewer panel. Choose among grids and the various types of chart or graphic views.

Changing View Layouts

To change the visual arrangement of individual channels within a view container, such as data monitors within a dashboard, click the **Layout** icon and choose to show or arrange the views by **Tab**, or **Tile Best Fit**, **Tile Horizontally**, or **Tile Vertically**.

Investigating Views

This topic explains how to use the Console's Investigate command to easily refine and explore channels contextually, using attributes of the events already being displayed in grid views. The Investigate command uses these attributes, and the values found in their events, to automatically formulate simple filters or conditions. When you create or refine a filter through Investigate, the Viewer panel automatically opens a new view of the channel with the filter applied. You explore the filter's effect in this view. You then have the option to keep the view by saving the channel under a new name, or discarding it by right-clicking in the grid and choosing **Close**.

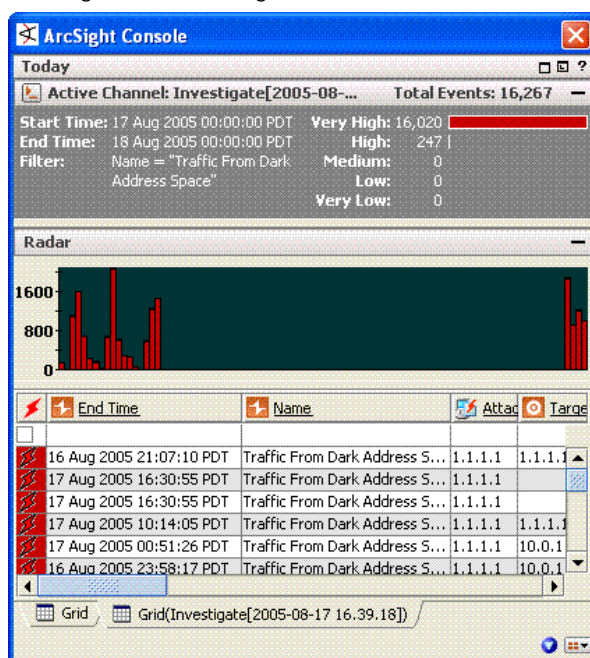


Figure 7-2 A temporary view created with the Investigate command

When you use Investigate to add a condition to a resource editor such as Rules or Filters, the condition appears in the editor panel where you can modify it or click **Apply** to put it into effect.

The new or modified views you generate with the Investigate command can be grids, or you can choose to display them in applicable chart formats using the **Viewer Selector** icon in the lower-right corner of the Viewer panel.

To learn more about the event attributes these options use, please see [“Data Fields” on page 633](#).

Using an Event Attribute to Show a New Filtered View

These options completely control the new view created, ignoring the filter in the original view. You most often use them to test and explore.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Create Filter [Attribute=Value]	Show only those events in which the selected attribute matches the value in the selected event.
Create Filter [Attribute!=Value]	Show only those events in which the selected attribute does not match the value in the selected event.
Create Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. Generally, attributes are considered related if they share a common focus such as IP addresses.

Refining a Filter with an Event Attribute

These options open a new view that uses a version of the prior filter modified to include the new filter component just selected. You usually apply these as part of a filter-refinement process.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add [Attribute=Value] to Filter	Show only those events that match both the prior and new filter elements.
Add [Attribute!=Value] to Filter	Show only those events that do not match both the prior and new filter elements.
Add to Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. This filtering element is applied in addition to any other already present. Generally, attributes are considered related if they share a common focus such as IP addresses.

Adding an Event Attribute to a Filtering Condition

The **Add condition to editor** options apply to the editor in the Inspect/Edit panel that currently has focus. If no editor is open, the default target is the Filters Editor.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add Condition [Attribute=Value] to Editor	In the current editor, insert a new condition in which the selected attribute matches the value in the selected event.
Add Condition [Attribute!=Value] to Editor	In the current editor, insert a new condition in which the selected attribute does not match the value in the selected event.
Add Condition to Editor [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, add a condition to the current editor using the available list of attribute-value pairs that do (or do not) equate. Generally, attributes are considered related if they share a common focus such as IP addresses.

To remove a condition from the editor, right-click it and choose **Delete**.

When you are using these options to affect a view that is subject to the editor in use, click **Apply** or **OK** in the editor to put the condition into effect.

Contextual filters (in contrast to conditions) are temporary unless you save the modified view as a named active channel. Condition statements are saved with their relevant editors.

Permanently Modifying an Active Channel

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

Showing an Exploited Vulnerability

The Investigate options include the ability to look for potentially exploitable vulnerabilities associated with an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Exploited Vulnerabilities**. Available information appears in the Vulnerabilities tab of the relevant Asset Editor.

Showing a Targeted Asset

You can also find out more about an asset targeted by an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Targeted Asset**. Available information appears in the Asset Editor.

Using Field Sets

Field sets are simply named subsets chosen from the available *data fields*. Field sets can help you quickly focus a grid view, Event Inspector, or other field array on a particular context such as customer accounts or vulnerability.



Field sets are a shareable resource that you can manage and apply through the Field Sets resource tree in the Active Channels section of the Navigator panel. (In the Navigator, choose **Active Channels**, and click the **Field Sets** tab.) These field sets also support the new variables data fields. Field sets supersede and include the previous concept of column sets.

ArcSight comes with a list of default field sets. These sets show you the types of uses to which this feature can be put. To make these completely applicable to your mission, you, or an analyst or a member of ArcSight Professional Services, will need to tailor these sets or create new ones.

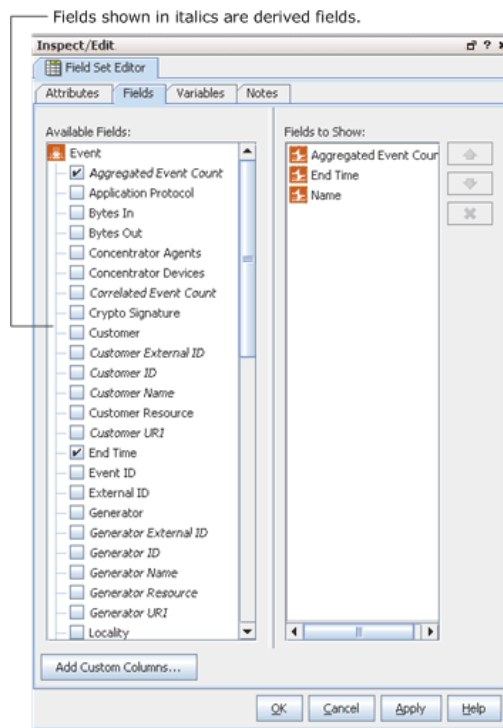


Looking for information about custom columns? If you want to add a "custom column", you need to create or define it first. Once a custom column is created, it shows up in the Available Fields list under "Custom Column" and you can include it in grid views the same as any other field. For information on creating custom columns, see ["Customizing Grid Columns" on page 111](#). For information on working with grid views, see ["Using Grids" on page 105](#).

Creating a Field Set

- 1 Choose **File>New** on the Console's menu, or the **New Resource** button , and the Field Set  command. You can also right-click a folder in the **Field Sets** resource tree and choose **New Field Set** or **New Sortable Field Set**.
- 2 In the Field Set Editor, name the set in the Attributes tab.
- 3 Enter values in the other Attributes fields if appropriate.

- 4 Click the Fields tab and select the available fields you want to include in the new set. Selected fields appear in the Fields to Show list.



Fields shown in italics are *derived* from data in other fields. Derived fields show up in various places on the Console UI including on the Field Set editor, and the Common Conditions Editor (CCE) aggregation tabs (e.g., Rules, Filters, and so forth). See also, [“Using Field Sets” on page 623](#) in the [“Common Conditions Editor” on page 616](#) reference topic.

- 5 If you need to add variables to the available fields, use the Variables tab.
- 6 Once you have made your choices, use the **Up** arrow, **Down** arrow, and **Remove** buttons to arrange selected fields.
- 7 Click **Apply** to save the set in the resource tree and continue editing. Click **OK** to save the set in the resource tree and close the editor.

Editing a Field Set

- 1 In the Field Sets tab of the Active Channels resource tree, right-click a field set and choose **Edit Field Set**.
- 2 In the Field Set Editor, use the **Attributes** tab to change the field set's name.
- 3 Click the **Fields** tab and use its Available Fields list to select fields to add to the list.
- 4 Use the **Variables** tab to make additional variables available in the list.
- 5 Rearrange or remove fields in the Fields to Show list.
- 6 Click **Apply** to save the set in the resource tree and continue editing. Click **OK** to save the set in the resource tree and close the editor.

Sharing a Field Set

When you create a field set below the Shared folder in the Field Sets resource tree, it is available to other users who have permission for those folders. If you create one in your own folder, it is not available to other users unless you move, copy, or link it into a Shared folder.

- 1 Click the field set in your folder and drag it to the appropriate Shared folder.
- 2 In the Drag and Drop dialog box, choose to **Move**, **Copy**, or **Link** the resource in its new location.

Moving relocates the resource, leaving a single instance of it in the tree. Copying makes a duplicate, leaving two independent instances of the resource. Linking leaves the original in place, and creates a connected copy in the new location that will change whenever the master instance changes.

You create sortable field sets in the same way, but without the option to add variables to the sets.

You control access to field set folders like any other resource.

See also [“Applying a Field Set to an Active Channel” on page 94](#) and [Sorting Events in a Channel](#).

Using Charts

The Console offers several chart view options for active channels and for data monitors. You can add chart views of the data in many active channels or data monitors simply by choosing a chart type from the **Format** pop-up menu in the view's lower-right corner.

ArcSight charts remain linked to the data they represent. You can immediately see a chart's events in a grid view that presents the data as charted, or filtered further using the options of the Investigate command.

You can click and drag three-dimensional charts on their vertical or horizontal axes to tilt them for better viewing.

Charting an Active Channel's Contents

- 1 In the Navigator panel's Active Channels resource tree, right-click a channel and choose **Show Active Channel**.
- 2 In the Viewer panel, in the lower-right corner of the newly opened active channel, click the **Viewer Selector** icon to open its menu.
- 3 In the menu's **Chart** branch, choose one of the chart types described below.
- 4 The data in the view opens in an additional chart presentation, in the chosen format, within the active channel.
- 5 Click the **Layout** icon in the channel's lower-right corner to change the visual arrangement (tabbed or tiled) of the views within the channel, if needed.

Charting a Data Monitor's Contents

- 1 In the Navigator panel's Dashboards resource tree, double-click a dashboard or right-click it and choose **Show Dashboard**.
- 2 In the Viewer panel, in the lower-right corner of an applicable data monitor, click the **Viewer Selector** icon to open its menu.

3 In the chart menu, choose one of the types described below.

4 The data in the monitor switches to a chart presentation.

For data monitors, the **Chart Showing Priorities** submenu offers many of these same charting options, but with graphic elements (e.g., pie wedges or bar segments) that distinguish their priority-level components.

Remember that the contents of charts are affected by the things that affect active channels or data monitors, such as changing time parameters or filters. Not all charts are applicable to, or available for, all views.

Table 7-4 Chart Types

Chart Type	Description
Area	A horizontal chart in which bands occupy various amounts of the displayed area to indicate relevant values.
Area Radar	A circular chart that shows proportional values as solid graphic extensions from a central zero point, outward to a higher-value border, and occupying relative numbers of degrees of the available circle.
Horizontal Bar	A horizontal chart that shows changes in relative quantities, usually by time units seen as solid rectangles, over a span of time.
Line	A horizontal chart that shows changes in relative quantities, usually by time units plotted on a line, over a span of time.
Pie	A circular chart with proportional wedges for the relevant values.
Radar	A circular chart that shows proportional values as a line plot from a central zero point, outward to a higher-value border, and occupying relative numbers of degrees of the available circle.
Scatter Plot	A horizontal chart that shows changes in relative quantities, usually by time units plotted as separate points, over a span of time.
Stacking Area	A horizontal chart in which stacked bands occupy various amounts of the displayed area to indicate relevant values.
Stacking Bar	A horizontal chart that shows changes in relative quantities, usually by time units seen as stacked solid rectangles, over a span of time.
3D Bar	A corner-anchored graph with height, width, and depth dimensions that can show three axes of categorical and quantitative information.

Exploring the Events Behind a Chart

To see a grid view of the events behind an active channel's chart, double-click the section of the graphic that represents those events. To filter those events further, right-click the relevant section of the chart and choose an Investigate command option. In charts that show color keys, such as Events by Priority, you can also double-click a color chip to open a grid view filtered by that key.

To see an active channel grid view of the events behind a data monitor's chart, double-click the section of the graphic that represents those events, or right-click and choose **Show Details**, or choose **Show Detailed Channels** to see a view for each of the chart's components.

Using Grids

The tasks in this topic explain how to monitor events in grid views. To better understand the details in grid views, please read more about event grid data fields.

Monitoring Events in the Grid View

Click an active channel's tab at the top of the Viewer panel and select the **Grid** view of that channel using the tab at the bottom. When new events occur, they are displayed at the top of a grid view as a new row. Events can appear in ArcSight Severity or filter colors. You can set the color-code for events by using the steps described in ["Changing User Preferences" on page 556](#).

Sorting Columns in the Grid View

Right-click and select **Sort Column** on the grid column header of a particular column (for columns that support sorting) to sort the contents of that column. If the column contains numerals, it sorts from highest to lowest value (or vice versa). If the column contains words or alphabetic characters, it sorts alphabetically from A to Z (or vice versa).

You can also perform an advanced sort on one or more columns in the grid view. When selecting a secondary sort column, select the secondary column first, then the primary column. For example, to sort by Event Name then by Detect Time, sort **Detect Time** first, then **Event Name**.

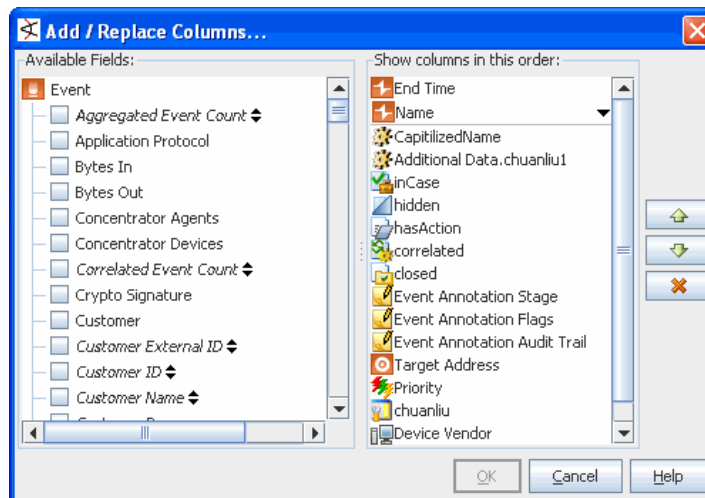
After you sort a column it automatically pauses the current channel, stopping events from appearing in the grid view. Click the **Play** button in the Replay Controls to restart the channel and resume receiving events in the grid view.



When you sort on time and on priority, you might observe cases where events with the same apparent time are not in priority order. Because events are timestamped to milliseconds, they may in fact be in time order although the milliseconds are not showing. In this case, you can show milliseconds to validate time order. Choose **Edit > Preferences**, then in the Date and Time panel change the **Date & Time** Format to also show milliseconds by adding "SS" to the seconds parameter, e.g., d MMM yyyy HH:mm:ss:SS z.


Adding, Replacing, or Removing a Column in the Grid View

- 1 Right-click the column header and select **Add/Replace Columns** to bring up the associated dialog. (Note that fields shown in italics are *derived* fields.)







Looking for information about custom columns? If you want to add a "custom column", you need to create or define it first. Once a custom column is created, it shows up here in the Available Fields list under "Custom Column" and you can include it in grid views the same as any other field. For information on creating custom columns, see ["Customizing Grid Columns" on page 111](#).

- ◆ **To add a column:** Select data fields (column titles) to add from the Available Fields list on the left. Check marks indicate selected columns. The selected columns show up in the list on the right as you select them. (Alternatively, when you deselect or uncheck a data field on the left, the column is removed from the right-hand list.)
- ◆ **To remove a column:** Select a field from the right-hand list and click the Delete button . Also, deselecting a data field from the Available Fields list on the left removes it from the right-hand list. Removing a column from a grid view does not delete the column information from the ArcSight Database.



You also can remove a column directly from the grid view without opening the Add/Remove Columns dialog. To do this, right-click a column header and select **Remove Column**.

- ◆ **To re-order the columns:** Select a data field (column title) in the right-hand list and click the Up  and Down  buttons to move it. The top-to-bottom order shown in the "Show columns in this order" list (on the right) translates to a left-to-right order when applied in the grid view. A column title at the top of this list will show as the first column in the grid view (on the far left in the grid display); a column title at the bottom of this list will show as the last column in the grid view (on the far right of the grid display).
- 2 Click **OK** to save changes you made on the Add/Remove Columns dialog. The grid view reflects added, replaced, removed, or re-sorted fields.

Sizing a Column in the Grid View

Right-click a column header and select **Size Column To Fit**.

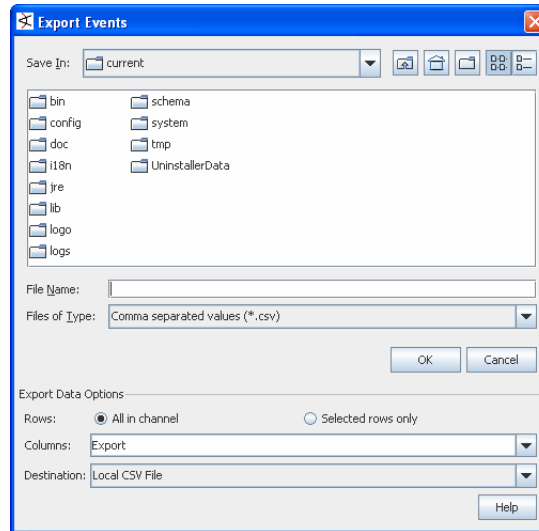
Showing or Hiding Grid View Column Text and Icons

Right-click a column header and select one of the following options:

Option	Display Result
Text and Icon	Display the column heading and its icon.
Text Only	Display only the column heading.
Icon Only	Display only the icon.

Exporting Events to a File

- 1 Right-click one or more events in the Viewer panel and choose **Export > Events** in channel. This brings up the Export Events dialog.



- 2 Use the file browser to navigate to the location where you want to save the file. You can use the buttons across the top right of the dialog to move up one directory level, go to your desktop, create a new folder, show files as a list or a list with details. Also, you can use the **Files of Type** drop-down menu to display only comma-separated values (CSV) format files or all files while you are browsing the directories.
- 3 In the **File Name** field, enter a name for the file to which you want to export the event(s).
- 4 Under **Export Data Options**:
 - ◆ Select **All in channel** to export all the events in the channel. The system will export all events in the channel to the specified file, regardless of which events you originally selected in the grid view. (This is option is selected by default.)
 - ◆ Select **Selected rows only** to export only the events you selected in the grid view.
 - ◆ From the **Columns** drop-down menu, choose a fieldset to use for the exported events. This limits the fields exposed in the exported events to the chosen fieldset. (An "Export" fieldset is selected by default.)
 - ◆ Select a **Destination** for the file. Local CSV File is selected by default, and is typically the only option.
- 5 Click **OK** to export the events to a file with the specified settings.

Choosing Grid View Menu Commands

Right-click an event or event field in a grid in the Viewer panel to open a context menu. The commands available are those that apply to the current combination of event type, view, filter, and so forth.

Table 7-5 Grid View Context Menu Commands

Command	Description
Show Event Details	Use the Event Inspector to examine all the attribute details associated with the event.

Command	Description
Rule Options	<ul style="list-style-type: none"> • Simple chain: Show this event's base and correlated event tree in the Event Inspector. • Detailed chain: Show this event's base and correlated events in detail in a new grid view. • Show triggering resource: Show the rule that triggered this event in the Rule Editor. • Clear rule actions: Clears the list (if one is showing) of rule actions pending on the ArcSight Manager.
Investigate	Create a temporary filter "on the fly" based on the field's highlighted event. The Investigate command uses the event's attribute type (its column heading), and the particular event's field value (e.g., an exact IP address), to formulate simple filters based on these two factors. The filter's operators can include Create Filter [X = Y] and Add Condition [X = Y] to Editor . The Investigate submenu also offers the Show Exploited Vulnerability and Show Targeted Asset commands to open detailed views of assets or vulnerabilities, if present in the selected event.
Active List	Add the selected event to, or remove it from an active list. This is explained further in "Active Lists" on page 574 and "Managing Active Lists" on page 385 .
Annotate Event	Open this event in the Annotate Events dialog box, where you can click the Stage field to set a collaboration workflow sequence for this event. When you select a stage you automatically place the event in the corresponding group in the Stages resource tree in the Navigator panel, where you and other analysts can collaborate on its investigation and resolution.
Move Timeline to Current Event	Reset the event timeline in the view to the time of the currently selected event.
Select Events with Matching Cell	Select any other events in the view that have values matching that in the currently selected cell.
Invert Selection	Select all events not currently selected, and deselect those that are currently selected.
Event Graph	Graph any logical relationships (i.e., source/target IP address connections) that exist among the currently selected events.
Rule Chain Graph	Graph the rule chain(s) behind the currently selected triggered events.
Geographic View	Geographically map the source and destination IP addresses of the selected events.
Tools	Run your choice of the standard network lookup tools, using field values from the selected events.
Create Rule	Use the Rule Editor to create an ArcSight rule to apply to the selected events.
Export	Export the selected events to an external event-tracking system, such as comma-separated-value (CSV) data in a report or for a spreadsheet, or save it as an HTML or a JPEG file.
Add to Case	Add the selected events to a new case for tracking.
Payload	Keep or discard the payload associated with a selected event.


Command	Description
Show Context Report	Output a report concerning rules and events within a specified time window.
Close	Close the current individual view within the selected view type.
Knowledge Base	Show the Knowledge Base pages associated with the selected events, or associate new pages.
Vendor Page	If available, show vendor Web page of the event's sensing device.
Help	Open the online Help to this topic.

Filtering Grid Views with Inline Filters

Active channels that display grid views have an inline means for creating simple filters. These filters are based on using a value found in one column, or creating AND conditions between values found in two or more columns. Inline filtering is a very rapid way to constrain detailed views.

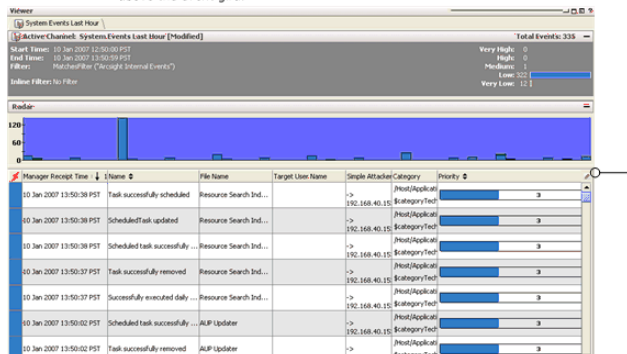
These filters are called "inline filters". Also, note that while they are in effect, inline filters affect all views generated for the channel.

You can create, change, save, hide, and remove inline filters from the grid view. Also, you can create and manage multiple inline filters from this view.

- To create an inline filter, click the Inline Filter link in the event header or click the Edit Inline Filter  button at the top right of the grid view to display the inline filtering fields. Type a value by which you want to filter for one or more fields relating to a column in the grid. Click **Apply** to immediately apply the filter to the view. The inline filter is displayed in the header under the standard filter.
- To change an inline filter, click the **Edit Inline Filter** button again, and choose new values, and apply. The **Clear** button clears the inline filter fields, and **Cancel** closes the inline filtering window without saving current changes.
- To remove an inline filter, right-click over the Inline Filter name in the header for the selected event and choose **Remove Inline Filter**.
- To save an inline filter, right-click over the Inline Filter name in the header for the selected event and choose **Save Inline Filter**. This brings up a Filters Selector dialog that shows the Filters tree. Navigate to the folder where you want to save the current filter, and click **OK**.
- To highlight the filtered events, click the Highlight checkbox ("on" is check marked) and use the drop-down color selector to select a color from the palette.
- To create and manage multiple inline filters, click the + button next to the Highlight options under the inline filters to add filter definition rows. (Click the - button to remove filter rows.) The potential uses of multiple inline filters are extensive, but essentially this provides a means of creating a filter with complex conditions, inline in an active channel. For example, in the Name column for an event, you could specify that the event name contains "ActiveList" on the first filter row and that the name does not contain "Successful". You could extend this filter by specifying what you are looking for in some of the other fields or even add more qualifiers on the Name field.

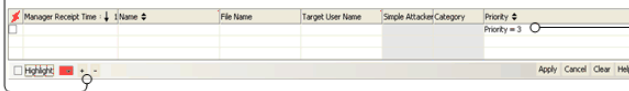
All fields can be narrowed down in this way, using multiple filter definition rows.

To add an inline filter, click the **Edit Inline Filter** button to the right of the viewer above the event grid.



Clicking the **Edit Inline Filter** button opens an inline filtering window. Type a value in one or more fields to further filter the event stream. In this example, we add an inline filter on the Priority field to specify showing only events of Priority 3. Click **Apply** to apply the inline filter.

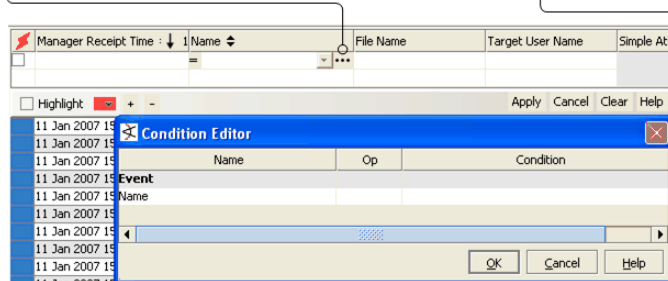
Also, you can click the + button to add filter definition rows and create multiple inline filters. Click the - button to remove rows.



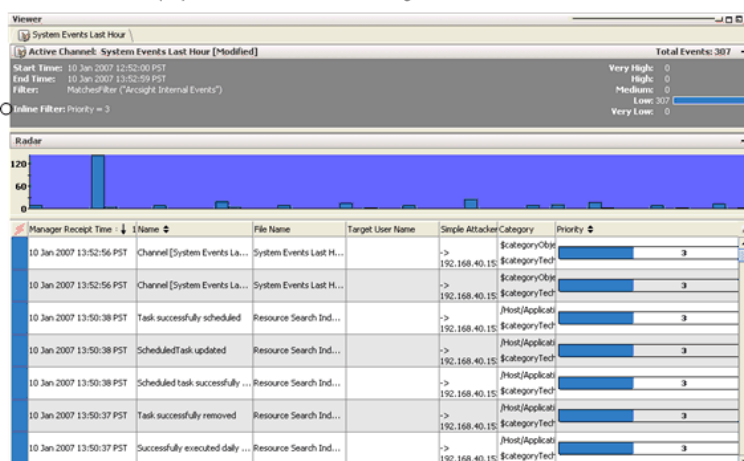
When you click into a field, you get an equals operator, a drop-down list of available values for that field based on the events currently displayed, and an ellipsis (...) indicating another dialog is available.

If these inline options are not enough to create the filter, click the ellipses (...)

to bring up a Conditions Editor dialog in which to create the filter for the selected field.



Once the inline filter is applied, only events that match current filter and the inline filter are shown. The inline filter used is displayed in the header under the original filter.



Custom columns are not available as arguments for inline filtering.

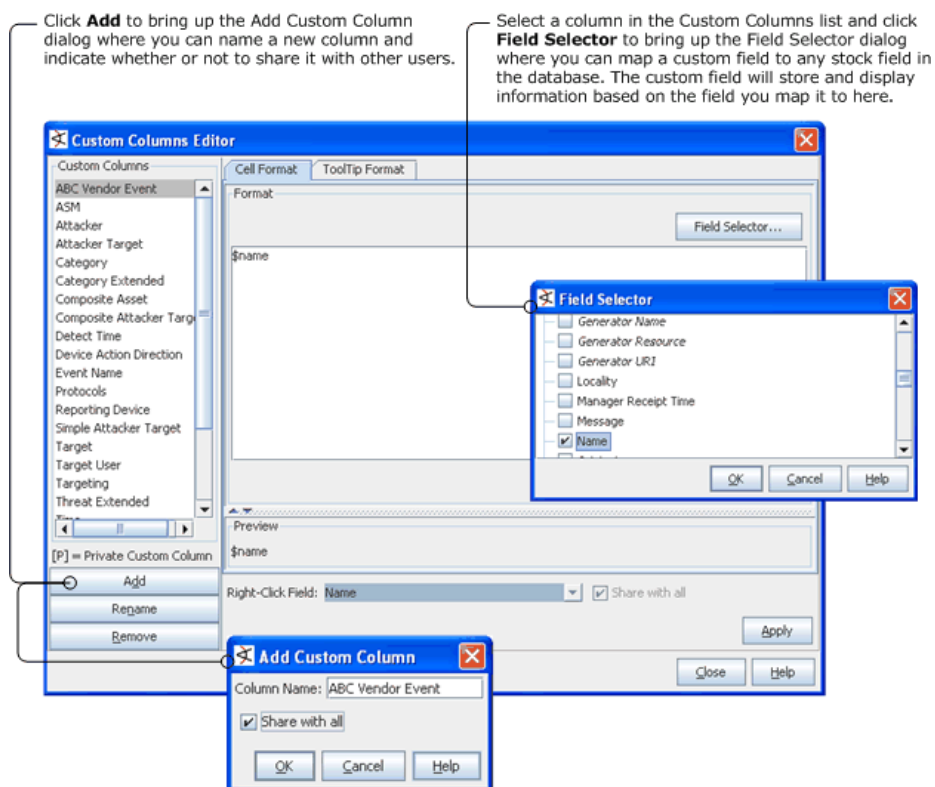
Customizing Grid Columns

You can create Viewer panel grid view columns with customized cell content and presentation formats, tooltip contents, and right-click pop-up values.

You make these changes through the Custom Columns Editor. In the Editor you create new named columns. For each column you select event data fields to display, and if you wish, the HTML formatting to use in its cells. The tooltip option specifies the formatting and content of the tooltips you see when you hover the pointer over cells in that column. The right-click field option sets the event data field to use in columns where there are right-click commands that use field names as arguments (e.g., "Investigate...").

Creating a Custom Column

- 1 Right-click a column header in a Viewer panel grid view and choose **Edit Custom Columns**. This brings up the Custom Columns Editor.



- 2 Click **Add** to name a new column. If you want everyone to see the new column (not just administrators), select the **Share with all** check box. (You can toggle this option on or off later too from the Cell Format tab.) When you click OK on the **Add Custom Column** dialog, the new column name is added to the Custom Columns list on the left side of editor.
- 3 Click **Field Selector** on the **Cell Format** tab to pick the event attribute(s) you want to display in this column and click **OK**.
- 4 In the **Format** text box apply Java-compatible HTML formatting around the field strings, if appropriate. Remember to bracket such formatting with the HTML tag, e.g., `<HTML>$type</HTML>`.
- 5 Click **Preview** to see how the contents of the **Format** box will look in the grid view.

- 6 Click the **ToolTip Format** tab to define a tooltip.
- 7 Choose a target event attribute in the **Right-Click Field** menu to populate variable right-click commands, when applicable.
- 8 Click **Rename** or **Remove** to change or take away selected items in the **Custom Columns** list.
- 9 Click **Apply** to put your changes into effect and **Close** to close the Custom Columns Editor.

You can edit custom columns after they are created, including toggling on/off the "Share with all" settings for a column, renaming it, changing its Field Selector mappings, and so forth.



Custom columns are not available as arguments for inline filtering.



The Java Swing based browser supports basic HTML per the HTML 3.2 specification. Some more advanced tags may not be supported. For Technical Reports describing HTML 3.2, please refer to the World Wide Web Consortium (W3C) site at <http://www.w3.org/>. For information on HTML support in Java Swing, please refer to the Sun Developer Network at <http://java.sun.com/javase/reference/index.jsp>.

Showing a Custom Column

Once a custom column is created, it is available for use in the Console. Right-click the column header in a Viewer panel grid view and choose **Add/Replace Columns** to add the new column to a grid view. Custom columns show up in the Available Fields list under "Custom Column". (If a column is configured as "Share with all" it is available to all administrators. If not, it is available only to the user who created it.) For more information, see ["Adding, Replacing, or Removing a Column in the Grid View" on page 105](#).

Advanced Example: Creating a Custom Column with Velocity

Custom columns can display different contents based on external conditions. Use the Velocity template language to specify these conditions.

To create a custom column that displays a particular image when an event's target is in a specific Zone, create the custom column as described previously, but specify Velocity template-language script in place of the HTML format.

The code in the **Format** text box might look like this:

```
<HTML>

#if (($targetZoneUri.length()>0) &&

    ($targetZoneUri.startsWith("/All Zones/

    System Zones/Public Address Space Zones/

    Ford Motor Company")))

    <IMG src="file:///c:/fordlogo.gif" />

#end

</HTML>
```

Using Dashboards

Administrators can limit visibility of, or control access to, dashboards and data monitors by changing access control lists (ACLs) as needed. For more information on general use of ACLs on any resource, see [“Managing Permissions and Resources” on page 443](#).

With ACLs, administrators can also control which users are allowed to *deploy* (enable) or *un-deploy* (disable) a data monitor.

Monitoring Dashboards

Using dashboards to organize and present the events displayed by data monitors includes basic tasks such as loading dashboards and displaying dashboards; inspecting events; using zoom, slideshow or manipulating the views in various ways; working with dashboard layouts; saving dashboards, and so on.

Loading Dashboards

- 1 Choose **Views>Show Dashboard** to open the Load Dashboard dialog box.
- 2 Expand the dashboard groups to locate the dashboard(s) you want to include in your display.
- 3 Select the check boxes next to the dashboards you want to include.
- 4 When you've finished your selections, click **OK**.

Inspecting Events in Dashboards


You can investigate the events in a dashboard's data monitors by selecting and right-clicking those events and choosing **Show event details** (in LastNEvent data monitors) or **Show details** for all other data monitors. If you select events from a Last N Events data monitor, the details appear in the Event Inspector. If you select events from any other data monitor, a new Dashboard Drill-Down View opens in the Viewer panel for you to investigate.

Displaying Dashboards

In the Navigator panel's Dashboards resource tree, right-click a dashboard and choose **Show Dashboard**.

Rotating Dashboards Automatically

To automatically sequentially display all the dashboards present in the Viewer panel, choose **Views>Slideshow>Interval** in the Console's menu. Use **Interval** to set the number of seconds to pause on each dashboard, then choose **Views>Slideshow>Start**,

or use the toolbar button  , to begin rotation. Slideshows appear full-window. Also, **Tile Best Fit** is the best display choice in slideshow dashboards so all data monitors are visible. Use **Views>Slideshow>Stop**, or the toolbar button, to end a slideshow and return to the previous view.

Changing Dashboard Layouts

You can change a dashboard's layout simply by dragging and dropping data monitors into it. You can also click a data monitor's header and drag it to another location in a dashboard.

Using Dashboard Menu Options

Right-click a data monitor in a dashboard to use the **Dashboard** subcommands on its context menu. The nature of the data monitor determines which commands are applicable and enabled.

Zooming In or Out of Dashboards

In a data monitor within a dashboard, right-click and choose **Dashboard>Zoom In** or **Dashboard>Zoom Out**.

Fitting all Data Monitors within Dashboards

In a data monitor within a dashboard, right-click and choose **Dashboard>Fit in Dashboard**.

Saving Dashboard Layouts

In a dashboard, right-click and select **Save Dashboard**.

Closing a Dashboard

In a dashboard, right-click and select **Close Dashboard**.

Editing Dashboard Data Monitors

Right-click in the data monitor and choose **Data Monitor>Edit**.

Changing a Dashboard's Layout

Click the **Layout** button at the lower-right corner of the dashboard in the Viewer panel and choose a tab or tile option.

Managing Dashboards

Dashboards display a set of data monitors. When you create a new dashboard you can add new or existing data monitors to it.

Creating a Dashboard

In the Navigator panel's Dashboards resource tree, right-click and choose **New Dashboard**. Alternatively, drag an existing dashboard to a different group, choose **Copy** to copy the dashboard, and then rename it. Once you've created a new dashboard, you can populate it from the Data Monitors tab in the Dashboards resource tree, or create new ones.

- 1 On the Dashboards tab, right-click a dashboard group and choose **New Dashboard**.

An untitled dashboard appears in the Viewer panel and the Data Monitors tab automatically comes forward so you can choose monitors to add.

- 2 On the Data Monitors tab, navigate through the groups of existing data monitors to find ones you want to add to the dashboard.
- 3 Select a data monitor to add, right-click it and choose **Add to Dashboard As**. The format options are described below.
- 4 Repeat the above step to add other data monitors, as needed. When you've finished, right-click the dashboard in the Viewer panel and choose **Save Dashboard**.
- 5 In the Save As dialog box, navigate to a group and type in the **Name** text field.
- 6 Click **Ok**.

To add a data monitor to another dashboard, open that dashboard in the Viewer panel. Or, from the Data Monitors tab, right-click an existing Data Monitors group and choose **New Data Monitor**. After creating a new data monitor, you add it to the dashboard in the same way, with the **Add to Dashboards** option. See ["Using Data Monitors" on page 117](#) for more detail.

Adding a Data Monitor to a Dashboard

- 1 On the Dashboards tab, right-click a dashboard and choose **Show Dashboard**.
- 2 On the Data Monitors tab, right-click a data monitor and choose **Add to Dashboard As**, then choose an applicable display format. The format options are described below.
- 3 To save the updated dashboard, right-click it and choose **Save Dashboard**.

Data Monitor Display Formats

The display options available depend on the nature of the data monitor.

Display Format	Description
Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data.
Bar Chart Table	A grid of proportional bar elements.
Horizontal Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. This format forces the bars to run left-to-right rather than up-and-down.
Pie Chart	Shows data as a circle with proportional wedges for elements.
Statistics Chart	Displays Moving Average data monitors, especially those that contain and need to arrange (overlay) multiple graphs in one monitor space. Compare Statistics Chart to Tile, which arranges individual-graph monitors into fixed arrays.
Table	Displays data as a grid.
3D Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. The graph also has a third axis (depth) to display more data and can be rotated by dragging.
Tile	Arranges individual Moving Average data graphs into separate, fixed positions on a data monitor, when multiple graphs are present. Compare Tile to Statistics Chart, which displays multiple graphs (overlaid) in the same monitor space.

Editing a Dashboard

You edit dashboards by editing the data monitors within them as described in ["Using Data Monitors" on page 117](#).

Deleting a Dashboard

- 1 In the Dashboards tab of the Dashboards resource tree, right-click the dashboard's name and choose **Delete Dashboard**.
- 2 In the dialog box, click **Yes**.

Managing Dashboard Groups

The groups in the Dashboard tab of the Navigator panel's Dashboard resource tree store individual dashboards or other dashboard groups. You use groups within groups to help organize larger numbers of resources.

You can manage groups by drag-and-drop. You can move or copy dashboards or groups within the Dashboards resource tree. And deleting a group also deletes the resources it contained.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **New Group**.
- 2 Type a name in the group's text field.
- 3 Press **Enter**.

Renaming a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Rename**.
- 2 Type a name in the group's text field.
- 3 Press **Enter**.

Editing a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, navigate to a group and drag it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Using Data Monitors

You populate dashboards with *data monitors*, which you most often select from the Data Monitors resource tree in the Navigator panel (under Dashboards). However, when you need to use data monitors that aren't pre-defined, you need to be able to create, edit, and delete them.

Administrators can limit visibility of, or control access to, data monitors by changing access control lists (ACLs) as needed. For more information on general use of ACLs on any resource, see [“Managing Permissions and Resources” on page 443](#).

With ACLs, administrators can also control which users are allowed to *deploy* (enable) or *un-deploy* (disable) a data monitor.

Creating a Data Monitor

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor group and choose **New Data Monitor**.
- 2 In the Data Monitor Editor, select a **Data Monitor Type** from the drop-down menu. See [“Data Monitor Types” on page 120](#) for descriptions of each type. (See also, [“Data Monitors” on page 692](#) in the reference section of this guide.)
- 3 Based on the [Data Monitor Types](#) you've selected, specify values and options in the applicable fields to define the data monitor's data collection. Details on fields and appropriate values are given in the information about each data monitor type.



Depending on the permissions associated with the user group to which you belong, you may or may not have an option to **Enable** (*deploy*) or **Disable** (*un-deploy*) the data monitor. For more information, see [“Enabling or Disabling a Data Monitor” on page 118](#).

- 4 If the data monitor uses data fields for evaluation, you can use the Variables tab to create a new specialized field if necessary



The following data monitors support variables:

- Event graph
- Hierarchy Map
- Last N Events
- Last State
- Moving Average
- Statistics
- Top Value Counts (bucketized)

If you select a data monitor that does not support variables, the Variables tab is disabled.

- 5 Click **OK**.

To add the new monitor to the current dashboard, right-click it and choose **Add to Dashboard As**.

Editing a Data Monitor

- 1 Do either of the following to bring up the Data Monitor editor:
 - ◆ In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor and choose **Edit Data Monitor**.
 - ◆ If a Dashboard containing a given Data Monitor is already displayed, hover the cursor over that Data Monitor in the Viewer panel, right-click, and choose **Data Monitor > Edit**.
- 2 In the Data Monitor Editor, edit the applicable fields.
- 3 Click **OK** to save your changes and close the Data Monitor Editor. (Or click **Apply** to save the changes and leave the editor open.)

See ["Data Monitor Types" on page 120](#) and ["Data Monitors" on page 692](#) for field details on all data monitors.

Deleting a Data Monitor

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor and choose **Delete Data Monitor**.
- 2 In the dialog box, click **Yes**.

Enabling or Disabling a Data Monitor

When a data monitor is enabled (*deployed*) it is actively processing events and updating its display.

When you disable (undeploy) a data monitor, it stops processing events and updating its display. You might choose to disable a data monitor because it is not needed or should not be considered under certain circumstances.

Data monitors can be enabled at time of creation (see ["Creating a Data Monitor" on page 117](#)) or edited later to enable deployment.



Starting with ESM 4.5, data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions.

Depending on the permissions associated with the user group to which you belong, you may or may not have an option to **Enable** (*deploy*) or disable (*un-deploy*) the data monitor.

- Administrators (all users belonging to the `admin` group) have permissions to deploy/undeploy data monitors.
 - Administrators can grant permissions to deploy/undeploy data monitors to other non-Administrator users through the Access Control Lists (ACLs) editor. For more information, see ["Controlling Who Has Permissions to Deploy Data Monitors" on page 452](#), ["Managing Permissions and Resources" on page 443](#), and ["Granting or Removing Resource Permissions" on page 444](#).
-

Enabling or Disabling a Data Monitor from the Editor



Starting with ESM 4.5, you can set *operations* permissions on data monitor deployment by editing Access Control Lists (ACLs) on user groups. Administrators can allow or block user groups for data monitor deployment permissions. (This is different than controlling permissions on who has access to the data monitors *resource*.)

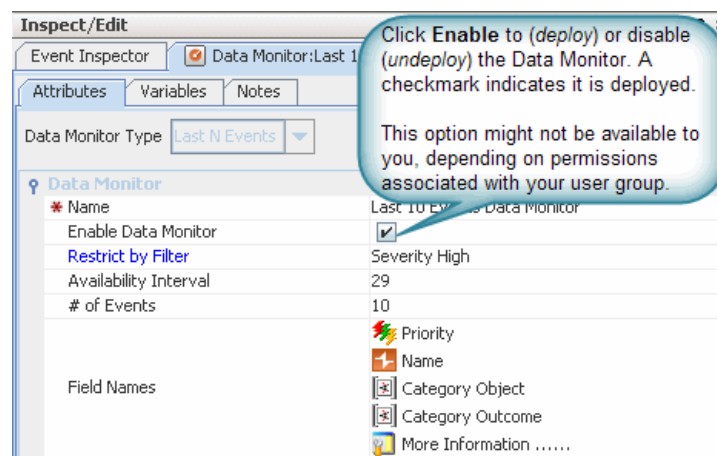
To set permissions for *deploying* data monitors, click the **Operations** tab, then click the **Add** button to get the Permissions Selector dialog for operations, select **Deploy** and click **OK**. For more information, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 452](#).

By default, only Administrators have permissions to enable and disable data monitors. Administrators can grant permissions to enable and disable data monitors to other non-Administrator users through the Access Control Lists (ACLs) editor. For more information, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 452](#).

If you have appropriate permissions, you can enable and disable data monitors in the Data Monitor Editor. (See [“Editing a Data Monitor” on page 118](#) for information on displaying the editor.)

In the Data Monitor Editor, click the checkbox for **Enable** to toggle the data monitor on or off. (Be sure to click Apply or OK on the editor to save your changes.)

- ◆ A checkmark indicates the data monitor is enabled/deployed.
- ◆ If the box is unchecked, the data monitor is disabled/undeployed.

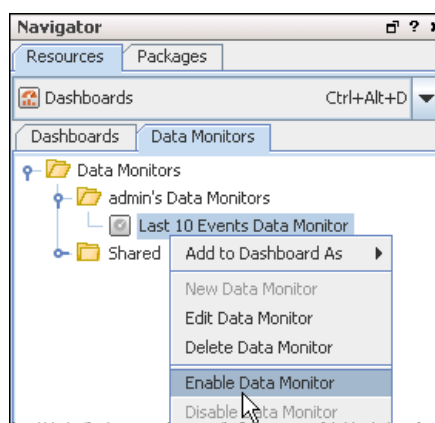


Enabling or Disabling a Data Monitor in the Navigator

You can also enable and disable data monitors in the Navigator by right-clicking data monitors or a data monitor groups.

- 1 In the Data Monitors tab of the Dashboards resource tree, right-click a data monitor or a data monitor group.

- 2 Choose **Enable Data Monitor** to *deploy* or activate the monitor(s) (if disabled) or **Disable Data Monitor** to *undeploy* or deactivate (if enabled).



For information about granting permissions to user groups to enable or disable data monitors, see [“Controlling Who Has Permissions to Deploy Data Monitors”](#) on page 452.

Overriding a Data Monitor's Last State

Last State data monitors can sometimes display a status that has served its purpose as soon as you have seen it. Once seen, you may want to directly reset or change the status so you can watch for a new status change, without waiting for an automatic system update.

When you see a status in a Last State data monitor that you want to reset, de-escalate, or otherwise override, right-click a cell in the monitor and choose **Override Status**. In the Select dialog box, select the new status and click **OK**.

Data Monitor Types

The ArcSight Console offers these predefined types to choose from when creating a new data monitor. Data monitor types are listed here with a quick glance description for each. For full detail on each type of data monitor, follow the links or cross-references to the associated topic in [“Data Monitors”](#) on page 692 in the reference section of this guide.

Table 7-6 Data Monitor Types

Data Monitor Type	Description
“Asset Category Count Data Monitor” on page 692	Enumerates the number of real-time hits (events) that occur per asset category, by priority, within a time interval.
“Event Correlation Data Monitor” on page 693	Provides flow-volume level correlation between two different event streams (based on two different specified filters).
“Event Graph Data Monitor” on page 694	Draws real-time diagrams of selected event activity. Automates the graphing of attacks in real-time. The <i>manual</i> operations are described in “Graphing Attacks” on page 125.

Data Monitor Type	Description
"Event Reconciliation Data Monitor" on page 695	Correlates events arriving from one sensor with events arriving from another sensor. When qualifying events occur on either or both sensors, this data monitor issues a new event to signal it. Useful in helping to determine the effectiveness of a firewall or IDS deployed in your environment.
"Geographic Event Graph Data Monitor" on page 698	Draws a real-time geographic map of selected events. In effect, it does automatically and in real-time what you can do manually, as described in "Graphing Attacks" on page 125 .
"Hierarchy Map Data Monitor" on page 699	Draws an image made up of proportionally sized panels where each panel represents a group of events selected by group fields selected in the source node identifier. A source-node criteria could be a combination of fields. Starting with ESM v.4.5, the Hierarchy Map data monitor includes several enhancements, as described in "Enhancements for ESM v.4.5" on page 699 in Hierarchy Map Data Monitor .
"Hourly Counts Data Monitor" on page 707	Displays the total count of events on an hourly basis along with their Priority.
"Last N Events Data Monitor" on page 708	Orders events based on a specified configuration. In the Table Viewer, the monitor displays the most recent events by Priority, Event Name, Protocol, and Category. With the BarChartTable configuration, the order is by Priority and Event Name. The PieChart configuration is ordered by Priority.
"Last State Data Monitor" on page 709	Provides an extra level of abstraction that you can use to simplify the information presented to operators. Sometimes called "indicator lights" or "heads-up displays," these monitors show graphics that translate more complex values into simple, rapidly observable results such as green/amber/red "signal lights" or checkmark/asterisk/exclamation point symbols. "Last State" data monitors could also be called "most recently known state" monitors.
"Moving Average Data Monitor" on page 710	Displays the moving average of events by a selected data field. The display provides a running count of events within a specified time frame and generates an event when the moving average changes significantly.

Data Monitor Type	Description
“Rules Partial Match Data Monitor” on page 713	Displays rules that have partial matches and the total number of partial match events within a specified time frame. For more information on partial matches, see “Creating Rule Actions” on page 310 .
“Session Reconciliation Data Monitor” on page 713	Correlates events on the basis of their occurrence within a relevant time period, as established by a "session" event.
“Statistics Data Monitor” on page 715	Provides a broader generalization of Moving Average data monitor functionality, except that it allows selection of other statistical methods in addition to Moving Average. Statistical methods include Average, Moving Average, Standard Deviation, Skew and Kurtosis, as well as Moving Average. These added capabilities could be used to detect anomalous behavior that could not be detected using moving average alone.
“System Monitor Data Monitor” on page 717	Provides measurements based on ArcSight Manager internal monitoring system Java classes and attributes. A number of system monitors that might be particularly useful to ArcSight administrators are provided as predefined System Data Monitors that you can include in your dashboard displays to monitor system performance.
“System Monitor Attribute Data Monitor” on page 718	Similar to System Monitor, except that, rather than providing measurements for all attributes of a specified Java class, focuses on a single specific attribute of a given ArcSight Java class. Used primarily for measurements on attributes that provide complex data structures.
“Top Value Counts Data Monitor” on page 718	Displays top events by selected data field, the total number of events, and the event Severity within the total number of events with the Table and BarChartTable viewer configurations.

Managing Data Monitor Groups

Data monitor groups store similar data monitors in a single location. You can create groups within groups to meet enterprise needs.

You can manage groups by drag-and-drop. You can move or copy dashboards or groups within the Dashboards resource tree. And deleting a group also deletes the resources it contained.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **New Group**.
- 2 Type a name in the text field.
- 3 Press **Enter**.

Renaming a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and select **Rename**.
- 2 Type a new name in the group's text field.
- 3 Press **Enter**.

Editing a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, navigate to a group and drag it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Enabling or Disabling Data Monitor Groups

Data monitors are enabled by default. When you disable data monitors they stop processing events and updating their displays. You might choose to disable a data monitor group because it is not needed or should not be considered under certain circumstances.

You can also enable and disable data monitors individually in the Data Monitor resource tree or Data Monitor Editor.

- 1 In the Data Monitors tab of the Dashboards resource tree, right-click a data monitor group.
- 2 Choose **Enable Data Monitor** to activate all the monitors in the group (if they are disabled) or **Disable Data Monitor** to deactivate them (if they are enabled).

Monitoring Active Lists

You can directly examine and modify the active lists available in the Navigator panel's Active Lists resource tree.

Viewing Active List Contents

- 1 Choose the Active List resource tree in the Navigator panel.
- 2 Right-click an active list and choose **Show Entries**.

Refreshing Active List Views

Active lists show results as of the time they opened for viewing, or the last time they were refreshed.

Click the **Refresh** button in the view header to update the contents.

Adding to or Subtracting from an Active List

You can conveniently add or remove event-attribute-based active list entries using selected events in active channel grid views. This feature automatically offers the name of the active list that is appropriate for the selected event.

- 1 In an active channel grid view, select an event that is relevant to an active list of interest.
- 2 Right-click the event and choose **Active List>Add to><active list>** or **Active List>Remove from><active list>**.



If an active list uses the Old File Size event attribute, note that the value required when adding an entry will be in bytes (not kilobytes or megabytes).

Filtering Active Lists

In addition to the constraints of an active list itself, you can place a temporary filter on an active list view to aid your analysis. Such filters are not saved with the active list.

- 1 Open an active list in the Viewer panel as described above.
- 2 Click the **Filter** status description in the view header to open the Common Condition Editor. For example, the status **No Filter Defined**.
- 3 Use the Common Condition Editor as described in [“Creating Filters” on page 147](#).

Editing Active Lists

You can change an active list's definition or simply add a new entry to its parameters.

- Right-click an active list in the Navigator panel and choose **Edit Active List** to open it in the Active List Editor. See [“Managing Active Lists” on page 385](#) to use the editor.
- Click the **Add Entry (+)** button in the active list view header to open the Add Entry editor which you use as described in [“Managing Active Lists” on page 385](#).

Clearing Active List Views

While monitoring a particular active list grid view, you may want to see only traffic that happens after a certain point in time. You can accomplish this by clearing the view.

- 1 In the Navigator panel's Active List resource tree, select the active list to clear.
- 2 Right-click and choose **Clear Entries**.

Customizing Active View Grid Columns

You can modify active list grid views just like other grid views, as described in [“Customizing Grid Columns” on page 111](#).

Active List Grid Context Menu Commands

You can also use a set of right-click context commands available in active list grid views.

Table 7-7 Active List Grid Context Menu Commands.

Menu Command	Description
New	Add an entry to the active list using the Active List Entry Editor.
Edit	Edit the selected entry using the Active List Entry Editor.
Delete	Remove the selected entry from the active list.

Graphing Attacks

You use graphic analytics to quickly identify high-volume attackers or targets at a glance. You can immediately locate and typify cascading attacks (e.g., worms and viruses), and rapidly isolate and analyze events involving interactions between two or more devices (e.g., threat discovery).

The event data you visualize can be **static** (a snapshot of the selected events) or **live** (continuously updated with specified real-time event data). You create static graphs by selecting certain event data out of a source and casting it as a graphic. You create live graphs using a graphic data monitor type.

See [“Changing User Preferences” on page 556](#) to set or change your event graph preferences.

Creating Static Event Graphs

- 1 Select an array of events in a grid, data monitor, or event inspector.
- 2 Right-click the selected set and choose **Event Graph** or **Geographic View**.

The Viewer panel displays the selected events in a new view, using the graphic or geographic styles described below.

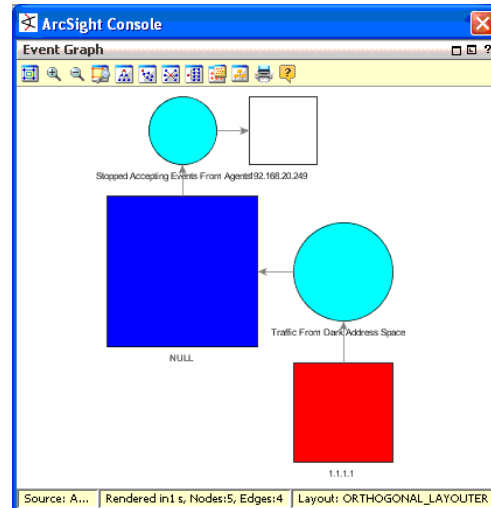


Figure 7-3 An Example Event Graph

Creating Live Event Graphs

- Select an Event Graph or Geographic Event Graph data monitor in the Dashboards tab of the Navigator panel's Dashboards resource tree. Right-click it and choose **Add to Dashboard As>Geographic Graph** or **Graph**.
- Alternatively, right-click your personal Data Monitors folder in the Navigator and choose **New Data Monitor**. In the Data Monitor Editor, in the Data Monitor Type drop-down list, choose **Event Graph** or **Geographic Event Graph**. Define the graphic data monitor in the usual way.

The Data Monitor Editor has certain attributes for these types.

Table 7-8 Event Graph Attributes

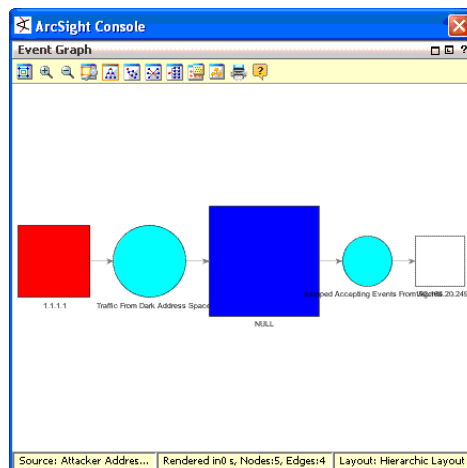
Attribute	Usage
Max Event Count	The number of most-recent events to show. Events older than this are discarded.
Event Node Identifier	The fields that are available to use to uniquely identify the event type in a transaction.
Availability Interval	The number of seconds for the interval between updates to the graphic.
Show Source-Target Nodes as	See "Changing User Preferences" on page 556 .
Source Node Identifier	See "Changing User Preferences" on page 556 .
Target Node Identifier	See "Changing User Preferences" on page 556 .
Show Event Nodes	See "Changing User Preferences" on page 556 .

Table 7-9 Geographic Event Graph Attributes

Attribute	Usage
Max Event Count	The number of most-recent events to show. Events older than this are discarded.
Availability Interval	The number of seconds for the interval between updates to the graphic.

Event Graph Notes

Link-analysis visualizations are chart-like or logically oriented. Geo-spatial visualizations are map-based or physically oriented. Node size indicates increasing event volume.

**Figure 7-4** Node sizes indicate relative event volume

Each event is composed of the event node itself (a turquoise circle) and its connected source node (red square) and target node (white square) device assets. The source and the target may be the same asset.

Blue squares indicate a combined source and target node (a "point event"). Pink nodes indicate IP addresses that are worm or virus infection sources for other nodes.

Point events occur on a single host; for example, a syslog entry for a running process. They graph as IP address nodes that loop to an event node and back.

In geo-spatial displays, source and target location plotting is based on the physical addresses registered for IP addresses. ArcSight includes standard plotting information for this purpose. The addresses are plotted against a world map that you can zoom in or out. All the specific location data that supports this feature also appears as attributes in the Event Inspector.

You can modify the way graphs plot events, choosing to keep the source-event-target visual relationships compact, or to emphasize unique sources, targets, or both in order to more easily clarify the nature of attacks or situations.

Pattern Discovery

You discover both normal and potentially threatening patterns of network activity through the same process of creating profiles, using those profiles to take snapshots of network

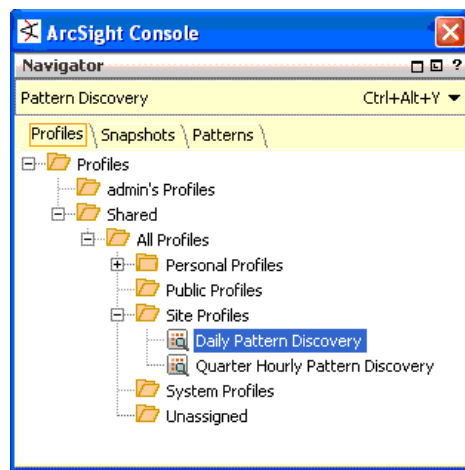
activity, and analyzing the patterns of activity captured in those snapshots. Along with these basic functions, you also need to be able to delete unwanted items and schedule activity.

It is important to point out that the goal of pattern discovery is to learn which patterns are benign, so you can apply ArcSight's capabilities to those that are not.

Creating a Profile

A profile is a set of constraints, similar to a filter, that determines which events from the overall stream will be examined for patterns, and on what basis. The profile is summarized in text at the top of the editor. You can change its details by editing the individual fields below.

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Profiles** tab.



- 3 Right-click a group in the resource tree and choose **New Profile**.

- 4 In the Profile Editor, click the **Attributes** tab and enter or choose the information necessary to define a new pattern-discovery profile, according to the “[Profile Properties](#)” on page 130.

ArcSight Console
Profile Editor : Daily Pattern Discovery

Attributes | Actions | Notes

Discover patterns having at least 3 elements and observed at least 4 times. Use events between \$Now - 1d and \$Now and filter events using the All Events filter. Use the event fields [Name] when searching for patterns.

Name	Value
Profile	
* Name	Daily Pattern Discovery
* Minimum Pattern Length	3
* Minimum Pattern Occurrences	4
* Start Time	\$Now - 1d
* End Time	\$Now
Events	
* Event Fields	Name
* Source	Source Address
* Target	Destination Address
Restrict by Filter	All Events
Advanced	
Record Time Order	<input type="checkbox"/>
Split On Inactivity	<input type="checkbox"/>
Discovery Results	
Snapshot Retention Time	\$CurrentDateTime + 7d
Snapshot Group	/All Snapshots/System Snapshots
Pattern Group	/All Patterns/System Patterns
Common	
External ID	
Alias	
Description	

OK Cancel Apply

- 5 Click the **Actions** tab to add actions that will trigger when new patterns are discovered (`OnNewPatternDiscovered`) or when old patterns are rediscovered (`OnPatternRediscovered`). See “[Creating Rule Actions](#)” on page 310 to learn how to use Actions tabs.
- 6 Click **Apply** to put your changes into effect and leave the editor open, or **OK** to apply the changes and close the editor.

You can also discover patterns directly from active channels. Right-click a channel in the Navigator panel and choose **Discover Patterns**.

As a matter of expertise, select the fields:

- **Record Time Order:** To retain statistics about the sequence of the events that make up patterns. Because event sequences can reveal intent, you can possibly detect and act upon certain kinds of activity even sooner.
- **Split on Inactivity:** To sensitize pattern discovery to potentially meaningful decreases in activity between duplicate source/target pairs. Sometimes what may otherwise seem to be one stream of activity isn't - and only its fluctuations can show this.



Be aware that using both of these options together usually increases the amount of memory required for efficient processing.

Editing a Profile

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Profiles** tab.
- 3 Right-click a profile in the resource tree and choose **Edit Profile**.
- 4 In the Profile Editor, click the **Attributes** tab and change the information necessary to modify the profile, according to the [“Profile Properties” on page 130](#).
- 5 Click **Apply** to put your changes into effect and leave the editor open, or **OK** to apply the changes and close the editor.

Deleting a Profile

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Profiles** tab.
- 3 Right-click a profile in the resource tree and choose **Delete Profile**.
- 4 Click **Yes** in the confirmation dialog box.

Profile Properties

Property	Usage
Summary	A profile summary appears just below the Attributes tab. The underlined items represent the contents of the Value fields below.
Name	The name given to the profile.
Minimum Pattern Length	The minimum number of unique associated events necessary to qualify that association as a pattern.
Minimum Pattern Occurrences	The minimum number of times that an event-association of the specified length has to reoccur in order to qualify it as a pattern.
Start and End Times	The event time-brackets for collecting snapshot contents. Click the fields to use the drop-down menu of timestamp expressions.
Event Fields	The event attributes that serve as common denominators for associating events. Use Ctrl+click to choose multiple fields.
Source	A field or set of fields that identify a pattern's source. The Source and Target specifications, combined, define a network transaction. Source and Target can share attributes but must differ in at least one.
Target	A field or set of fields that identify a pattern's destination. The Source and Target specifications, combined, define a network transaction. Source and Target can share attributes but must differ in at least one.
Restrict by Filter	Click this field to choose a filter from the Filters resource tree.

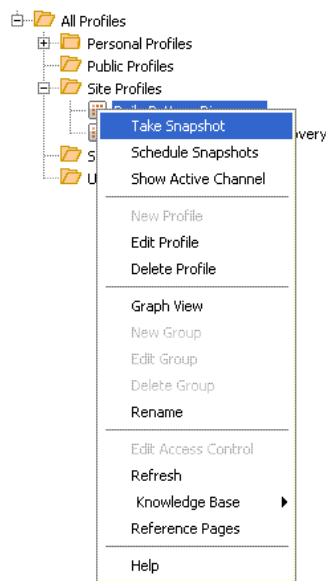
Property	Usage
Record Time Order	Select this check box to include the time sequence of the events contained in patterns. For example, for a three-event pattern, it could record that A-B-C occurred 40%, B-A-C 35%, and A-C-B 25%.
Split on Inactivity	Select this check box to cause a pause or significant drop in the volume of a particular pattern to be treated as a break, meaning that the flows of the pattern on either side of the break are treated as separate occurrences.
Snapshot Retention Time	Choose a time expression from the list, or enter one manually, to set how long snapshots remain in the resource tree.
Snapshot Group	Choose a group in the Snapshot resource tree in which to store the resulting snapshots.
Pattern Group	Choose a group in the Patterns resource tree in which to store the resulting patterns.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. Your ArcSight administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight. A given alias will appear in place of the resource's name everywhere it may be seen. Your ArcSight administrator can advise you on the correct values for this field, if applicable.
Description	A text description of the profile.
Owner	The ArcSight user with responsibility for the profile.
Notification Groups	The ArcSight user group(s) to notify concerning changes to a profile.

Taking a Snapshot

You use profiles to generate snapshots, which are records of qualifying event activity. Generating a snapshot manually is called "taking a snapshot." You can also schedule snapshots, which is described next.

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Profiles** tab.
- 3 Right-click a profile in the resource tree and choose **Take Snapshot**.

You can also take snapshots directly from active channels in the resource tree. Right-click a channel and choose **Discover Patterns**. ArcSight takes a snapshot of the channel's current contents and examines it for patterns. You see the snapshot in the Viewer panel and the profile that generated the pattern appears in your personal folder in the Pattern Discovery resource tree.



- 4 When the snapshot's graphic has formed in the Viewer panel, you can click the icons at the top of the view to change its layout as described in [“Visualizing Resources” on page 537](#). You can also right-click the pattern-component graphics for the event hierarchy (above) and complete pattern (below), and use the [Pattern Options](#) or buttons.

See also, [“Scheduling a Snapshot” on page 133](#), [“Showing a Snapshot” on page 133](#), [“Deleting a Snapshot” on page 133](#), and [“Exploring a Snapshot” on page 133](#).

Pattern Options

You use these options to analyze and respond to the patterns you discover in snapshots.

Table 7-10 Pattern Options

Option	Usage
Create Rule	Use the Rules Editor to create a rule that responds to the combination of events represented by the complete pattern or selected event-level in the pattern hierarchy. The Conditions tab is automatically populated with the applicable statements.
Show Related Events	Open a new channel filtered with a matchesPattern operator that uses the contents of the complete pattern, or selected event-level in the pattern hierarchy, as its argument.
Show Event Graph	Graph the complete pattern for analysis, or a selected event-level in the pattern hierarchy, using the ArcSight Console's visualization tools.
Inspect Pattern	Open the pattern in the Pattern Inspector where you can examine its details, rename it, or click the Actions button to apply the options described in this table.
Investigate	Choose to create an active channel, or add a filter condition to the editor, using (or not using) the name of the selected event item in the pattern.

Option	Usage
Tools	Choose one of the network tools ArcSight provides to explore the origin of the selected event item.
Annotate Pattern	Use the Annotations dialog box to mark the pattern with a workflow collaboration Stage and Assign to ArcSight user so it can be filtered using Stages and Users resources.

Scheduling a Snapshot

The frequency and timing you choose for snapshot schedules can be an important analysis factor.

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Profiles** tab.
- 3 Right-click a profile in the resource tree and choose **Schedule Snapshot**.
- 4 In the Scheduled Task Editor, click the space labeled **Click here for a new schedule** or the **Add a New Schedule** button.
- 5 Click the schedule-building buttons in sequence from left to right, to provide specific timing information. These buttons are described in [“Scheduling Jobs” on page 756](#).
- 6 Repeat Step 4 to add another schedule for the same snapshot.
- 7 Click **OK**.

Showing a Snapshot

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Snapshots** tab.
- 3 Right-click a snapshot in the resource tree and choose **Show Snapshot**.
- 4 When the snapshot's graphic has formed in the Viewer panel, you can click the icons at the top of the view to change its layout as described in [“Visualizing Resources” on page 537](#). You can also right-click the pattern-component graphics for the event hierarchy (above) and complete pattern (below), and use the [Pattern Options](#) or buttons.

Deleting a Snapshot

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Snapshots** tab.
- 3 Right-click a snapshot in the resource tree and choose **Delete Snapshot**.
- 4 Click **Yes** to confirm the deletion.

Exploring a Snapshot

Whether you produce them manually ([“Taking a Snapshot” on page 131](#)) or by schedule ([“Scheduling a Snapshot” on page 133](#)), each snapshot is a picture of the transactionally related events that appeared within the scope of a given profile. Once graphed in the Viewer panel, there are several ways to manipulate a presentation to better understand its significance, but first you need to know how the Viewer panel makes this data available.

The Viewer panel presents snapshots as a two-pane window. The upper pane shows the overall pattern tree (or set of trees) captured by the profile. This is called the **tree view**. The lower pane is called the **tilde view** and shows individual patterns.

Each pattern (block of items) in the lower pane represents one pattern tree, or one specific path through a pattern tree.

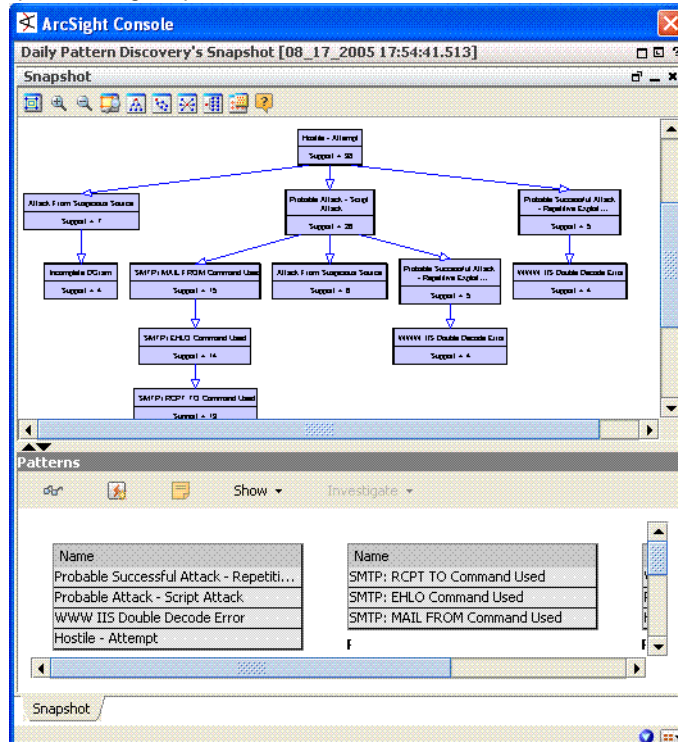


Figure 7-5 A pattern snapshot in the Viewer panel

The tiled view, by default, shows all the patterns in the tree view. Once you select a pattern item in the tree, however, the tiled view shows just the pattern or patterns that include that item. The higher the item you select on the tree, the more patterns its path is likely to include.

The tree view structures its items on the basis of transactional relationships, and descending degrees of support for the pattern through various paths of transactional relationships (specific patterns).

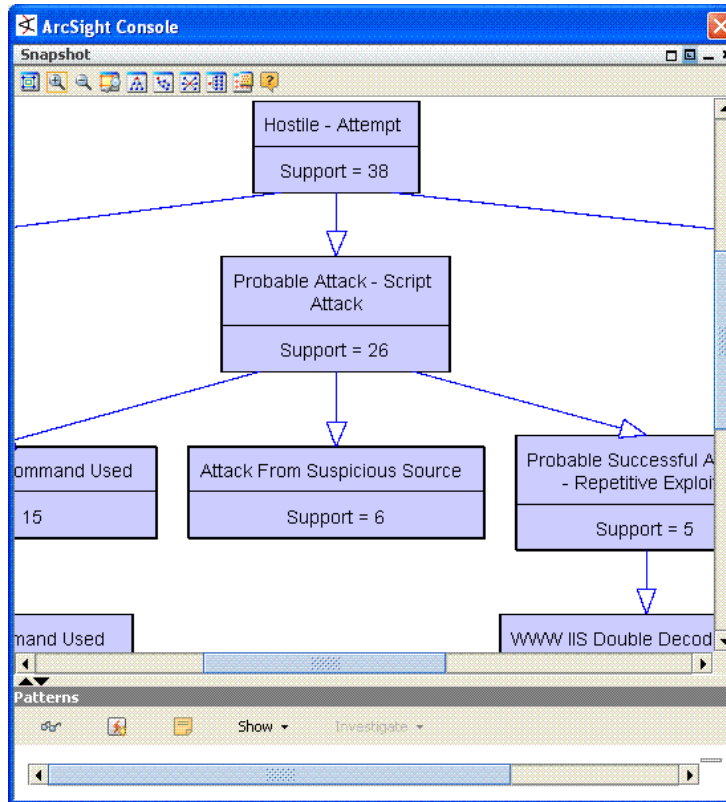


Figure 7-6 Zoom-in on snapshot tree view

Trees are arranged in nodes of decreasing support. Note in the graphic above that the highlighted item at the bottom of the tree represents a subset of support (6) compared to the most-supported item at the top of the tree (71). Sharp differences in support from one item to the next (e.g., from 36 to 6) are automatically treated as demarcation points in the tree.

In a snapshot's **tree view** you can:

- 1 Select individual items to see their associated patterns in the tiled view.
- 2 Drag individual items around graphically to better see or evaluate their relationships.
- 3 Right-click an item and use the **Create Rule** or **Show Event Graph** commands to build rules or event graphs based on the item's pattern (described further below).
- 4 Click the graphic control buttons in the snapshot's toolbar to adjust the contents of the tree view.

Inspecting a Pattern

The Pattern Inspector details the **Items** that make up the pattern, the source/destination pairs of Transactions that the item sets appeared in, and lists the **Snapshots** the pattern appears in, so you can readily flip between them for comparison.

You can also click the **Actions** button to use any of the pattern commands from the Pattern Inspector.

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Patterns** tab.
- 3 Right-click a pattern in the resource tree and choose **Inspect Pattern**.
- 4 In the Pattern Inspector, examine the pattern's details, rename it, or click the **Actions** button to apply the options described in the Pattern Options table above.

Creating Rules

The Rules Editor opens with the pattern's items already loaded in the **Conditions** tab.

You can modify the conditions, then click the **Actions** tab, where you specify the exact response to the appearance of the pattern.



The OR conditions are intentional and should be left in place. The Rules engine uses OR as a much more memory-efficient way to process rules than AND. It can do so because it also applies a threshold value (the number of items involved) and distinct item names to track the components of the rule, rather than a blanket (join) approach.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See ["Velocity Templates" on page 793.](#))

Always review the aggregation parameters for the rule; especially the **Time Frame** because the default value is unlikely to be appropriate.

Showing Event Graphs

When you show an event graph, you see a representation shaped by the currently selected level in the pattern hierarchy.

You can drag elements to make relationships more clear. Use the **Cluster similar selected nodes** and **Uncluster similar selected nodes** right-click commands to group or break out activity details for further analysis.

Showing Related Events

This command opens a new active channel, filtered with a `matchesPattern` operator that uses the contents of the complete pattern, or selected event-level in the pattern hierarchy, as its argument.

Here you can apply all the manipulation, filtering, selection, and inspection tools that ArcSight Console grid views offer, to pursue your analysis.

Note that the automatically generated view filter is customized get the right set of events with the greatest efficiency.

Annotating Patterns

You can choose to annotate a pattern to place it in, or move it further along, an analysis workflow.

Marking the pattern with a workflow collaboration **Stage**, and an **Assign** to ArcSight user, makes it subject to Stages and Users resources filtering.

Viewing a Pattern

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Patterns** tab.
- 3 Right-click a pattern in the resource tree and choose **View Pattern**.
- 4 When the pattern's graphic has formed in the Viewer panel, you can right-click it and choose **Inspect** to examine it more closely in the Pattern Inspector.

Viewing a Filtered Pattern

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Patterns** tab.
- 3 Right-click a pattern in the resource tree and choose **View Patterns with Filter**.
- 4 In the Filter Patterns dialog box, choose a **User** and/or **Stage** resource to confine the pattern's results.
- 5 When the pattern's graphic has formed in the Viewer panel, you can right-click it and choose **Inspect** to examine it more closely in the Pattern Inspector.

Deleting a Pattern

- 1 Choose the Pattern Discovery resource tree in the Navigator panel.
- 2 Click the **Patterns** tab.
- 3 Select one or more patterns.
- 4 Right-click the selected pattern(s) in the resource tree and choose **Delete Pattern(s)**.
- 5 Click **Yes** to confirm the deletion.

Chapter 8

Selecting and Investigating Events

This chapter describes how you use ArcSight to monitor enterprise security.

[“Handling Events in Grid Views” on page 139](#)

[“Showing Event Details and Rule Chains” on page 140](#)

[“Investigating Session Events” on page 141](#)

[“Collaborating on Events” on page 141](#)

[“Showing Event Payloads” on page 145](#)

[“Getting Knowledge Base Articles” on page 146](#)

Handling Events in Grid Views

In active channel or active list grid views you can select events to investigate. After selecting one or more events in a grid, you can handle them in several basic ways. This handling is in support of other analysis and authoring tasks.

Selecting Events to Investigate in a Grid View

Within a Viewer panel grid view, click an event or **Ctrl+click** a set of events. To select a range of events, click one event and **Shift+click** the event at the end of the range.

Inverting Event Selections in a Grid View

Select one or more events in a grid view, right-click and choose **Invert selection**.

Selecting Events with Matching Cells in a Grid View

Select a cell in a grid view, right-click and choose **Select events with matching cell** to see if other events in the grid view have matching cell values.

Exporting Data Fields to a .CSV File

- 1 In a grid view, select one or more events.
- 2 Right-click and choose **Export**, then **CSV - Visible Columns** or **CSV - All Columns**.



Always choose **visible columns** rather than **all columns**, unless you have a pressing need to export everything. Because the total number of columns is often very large, exporting all could be time- and resource-consuming.

- 3 In the Save dialog box, navigate to a directory and enter a value in the **File name** text field.
- 4 Click **Save**.

Showing Event Details and Rule Chains

Displaying Event Details

In a grid view, select an event. Right-click and choose **Show event details**. The event's details appear in the Event Inspector.




If you encounter an "unable to retrieve event" message while viewing events in the Events tab of the Case Editor, be advised that those events are unavailable because they are archived in an offline partition.

Displaying Simple Event Rule Chains

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Simple chain**.

Displaying Detailed Event Rule Chains

Rule-based Correlation events are those generated by a triggered ArcSight rule as a reaction to an original sensor-generated event. In other words, an event concerning an

event. You recognize correlation events in grid views by their red **Flash** icon . To mask grid views so they show **only** correlation events, select the check box at the top of the grid's left most column.

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Detailed chain**.

The events leading up to the correlation event appear in the Description panel at the top of the Inspector. Click any event in the chain to see its details below.

Displaying Correlation-Event Rules

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Show triggering resource**.

The rule or resource that triggered the correlation event is selected in the Navigator panel's Rules resource tree and that rule appears in the Rules Editor.

Executing or Clearing Rule Actions in a Grid View

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Clear Rule Actions** to clear all actions associated with this rule. For more information, see ["Creating Rule Actions" on page 310](#).

Launching Event Details in a Browser

- 1 In a grid view, right-click an event and choose **Show event details**.
- 2 In the condition table of the Event Inspector, right-click and choose **Launch Event Details in Browser**.

A Web browser opens with the selected event's details.

Hiding Empty Rows in the Event Inspector

- 1 In a grid view, right-click an event and choose **Show event details**.
- 2 In the condition table of the Event Inspector, right-click and choose **Hide Empty Rows**.

Investigating Session Events

This topic explains how to use the Console's **Investigate > Session Events** command to easily refine and explore channels contextually, using attributes of the events already being displayed in grid views.

Session List entries can be investigated two ways: you can filter the set of entries based on the attributes of a particular entry, or you can create an Investigation Channel that contains only the entries that match one or more attributes of the initial Session List entry.

Investigating a Session Event

- 1 Right-click a Session List in the Navigator and choose **Show Entries**.
- 2 In the Viewer panel, select an entry that bears investigation by clicking on it.
- 3 Right-click the selected entry. The menu includes commands to **Create Channel** and **Add Condition to Channel Editor**. The details of each command will vary based on which column you right-click.

For example, if you right-click a Source IP column containing the value [192.168.10.0](#), the choices will be:

- ◆ Create Channel (Source IP = 192.168.10.0)
- ◆ Create Channel (Source IP != 192.168.10.0)
- ◆ Create Channel >
- ◆ Add Condition to Channel Editor (Source IP = 192.168.10.0)
- ◆ Add Condition to Channel Editor (Source IP != 192.168.10.0)
- ◆ Add Condition to Channel Editor >

The sub-menus (indicated by the >) will offer similar choices for all the other columns of the Session List entry.

If you Create Channel, a new grid is added to the Viewer panel. If you Add Condition to Channel Editor, a channel editor will open in the Inspect/Edit panel.

For more information about creating and using views for investigation, see [“Investigating Views” on page 98](#).

Collaborating on Events

You can use workflow-style annotation to collaborate with other users in analyzing or reviewing selected events. (See also [“Case Management and Queries” on page 397](#).)

When you are annotating, you can make collaboration-stage changes to just the event you originally selected, or have that change also affect a larger set of similar events that should also be carried forward in the review process.

The central tasks in annotating events for collaborative analysis are assigning them to yourself or another user, then assigning them to one of the available sequential workflow stages (dispositions). While ArcSight comes with a default set of stages, your enterprise will very likely have edited these stages and created new ones.

Compare collaborative annotation to cases, which are a more formal way to track sets of events that are under investigation.

Viewing Annotations for an Event

Annotations on an event are displayed in the **Annotations** tab of the Event Inspector when that event is selected.

To view the annotations for an event:

- 1 Right-click an event in a grid view (such as an active channel or active list) and choose Show Event Details to bring up the Event Inspector.
- 2 In the Event Inspector, click the **Annotations** tab.

Annotating an Event

- 1 Select one or more events in any grid view. If not already annotated, you can start a collaboration cycle.
- 2 Right-click the events and choose **Annotate Events** (or **Ctrl+T** keyboard command).
- 3 In the Annotate Events dialog box, set or change the events' Annotations fields, as described below.
- 4 To have this change also affect related events, use the **Mark Similar Events** fields, as described below.
- 5 Click **OK** to update the event.

Event Annotation Fields

Event Annotation Field	Usage
Stage	Click this field to choose a different disposition state for the events' collaboration cycle. The default stages run from Initial to Closed ; other stages may be available.
Assign to	Click this field to choose an ArcSight user to take the next step.
In Case	This read-only field tells you whether or not these events are already part of an ArcSight case. If they are, you have more ways to track their disposition.
Correlated	This read-only field tells you whether or not these events are part of a correlated event chain. If so, you can learn more through the rules authored to control that chain of correlation.
Hidden	This read-only field tells you whether or not these events are hidden from all but the assigned user(s) of this stage.
Closed	This read-only field tells you whether or not the investigation of these events has been marked as closed. Closed events may no longer be visible to interested parties through active channels, etc.

Comments Field

The **Comments** field is for text comments you can add as needed to clarify the collaborative process.

Mark Similar Events Fields

Event "similarity," for collaboration purposes, is defined as a combination of time constraints and having certain key event attributes in common. For example, you could apply a collaboration change to additional events received in the future on the basis of those events having the same Attacker value and having occurred within the last two days.

Similarity Field	Usage
Time Constraints	Choose a bracketing combination of Start Time and End Time or Duration.
Start Time	Date and time values to set the beginning of a time-constraint window. Choose from the drop-down menu of expressions or click the ellipsis button to set exact times.
End Time	Date and time values to set the end of a time-constraint window. Choose from the drop-down menu of expressions or click the ellipsis button to set exact times.
Duration	The length of the time window, relative to a Start Time or End Time, when using Duration as a time constraint.
Criteria	A menu of key event-attribute characteristics you can use to define similarity. The text box below specifies the criteria being set.

Creating New Stages


- 1 Choose the **Stages** resource tree in the Navigator panel.
- 2 Right-click the **All Stages** group and choose **New Stage**.
- 3 In the Stage Editor, enter a name for the stage.
- 4 Make other appropriate choices, as described in the following table showing [Stage Editor Fields](#).
- 5 Click **Apply** to save your changes and keep the editor open, or click **OK** to save and close.



Please keep stages provided as standard content in the given folders and do not move them into another folder. (See ["What is Standard Content?" on page 9](#).) Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.

Stage Editor Fields

Stage Editor Field	Usage
Subsequent stages	Select one or more stages to set as follow-on stages to this one. Events in this stage will show these other stages as options in the Stage field of the Annotate Fields dialog box.

Stage Editor Field	Usage
User required	Select whether you want to prompt for a user assignment when assigning this stage. If you don't prompt for a different user, or no change is made, the current user remains in effect.
Comment required	Select whether you want to require users to add a comment when assigning this stage.
Can be skipped	Select whether this stage can be bypassed when assigning from one stage to the next.
Mark similar required	Choose whether you want events that are similar to the selected events to be automatically assigned to this stage. Similarity is scoped at assignment time through the Mark Similar Events fields of the Annotate Events dialog box you see when you choose Annotate in a grid view. Note that similarity marking applies only to subsequent events received in the future. Events already processed are not affected.
Mark similar stage	Select whether you want to use this stage as a routing mechanism for other stages in a workflow. When selected, assigning one or more events to this stage causes all following (subsequent) similar events to be automatically redirected to the chosen stage. Events already processed are not affected. Similarity is scoped at assignment time through the Mark Similar Events fields of the Annotate Events dialog box you see when you choose Annotate in a grid view.
Hidden	Select whether you want events assigned to this stage to be hidden from all but the assigned users (True), left visible to everyone (False), or to leave the current visibility unchanged (Ignore).
Closed	Select whether you want events assigned to this stage to be marked as closed to investigation (True), not marked as closed (False), or left in their previous state (Ignore).
 With the assistance of ArcSight Professional Services, you can customize the similarity criteria selector for Mark Similar events. In this way you can have conditions that are different from the defaults. This is done with the Velocity scripting language, by modifying certain Velocity templates present on the Console, in the config/similarity directory. Ask your ArcSight administrator for more information or to make a request of ArcSight Professional Services.	

Editing Stages

- 1 Choose the **Stages** resource tree in the Navigator panel.
- 2 Right-click a stage under the **All Stages** group and choose **Edit Stage**.
- 3 In the Stage Editor, make any necessary changes to the fields as previously described in [Stage Editor Fields](#).
- 4 Click **Apply** to save your changes and keep the editor open, or click **OK** to save and close.




Please keep stages provided as standard content in the given folders and do not move them into another folder. (See [“What is Standard Content?”](#) on [page 9](#).) Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.

Showing Event Payloads

An event “payload” is the information carried in the body of the event's network packet, as distinct from the packet's header data. From the Console, you can search, retrieve, view, save to a file, or discard event payloads.

Finding Payloads

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view.

- 1 In a grid view, right-click a column header and choose **Add Column>Device>Payload ID**.
- 2 Look for events showing a Payload ID  in that column.

Retrieving Payloads

- 1 In a Viewer panel grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Retrieve Payload**.

Preserving Payloads

You can select to preserve the payload for an event in either of two ways:

- In a grid view, right-click an event with an associated payload, choose **Payload**, then **Preserve**.
- Or
- In the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discarding Payloads

In a grid view, right-click an event with an associated payload and choose **Payload**, then **Discard Preserved**.

You can also use the Event Inspector.

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Discard Preserved Payload**.

Saving Payloads to Files

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Save Payload**.
- 4 In the Save dialog box, navigate to a directory and enter a name in the **File name** text field.
- 5 Click **Save**.

Viewing Payloads in Other Viewers

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Launch External Payload Viewer**.
- 4 View the payload using the **Preferred Payload Viewer** and **Text to PCAP Converter**, specified in the Console's **Edit>Preferences>Programs** panel.

Getting Knowledge Base Articles

Knowledge Base articles can be associated with events, rules, or any ArcSight resource. Knowledge Base articles can have links or notes to help you respond to events.

Displaying Articles from the Knowledge Base Window

In the Navigator panel drop-down menu, select **Knowledge Base**. Navigate to and right-click an article, and choose **Show Article**.

You can also choose **Knowledge Base** from the **Help** menu.

Displaying Articles from a Grid View

In a grid view, right-click an event and choose **Knowledge Base**, then **Show**. Choose **KB entry for cell**, **KB entry for row**, or **KB entry for column**, then the article name.

The Knowledge Base article opens in an [ArcSight Web](#) client. For more information about grid views, see [“Using Grids” on page 105](#).

Displaying Articles from the Event Inspector

In the Event Inspector, right-click an event and choose **Knowledge Base**, then **Show Article**.

The Knowledge Base article opens in an ArcSight Web client.

Chapter 9

Filtering Events

This topic describes how you use ArcSight to monitor enterprise security.

[“Creating Filters” on page 147](#)

[“Debugging Filters to Match Events” on page 151](#)

[“Applying Filters” on page 155](#)

[“Investigating Views” on page 156](#)

[“Modifying Views” on page 159](#)

You can create and edit filters and inline filters for use in active channels.



For more details on managing and using filters, *see also* [“Managing Filters” on page 480](#), which includes additional topics on:

- [“Editing a Filter” on page 480](#)
- [“Importing and Exporting filters” on page 481](#)
- [“Moving or Copying Filters” on page 481](#)
- [“Deleting Filters” on page 481](#)
- [“Creating Filter Groups” on page 481](#)
- [“Renaming Filter Groups” on page 481](#)
- [“Editing Filter Groups” on page 482](#)
- [“Moving or Copying Filter Groups” on page 482](#)
- [“Deleting Filter Groups” on page 482](#)

Some of these tasks require with administrative privileges.

Creating Filters

This topic discusses creating and editing filter resources through the Filter Editor. As a matter of efficient authoring and enterprise-wide analysis consistency you should always seek to use the established filter resources you find in the Navigator panel's Filters resource tree. These filters should have been designed and tested to appropriately accomplish your organization's analytical goals.

As of v4.0, Inline filters offers you a user-friendly visual representation of Boolean logic, typically found in the [Common Conditions Editor](#). The inline filters feature allows you to preview matching events through highlighting, thereby verifying the accuracy of your filter prior to applying it, and the ability to create AND/OR conditions effortlessly.

Creating a New Filter

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a group and choose **New Filter**.
- 3 In the Filters Editor, type in the **Name** text field.
- 4 In the table, scroll to a relevant event field and choose a logical operator (**Op**), enter a conditional statement (**Condition**), select case-sensitivity (**Aa**), and select inequality or negate (**Not**), if appropriate.
- 5 Customize the filter, if appropriate, using the features described in [“Common Conditions Editor” on page 616](#).
- 6 Repeat the above step for each condition you want to add to the filter.
- 7 Click **Apply** below the Inspect/Edit panel to update the filter or click **OK** to add the filter to the resource tree.



Filter definitions (meaning the total text used in a filter's condition statements) cannot exceed 10,000 characters. If your filter uses more than 10,000 characters, create a second filter by splitting the definition, and use the **matchesFilter** operator to combine the two.



Because you can reference filters in other filters you can create hierarchies similar to style sheets. It is wise to plan your filtering needs in advance so you can create filters, filter groups, and filter hierarchies that will promote the most efficient and consistent analysis results.

Changing a Filter

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a filter and choose **Edit Filter**.
- 3 Make changes to the filter's conditions as described in [“Common Conditions Editor” on page 616](#).
- 4 Click **Apply** in the Inspect/Edit panel to put the modified filter into effect or **OK** to save the changes in the resource tree.



Be cautious when making changes to filters used in hierarchies.

Creating an Inline Filter



Steps to create an inline filter are summarized here. For more details and examples, see also [“Filtering Grid Views with Inline Filters” on page 109](#).

In any active channel grid view you can use the fields of the grid's top line to select filtering event-attribute values for certain columns, which will be used with implied AND operators to impose *ad hoc* filters and use the grid's bottom line to select filtering event-attributes values which will use OR operators.

These filters are **not** retained with the prior active channel, but you can give the revised channel a name and save it through the Active Channel Editor.



You cannot select a grayed-out column to include in your filter. Grayed-out columns have either variables or they are a custom column.

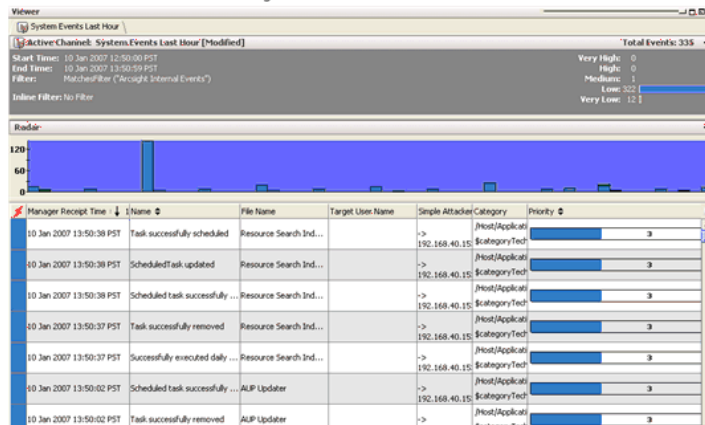
- 1 In the Navigator panel, choose **Active Channels**.
- 2 In the Active Channels resource tree, select a channel you want to add an inline filter.
- 3 In the Viewer panel, go to **Inline Filter** and click **No Filter**. This opens the inline filter pane.
- 4 Select the parameters for your inline filter: Manager Receipt, Name, Attacker, Target Address, Target Port, Priority, Device Vendor, and Device Product. Click **Apply**.
- 5 To highlight all matching events for your filter, select the **Highlight** checkbox. Highlighting allows you to preview the events that match your filter prior to saving the filter. Click **Apply** to activate the inline filter.

You can specify the highlight color by clicking the drop-down picker and select your color.

- 6 To add or delete rows to the inline filter table, click + (plus) or click - (minus).

To create and manage multiple inline filters, click the + button next to the Highlight options under the inline filters to add filter definition rows. (Click the - button to remove filter rows.) The potential uses of multiple inline filters are extensive, but essentially this provides a means of creating a filter with complex conditions, inline in an active channel. For example, in the Name column for an event, you could specify that the event name contains "ActiveList" on the first filter row and that the name does not contain "Successful". You could extend this filter by specifying what you are looking for in some of the other fields or even add more qualifiers on the Name field. All fields can be narrowed down in this way, using multiple filter definition rows.

To add an inline filter, click the **Edit Inline Filter** button to the right of the viewer above the event grid.



Clicking the **Edit Inline Filter** button opens an inline filtering window. Type a value in one or more fields to further filter the event stream. In this example, we add an inline filter on the Priority field to specify showing only events of Priority 3. Click **Apply** to apply the inline filter.

Also, you can click the + button to add filter definition rows and create multiple inline filters. Click the - button to remove rows.

The screenshot shows the inline filtering window. It has a table with columns: Manager Receipt Time, Name, File Name, Target User Name, Simple Attacker Category, and Priority. The 'Priority' column has a dropdown menu open, showing 'Priority = 3'. Below the table is a 'Highlight' checkbox and buttons for '+', '-', 'Apply', 'Cancel', 'Clear', and 'Help'.

When you click into a field, you get an equals operator, a drop-down list of available values for that field based on the events currently displayed, and an ellipsis (...) indicating another dialog is available.

If these inline options are not enough to create the filter, click the ellipsis (...)

to bring up a Conditions Editor dialog in which to create the filter for the selected field.

The screenshot shows the Conditions Editor dialog. It has a table with columns: Name, Op, and Condition. The 'Name' column has a dropdown menu open, showing 'Name'. The 'Op' column has a dropdown menu open, showing 'Equals'. The 'Condition' column has a text input field. Below the table are buttons for 'OK', 'Cancel', and 'Help'.

Debugging Filters to Match Events

Starting with ESM v.4.5, you can use a filter debugger to test whether a selected filter matches a certain type of event and, if there are mis-matches, to determine which filter conditions are not matching the event details.

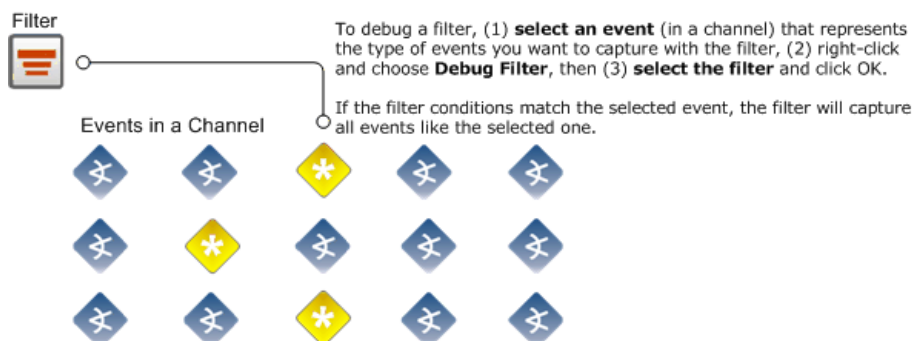


Figure 9-1 Debugging a Filter. On an Active Channel, select the kind of event you want to capture and test (debug) your filter against it.

The new debug filter utility is available as a right-click option on an event in an active channel. The filter debugger compares the conditions in a selected filter with the metadata that describes the selected event to determine whether the filter would capture such events. The filter definition is displayed to show the results of this comparison.

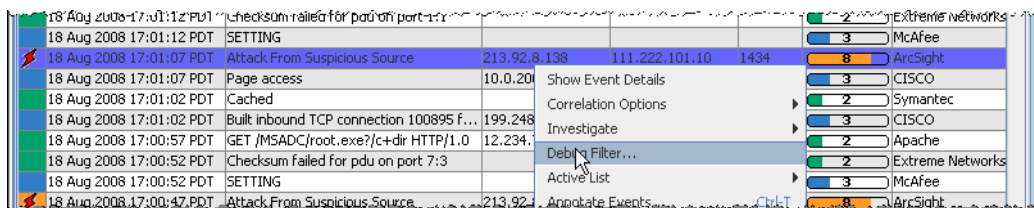
- If the selected filter matches the event, the filter definition shows no errors or mis-matches.
- If the filter does not match the event, the filter definition highlights the mis-matches between the filter conditions and the selected event with red-highlighted X's.



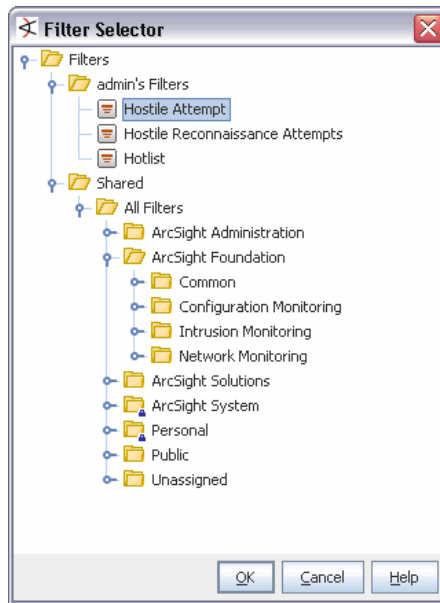
The display of red highlighted X's in a filter as a result of filter debugging on an event *do not necessarily indicate* that the filter is *invalid*. Red highlights are shown here only to highlight where the selected filter does not match the selected event.

To debug a filter against an event:

- 1 Select an event in the viewer in an active channel against which you want to test a filter.
- 2 Right-click and choose **Debug Filter** from the context menu.

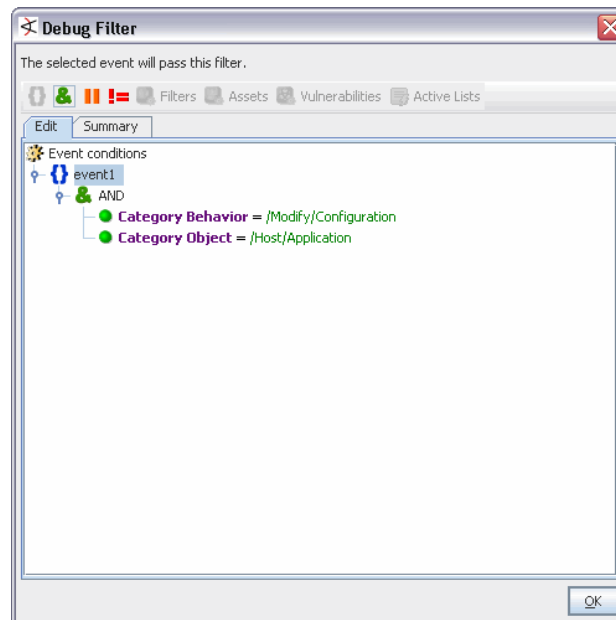


- 3 In the filter selector dialog, navigate to and select the filter you want to test.



The filter definition is displayed in its editor.

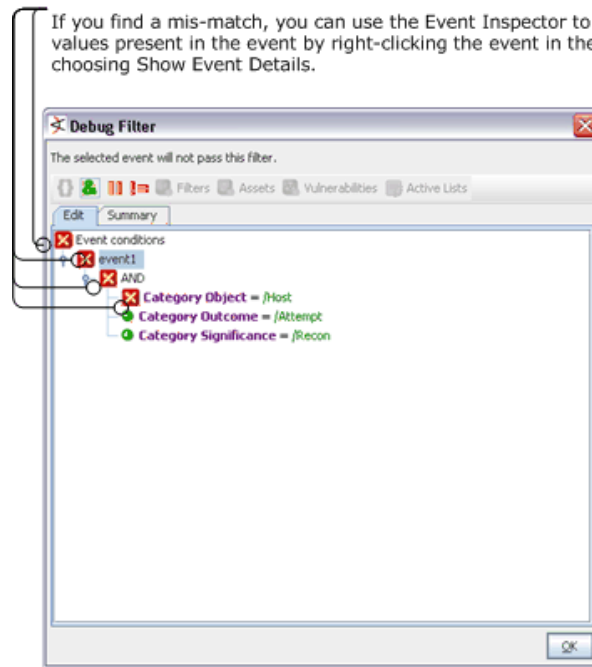
- ◆ If the selected filter matches the event, the Debug Filter dialog shows no errors or mis-matches in the definition.



- ◆ If the filter does not match the event, the Debug Filter dialog highlights the mis-matches between the filter conditions and the selected event with red **X**'s.

The filter definition highlights the mis-matches between the filter conditions and the selected event with red highlighted **X**'s.

If you find a mis-match, you can use the Event Inspector to check the field values present in the event by right-clicking the event in the channel and choosing Show Event Details.

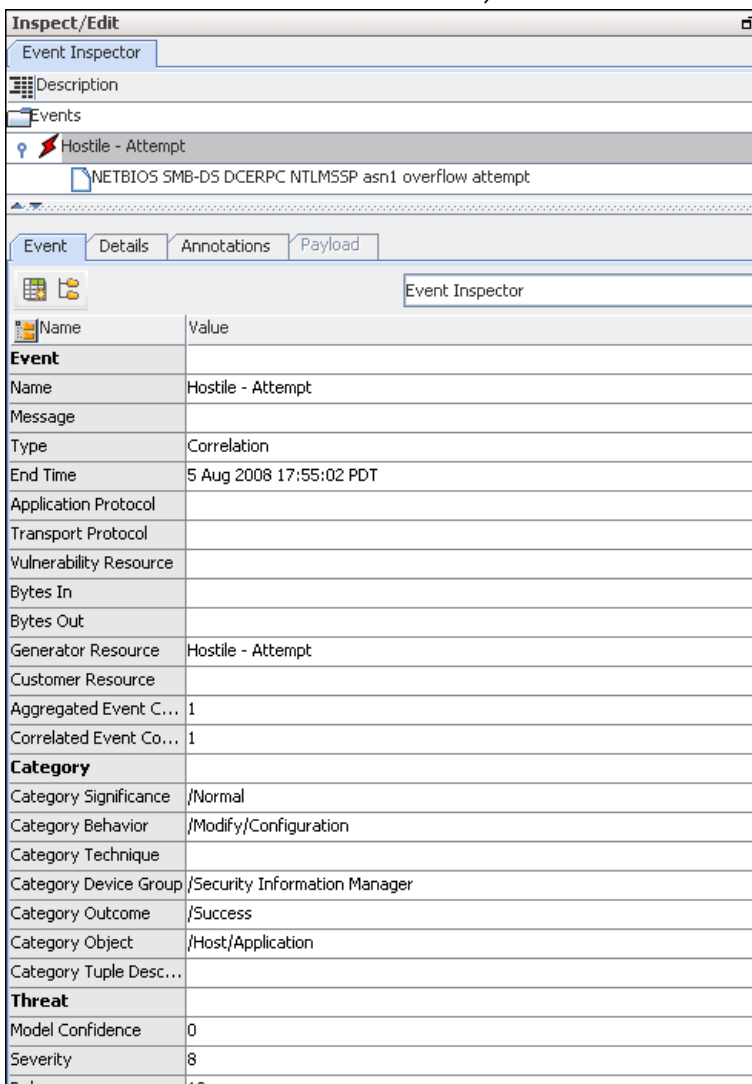


The display of red highlighted **X**'s in a filter as a result of filter debugging on an event *do not necessarily indicate* that the filter is *invalid*. Red highlighted **X**'s are shown here only to highlight where the selected filter does not match the selected event.

- 4 If you find mis-matches between filter conditions and an event type that you want to capture with the given filter, use the debug highlights in the filter definition along with the Event Inspector to adjust the filter to match the event.

In the example shown above, we are comparing a Hostile Attempt event to two different filters; a filter called "Hostile Attempt" and another filter called "Hostile Reconnaissance".

Here is a snapshot of the Event Inspector for this event. (To get this view, right-click the event and choose **Show Event Details**.)



Name	Value
Event	
Name	Hostile - Attempt
Message	
Type	Correlation
End Time	5 Aug 2008 17:55:02 PDT
Application Protocol	
Transport Protocol	
Vulnerability Resource	
Bytes In	
Bytes Out	
Generator Resource	Hostile - Attempt
Customer Resource	
Aggregated Event C...	1
Correlated Event Co...	1
Category	
Category Significance	/Normal
Category Behavior	/Modify/Configuration
Category Technique	
Category Device Group	/Security Information Manager
Category Outcome	/Success
Category Object	/Host/Application
Category Tuple Desc...	
Threat	
Model Confidence	0
Severity	8

- ◆ The first filter (our “Hostile Attempt” filter) matches the selected because both conditions on the filter match field values present in the event:

`Category Behavior = /Modify/Configuration`

and

`Category Object = /Host/Application`

Our “Hostile Attempt” filter would capture these types of events.

- ◆ The second filter (our “Hostile Reconnaissance” filter) has a condition that does not match field values present in the event.

The filter is looking for an event where `Category Object = /Host`, but ESM categorizes this event as `Category Object = /Host/Application`

To capture this type of event with our “Hostile Reconnaissance” filter, we would have to modify the filter.

The filter editor provides a *common conditions editor* (CCE) for define, edit, and debug filters. For more information on using the CCE, see [“Common Conditions Editor” on page 616](#).

For more information about using the Event Inspector to investigate events, see [“Inspecting and Editing” on page 66](#) and [“Event Inspector” on page 721](#).

See also, [“Creating Filters” on page 147](#) and [“Applying Filters” on page 155](#).

Applying Filters

This topic discusses how to apply the filtering resources in the Navigator panel to other filterable analysis resources: active channels, SmartConnectors, filters, reports, and rules.

Adding Filters to Resources

You apply existing filters to other resources by referencing them in those resource editors.

- 1 Right-click a resource in the Navigator panel such as a filter or rule and choose **Edit <resource>**.
- 2 Click the editor's **Conditions** tab if it isn't already at the front.
- 3 In the Inspect/Edit panel, click the **Filters** button and select a filter in the Filter Selector dialog box. The selected filter becomes a new condition line in this resource's filter.
- 4 Click **OK** or **Apply** to save the resource's definition including its new filter reference.



You can use hierarchies of filter references (including filters within filters) to better manage them, similar to style sheets.

Applying Resources as Filters to Active Channels

You can quickly apply or test the effects of using particular SmartConnectors, assets, categories, zones, vulnerabilities, customers, stages, or filter resources as conditions to filter active channels. These filters make the referenced resource a condition for the channel in use. You can choose to make the condition exclusive or additive.

- 1 Open the channel to filter in the Viewer panel or select it to bring it forward.
- 2 In an applicable resource tree in the Navigator panel, right-click an item and choose **Set as current filter** or **Add to current filter**. The filter change takes effect automatically and the channel's header immediately shows the new filter condition exclusively (set as) or as an addition (add to).
- 3 You can click the filter description in the channel's header to open the filter in the Active Channel Editor.

Removing a Filter Condition or Resource

You use the Filters tab of a resource's editor to change or remove any filters that affect it.

- 1 In the Navigator panel, right-click the filtered resource and choose **Edit <resource>**.
- 2 In the Inspect/Edit panel, click the **Filter** tab of the resource's editor.

- 3 In the Conditions editor, right-click the statement that imposes the condition you want to remove and choose **Delete**.
- 4 Confirm the deletion and click **Apply** to restart the channel.

Investigating Views

This topic explains how to use the Console's Investigate command to easily refine and explore channels contextually, using attributes of the events already being displayed in grid views.

The Investigate command uses these attributes, and the values found in their events, to automatically formulate simple filters or conditions.

When you create or refine a filter through Investigate, the Viewer panel automatically opens a new view of the channel with the filter applied. You explore the filter's effect in this view. You then have the option to keep the view by saving the channel under a new name, or discarding it by right-clicking in the grid and choosing **Close**.

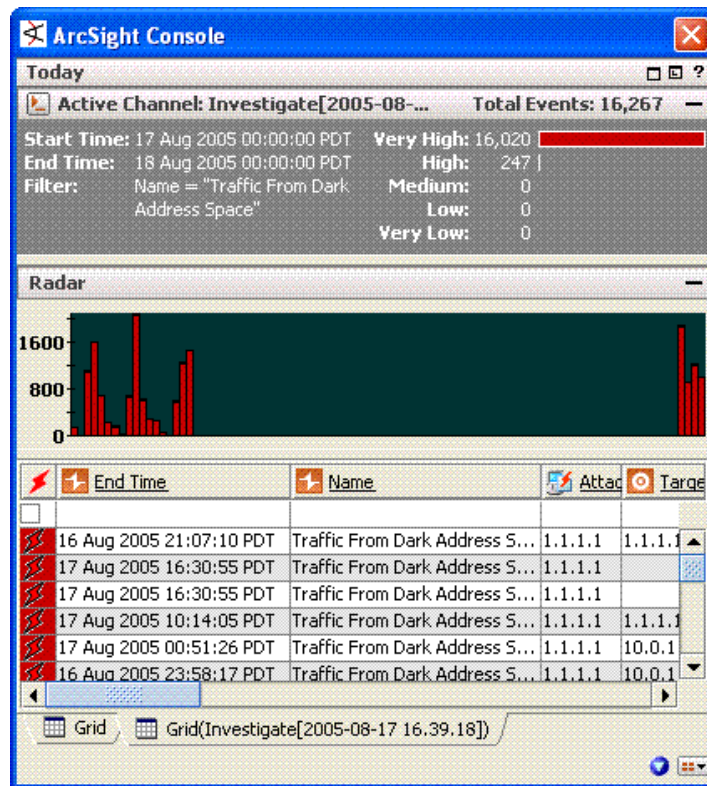


Figure 9-2 A temporary view created with the Investigate command

When you use Investigate to add a condition to a resource editor such as Rules or Filters, the condition appears in the editor panel where you can modify it or click **Apply** to put it into effect.

The new or modified views you generate with the Investigate command can be grids, or you can choose to display them in applicable chart formats using the **Viewer Selector** icon in the lower-right corner of the Viewer panel.

To learn more about the event attributes these options use, please see [“Data Fields” on page 633](#).

Using an Event Attribute to Show a New Filtered View

These options completely control the new view created, ignoring the filter in the original view. You most often use them to test and explore.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Create Filter [Attribute=Value]	Show only those events in which the selected attribute matches the value in the selected event.
Create Filter [Attribute!=Value]	Show only those events in which the selected attribute does not match the value in the selected event.
Create Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. Generally, attributes are considered related if they share a common focus such as IP addresses.

Refining a Filter with an Event Attribute

These options open a new view that uses a version of the prior filter modified to include the new filter component just selected. You usually apply these as part of a filter-refinement process.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

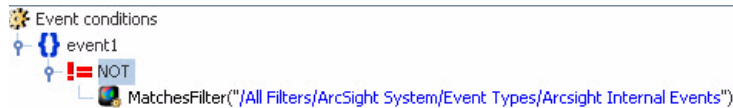
Option	Use
Add [Attribute=Value] to Filter	Show only those events that match both the prior and new filter elements.
Add [Attribute!=Value] to Filter	Show only those events that do not match both the prior and new filter elements.
Add to Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. This filtering element is applied in addition to any other already present. Generally, attributes are considered related if they share a common focus such as IP addresses.

Filtering Out ArcSight Events or Other Customizations

You can modify existing filters to refine your view to show only the events you want to see. Suppose you have an active channel that includes both system events and non-system events, but you want to see only the non-system events. You can modify the filter on the channel (or copy it and modify the copy) as follows:

- 1 Double-click on the filter in the channel header to get the channel editor.
- 2 Click the **Filter** tab in the channel editor.
- 3 Add this condition to the filter (with an AND):

```
!=NOT MatchesFilter("/All Filters/ArcSight System/Event
Types/ArcSight Internal Events")
```



To create or customize active channels in other ways, follow this same approach. Find a filter that does what you want and add condition statements to filters for a channel. Or, as in the example above, find a filter that does the opposite of what you want, add it to a channel, and negate the condition statement as shown above. Since we wanted to limit the channel to show only non-ArcSight events, we found the ArcSight Events filter, added the ArcSight Events condition to a channel, and negated it to get the effect of filtering out all ArcSight events

Adding an Event Attribute to a Filtering Condition

The **Add condition to editor** options apply to the editor in the Inspect/Edit panel that currently has focus. If no editor is open, the default target is the Filters Editor.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add Condition [Attribute=Value] to Editor	In the current editor, insert a new condition in which the selected attribute matches the value in the selected event.
Add Condition [Attribute!=Value] to Editor	In the current editor, insert a new condition in which the selected attribute does not match the value in the selected event.
Add Condition to Editor [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, add a condition to the current editor using the available list of attribute-value pairs that do (or do not) equate. Generally, attributes are considered related if they share a common focus such as IP addresses.

To remove a condition from the editor, right-click it and choose **Delete**.

When you are using these options to affect a view that is subject to the editor in use, click **Apply** or **OK** in the editor to put the condition into effect.

Contextual filters (in contrast to conditions) are temporary unless you save the modified view as a named active channel. Condition statements are saved with their relevant editors.

Permanently Modifying an Active Channel

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

Showing an Exploited Vulnerability

The Investigate options include the ability to look for potentially exploitable vulnerabilities associated with an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Exploited Vulnerabilities**. Available information appears in the Vulnerabilities tab of the relevant Asset Editor.

Showing a Targeted Asset

You can also find out more about an asset targeted by an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Targeted Asset**. Available information appears in the Asset Editor.

Modifying Views

This topic covers the use of "inline" (in the grid itself) grid view filtering options. The inline filter is the row of blank event values you see at the top of any grid in the Viewer panel.

Inline filtering directly affects the current view. Changes you make to a grid view by inline filtering also apply to any other versions of the view you open (e.g., its applicable chart types).

Modifying a View Inline

You use inline filters simply by clicking the inline fields at the top of view columns and choosing an event-attribute value to use as a constraint. When you choose multiple fields they automatically form AND conditions. Click the **Checkmark** icon to apply your filter selections.

Inline filters are temporary unless you save the modified view as part of a named active channel.

Undoing an Inline Filter

- 1 Click any of the filter fields in the top line of the grid view to show the inline filter control buttons.
- 2 Click the **X** (clear) button to remove the current filter elements and restart the view.

For details on working with filters and inline filters, see ["Creating Filters" on page 147](#) and ["Filtering Grid Views with Inline Filters" on page 109](#).

Permanently Modifying a View

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

Chapter 10

Query Viewers

This topic describes how to define and use query viewers to get high-level summaries about trends, events, other resources, and system health along with drill-down capability in a dynamic viewer.

- [“What are Query Viewers?” on page 161](#)
- [“Navigating to Query Viewers” on page 163](#)
- [“Pre-Built and Custom Query Viewers” on page 163](#)
- [“Running Queries and Viewing Results” on page 164](#)
- [“Adding Query Viewers to Dashboards” on page 174](#)
- [“Making Query Viewer Results Available to ArcSight Web” on page 175](#)
- [“Adding Query Viewers as Startup Views” on page 175](#)
- [“Generating Reports from Query Viewers” on page 176](#)
- [“Defining and Using Baselines” on page 177](#)
- [“Customizing Query Viewers” on page 184](#)
- [“Editing a Query Viewer” on page 197](#)
- [“Deleting a Query Viewer” on page 197](#)
- [“Example Queries for Common Scenarios” on page 197](#)

What are Query Viewers?

New in ArcSight ESM v.4.5, **query viewers** are a type of resource for defining and running SQL queries on other ESM resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results.

Previous to v.4.5, the only way to run SQL queries against ESM events and resources was to run reports, which use SQL queries and trend-queries. Starting with ESM v.4.5, you can use query viewers to run the same queries used for reports, and get results quickly. Then, if desired, you can generate a simple report directly from the query viewer results. Full-featured ESM reporting (with queries, trends, and templates) is still offered for more robust reporting requirements (see [“Building Reports” on page 205](#)), but query viewers provide a shortcut to running those same SQL queries apart from reporting.

Query viewers provide high-level summaries to monitor system health, reveal trends, and allow for drill-down investigation of all types of resources. Query viewers can work with

trend tables rather than event tables, and so can return results much faster than [Active Channels](#).

The SQL-based summary views and trend analysis in query viewers use aggregation to provide a higher-level perspective than data gleaned from exclusively event-focused active channels and snapshot, limited-range data monitors.

Query viewers offer a way to run queries outside of a full reporting paradigm (where queries and trends are always tied to a particular report). Also, you can generate simple reports directly from query viewer results.

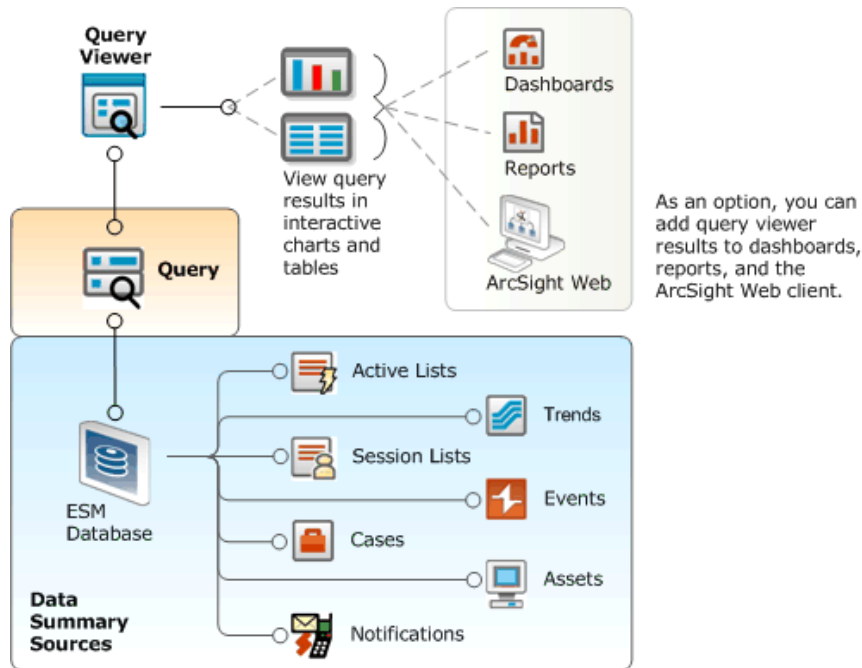


Figure 10-1 Query Viewers provide a quick way to run SQL queries on the data sources available to report queries. A Query Viewer leverages an existing report query to run SQL queries on ESM data sources, such as trends, active lists, session lists, assets, cases, events, and notifications. Each query viewer contains a base SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find trends, and performing drill-down investigation on a particular aspect of the result. The results are displayed in interactive charts and tables, which can be added to dashboards and published as reports.

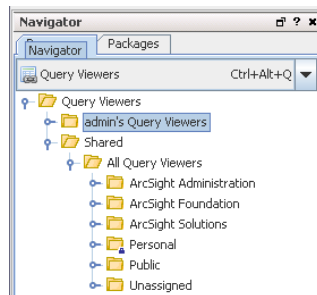
Query viewers provide:

- **A quick way to run SQL queries and trends apart from full-scale reporting.** If you want to run a pre-built SQL query and view results quickly, or build and test several iterations of a custom query, query viewers are an easy way to do it. (You can also generate a simple report directly from a query viewer.)
- **High-level summaries.** For example, using the aggregation provided by queries and trends allows summaries of "interesting things" over the last month, day, or hour.
- **Non-event-based summaries.** Queries can be used to analyze resources other than events (such as assets and cases).
- **Event-based summaries.** Queries can be used to analyze events, and will eventually lead to active channels (with drill-down investigation).

- **Baselines.** Analysts can apply a “baseline” to the information resulting from a particular run of a query viewer. A baseline acts as a reference point against which to compare results of other runs of the same query and highlights the *deltas* (differences) to help identify areas that vary significantly from normal.
- **Drill down.** Query viewers can provide drill-down investigation into the same or another query viewer for good performance on the next level of results as well. Ultimately, the drill-down can lead to an event channel, where the performance costs are the trade-off for the power of event-based analysis in an active channel. The query viewer author defines the appropriate drill-down paths and levels.
- **Performance.** Query viewers can use trend tables which are typically much smaller than event tables, and can be pre-built with summary views in mind. So, in most cases query viewers can return and display results faster than [Active Channels](#).
- **History.** When based on trends, query viewer result data can be kept for as long as desired and be independent of the event archival process.
- **Flexibility.** ArcSight ESM provides both pre-built query viewers and a resource editor for adding custom query viewers to suit the needs and environment of your organization.
- **Presentation Options.** Query viewer results can be displayed as tables (with baselines, if desired), pie charts, and bar charts, and added to [Dashboards](#) for quick display and monitoring.

Navigating to Query Viewers

In the Navigator panel, select **Query Viewers** resource from the drop-down menu.



Pre-Built and Custom Query Viewers

The Manager to which your Console is connected will have some pre-built query viewers available for use. At a minimum, you will have access to standard content query viewers that ship with ArcSight ESM. You might also have access to custom query viewers provided by content developers for your organization.

Standard Content

ArcSight ESM comes with a set of pre-built query viewers that address common network monitoring and trend analysis scenarios. To access the standard content query viewers, in the Navigator panel select **Query Viewers**, then click to expand the list to **Query Viewers/Shared/All Query Viewers**.

Folders for “ArcSight Foundation” and “ArcSight Administration” include the standard content query viewers.

If you have purchased ArcSight Solutions packages, query viewers for those are displayed under ArcSight Solutions.

For information on how to run and use any pre-built query viewer, see [“Running Queries and Viewing Results” on page 164](#), [“Generating Reports from Query Viewers” on page 176](#), and [“Defining and Using Baselines” on page 177](#).

Custom Query Viewers

When administrators or content developers at your organization create custom query viewers, they have the option of sharing these with other administrators and users. So, depending on your role and user permissions, you might have access to:

- query viewers that ship with ArcSight ESM
- custom-built query viewers that other administrators have shared
- your own custom-built query viewers

For information on how to create your own custom query viewers, see [“Customizing Query Viewers” on page 184](#).

Tweak Query Viewers as Needed

Of course you always have the option of taking provided query viewers and modifying them as needed to get the data you are looking for. Tweaking an existing query viewer can range from hiding or showing data fields and changing the sort order inherited from the base query to adding variables and modifying key fields. These kinds of modifications do not affect the base query, only the query viewer.

Once a query viewer is defined to reference a particular base query, that cannot be changed. If you want to reference a different base query, you need to create a new query viewer. Which brings us to an important point. *Where do you get the base queries you need?* See [“Query Viewers Need Base Queries” on page 164](#) to find out.

Query Viewers Need Base Queries

A primary attribute of any query viewer is the SQL query it references and uses. This is the “core” of the query viewer. If you create the query viewer yourself, you will define this as part of the initial query viewer attributes by browsing to and choosing a query from the [Reports/Queries](#) tree. If you are using a pre-defined query viewer, it will already reference a base query.

Reports, trends, and now *query viewers* are all “consumers” of SQL queries, which still must be created first in **Reports** resource **Queries** tab. So, if you don’t find a query viewer or query that gives the data view you are looking for, you will first need to create a new query (in Reports > Queries) and then jump back into the Query Viewers resource to create a new query viewer that references the base query you just created. (For information on creating queries, see [“Building Queries” on page 228](#).)

Running Queries and Viewing Results

To run a query defined in a query viewer, do either of the following:

- Select a query viewer and choose **View Data as...** > *<Display Format>*
- Or
- Double-click on a query viewer

Double-clicking provides the default view, as defined in the query viewer. For information on how to set the default view, see [related information on page 186](#) in “Query Viewer Attributes” on page 185.

The query runs, and returns results in the Viewer on the current state of the network and event flow.



Chart-style views (Pie and Bar charts) are limited to showing a maximum of 99 rows. This is a hard limit for charts to guarantee readability; it is not user-configurable. Therefore, results in chart views and table views for the same query viewer might not match (since table views can accommodate up to 10,000 rows of data in a query result).

Alternatively, you can add the result of a query viewer directly to a dashboard. For information on this, see [“Adding Query Viewers to Dashboards” on page 174](#).

Here are the details on how to run queries and view results:

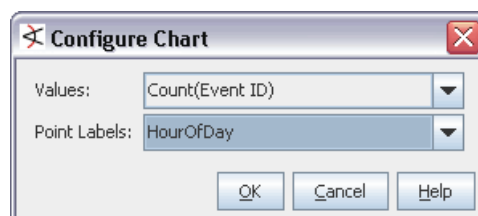
- 1 In the Navigator panel, choose the **Query Viewers** resource.
- 2 Navigate the tree, and select the query viewer you want to run.
- 3 Right-click the selected query viewer and select **View Data as > <Display Format>** and choose one of the following options:

Results Display Format	Description
Bar Chart	Displays query results as a bar chart
Horizontal Bar Chart	Displays query results as a horizontal bar chart
Pie Chart	Displays query results as a pie chart
Table	Displays query results in table format. Note: Baselines can only be applied to or viewed for query results shown in table format. (For more about establishing and using baselines, see “Defining and Using Baselines” on page 177 .)

Details on how to read and manipulate query results for each of these formats is provided

- 4 If you choose a Table display format, the results are displayed instantly. (Skip to example shown in [Figure 10-2](#).)

If you choose a bar chart or pie chart, you are asked to configure the chart display in Configure Chart dialog.



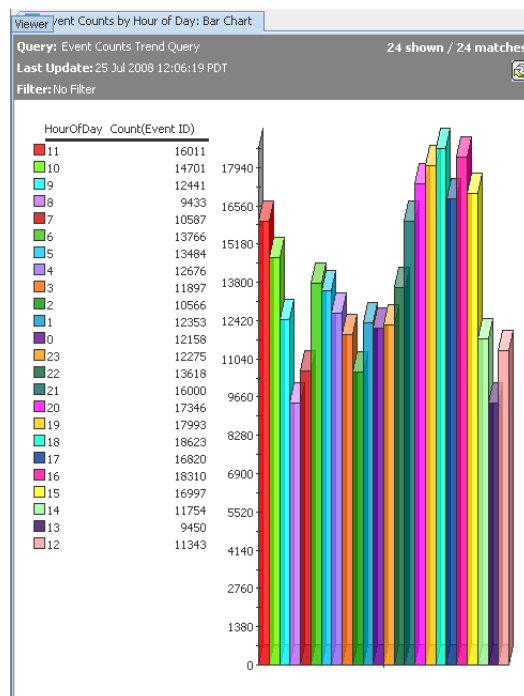
Select fields for “Values” and “Point Labels”.

Table 10-1 Configure Chart

Field	Description
Values	<p>The Values drop-down menu provides fields in the query result that contain data types. The value chosen will be used as the numbers by which to plot the vertical y axis points on a bar chart or the slice sizes on a pie chart.</p> <p>Values typically represent an unknown set of values, like a count. A common example of numeric data appropriate for values is a time like <code>HourOfDay</code> or a count like <code>Count(Event ID)</code>.</p>
Point Labels	<p>The Point Labels drop-down menu provides fields in the query result that contain non-numeric data types. The point labels are used to plot the horizontal x axis labels on a bar chart or the slice labels on a pie chart</p> <p>Examples of non-numeric data types appropriate for point labels are timestamps, strings such as are used for event names, and different types of addresses such as IP or MAC addresses. Point labels are typically a known set of limited values (like hours in a day denoted by timestamps).</p>

Example View Settings

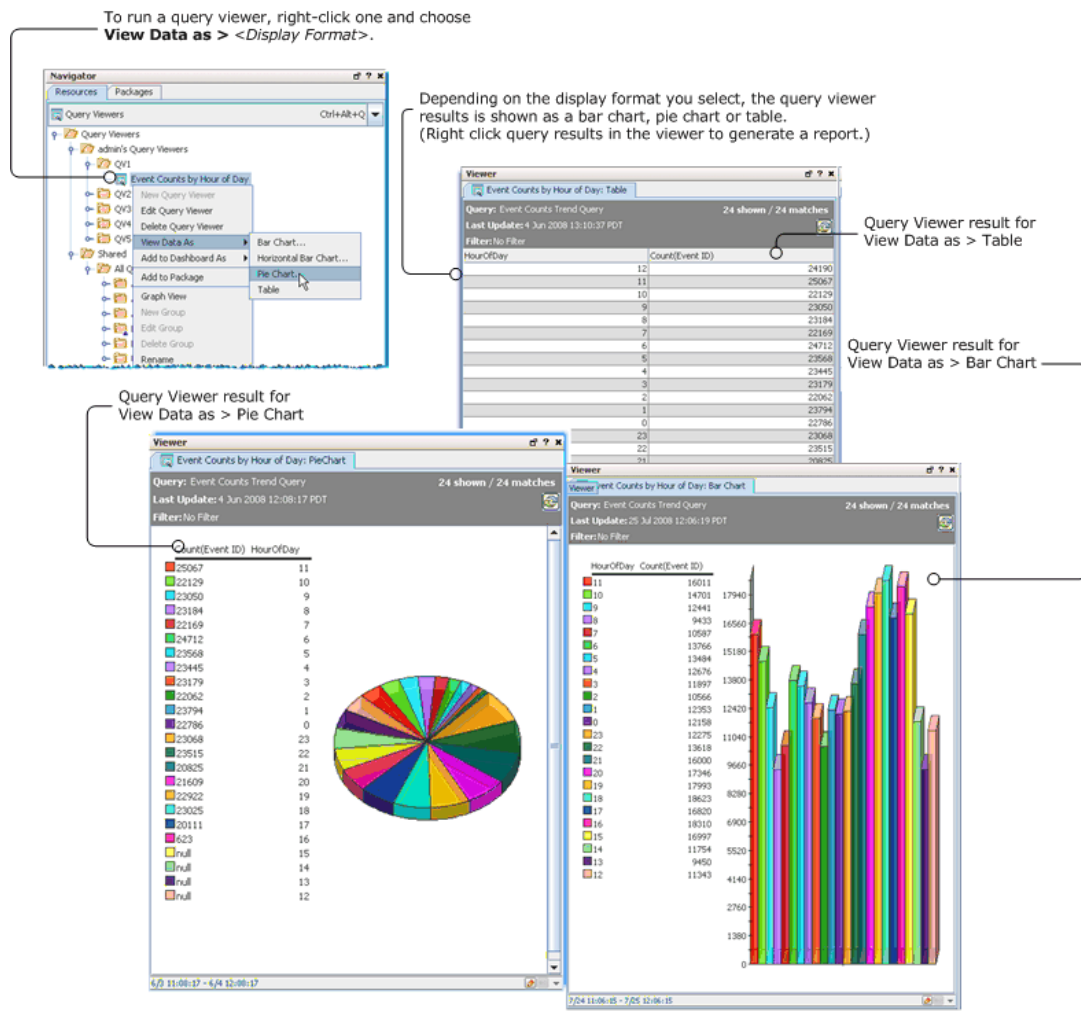
For example, for the Event Counts by Hour of Day query viewer, selecting “Count(Event ID)” for **Values** (the y axis) and “Hour of Day” (or Timestamp) for **Point Labels** (the x axis) results in the following display showing the event count for each hour of the day. The event count is depicted on the vertical y axis, with higher bars representing a higher event count for that hour. The hour of day (time) is represented on the horizontal x axis. The event count is shown for the last 24 hours starting at 11 am.



Understanding the Results View

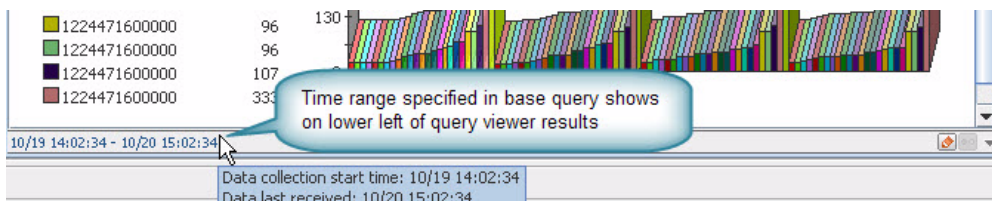
The results are displayed in the Viewer, as shown in Figure 10-2 and Figure 10-3.

Figure 10-2 “Event Counts By Hour of Day” query result as table, bar chart, pie chart.



Notice, also, that the time range for the base query is shown on the lower left of the query viewer results. Hover the cursor over the time range to see an annotated view of start and end times (“data collection start time” and “data last received”). This time range comes from the base query. (Another way to see the query time range is to open the query viewer in the editor and double-click on ***Query** in the Attributes display to drill down to the base query editor, which shows query start and end times.)

Figure 10-3 Time Range of Base Query



Working with Query Viewer Results

Various options are available to you with the different query result display formats (Bar Chart, Horizontal Bar Chart, Pie Chart, or Table).

Viewing query results in table format give you the ability to establish baselines and make comparisons, as well as manipulate the table data.

Bar charts and pie charts provide at-a-glance, graphical overviews of the results but with fewer options for manipulating the data after the fact.

Other options, such as filtering a query viewer results or running reports, are available on all result views.

Details of working with each view format are provided in the following topics.

Results in Table Format

To get results in Table format, right-click on a query viewer and choose **View Data as > Table**. You can sort, re-order, and create/compare baselines for data in a table view.

Left-click a table column header to sort or reverse-sort it. This affects the entire table.

The arrow next to a column header indicates the column is determining the current sort order for the table and shows the current sort order. (For example, this column is sorted showing highest count first.)

Right-click a table column header to get a list of sort and edit options for the column.

You can add a baseline to a **table** view of query result data, then run **baseline** comparisons to identify deltas in network behavior.

Only **table views** of query result data can be baselined and compared.

Timestamp	Name	Count(Event ID)	Count(Event ID) - (Reference Baseline)
16 Apr 2008 13:00 PDT	Sort Column	5460	5375
16 Apr 2008 13:00 PDT	Remove Sort	5896	772
16 Apr 2008 13:00 PDT	sp value count data monitor value...	773	5819
16 Apr 2008 13:00 PDT	Show Columns	5811	42
16 Apr 2008 13:00 PDT	Size Column to Fit	5704	42
16 Apr 2008 13:00 PDT	Help	5685	33
16 Apr 2008 13:00 PDT	Count(Event ID)	5630	3
16 Apr 2008 13:00:00 PDT	Count(Event ID) - (Typical Weekday Baseline)	5460	0
16 Apr 2008 13:00:00 PDT	Count(Event ID) - (Reference Baseline)	5460	0
16 Apr 2008 13:00:00 PDT	Starting Trend Query	96	0
16 Apr 2008 13:00:00 PDT	Sidetable Sizes (Rows)	30	0

Investigate View Options

The following right-click **Investigate** options are available on query viewer results in **table** format (obtained by choosing View Data as > Table):

- **Baselines.** Right-click *anywhere on the table result* in the Viewer to add a baseline or compare the current results to an existing baseline.
- **Drill-Downs.** Right-click a *row* in the table result to launch a given drill-down on that row item (if drill-downs are provided in the query viewer).
- **Channels.** Right-click a *cell* in the table result to create an active channel with a filter based on the value of the selected table cell.
- **Conditions.** Right-click a *cell* in the table result to add a filter condition based on the value of the cell.

These options are described in detail in [Table 10-2 on page 169](#).

Right-click a table in the Viewer over a table result to get **Investigate** options. (By default, add baselines and view available baselines here.)

If a query viewer includes drill-downs, these are shown as **Investigate** options (e.g., this one has drill-downs to source and destination addresses). Drill-downs are "row-specific". Right-click a row in a table view to get drill-down options for that row.

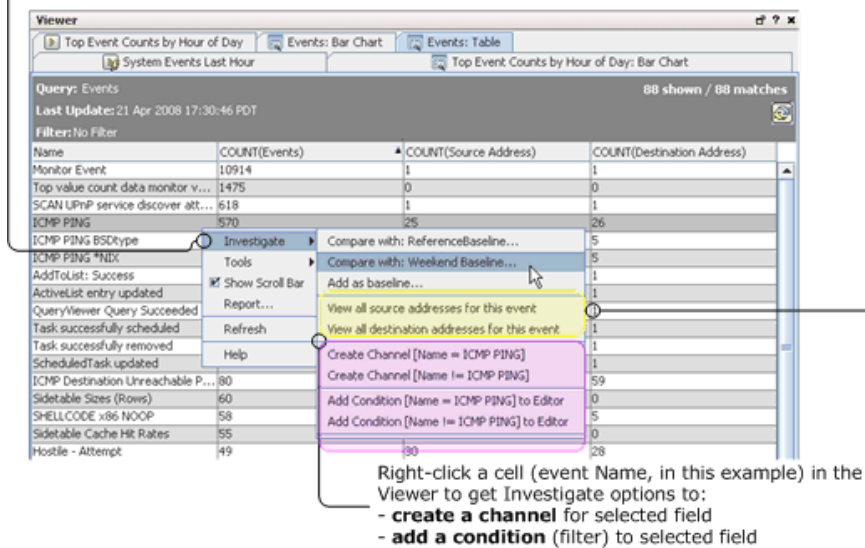


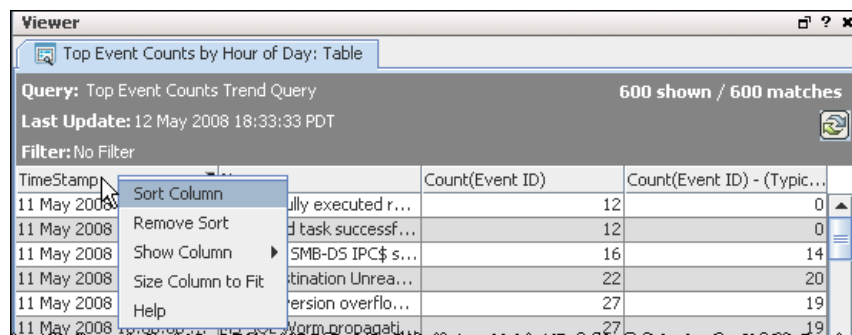
Table 10-2 Investigate Options for Results in Table Format

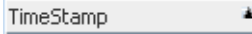
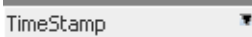
Option	Description
Add as baseline	<p>Adds the current results as a baseline for the query viewer.</p> <p>Right-click <i>anywhere on the table result</i> in the Viewer to add a baseline to the query viewer or compare the current results to an existing baseline.</p> <p>(See "Defining and Using Baselines" on page 177 and "Adding a Baseline" on page 179.)</p>
Compare with: < Baseline >	<p>Compares the current results with the selected baseline.</p> <p>Right-click <i>anywhere on the table result</i> in the Viewer to compare the current results to an existing baseline.</p> <p>This menu option is available if there is one or more baselines established for the query viewer. All baselines associated with the query viewer are available from this menu for comparison.</p> <p>(See "Comparing Displayed Results to a Baseline" on page 181.)</p>

Option	Description
Drilldowns	<p>Query viewers can provide <i>drilldowns</i> to Active Channels.</p> <p>If there are drilldowns associated with the query viewer, these are listed after the baseline options on the right-click Investigate menu for a selected row in the query viewer result.</p> <p>Right-click a <i>row</i> in the table result, and choose Investigate > <Drill-Down Option>.</p> <p>For example, an Events query viewer could provides drilldowns to view all source addresses for a selected event. Assuming each row in the result table represents an event, choosing this drilldown from the Investigate menu would lead to a table showing source addresses for the selected event.</p> <p>(See “Query Viewer Drilldowns” on page 193 and “Drill-Down Example” on page 200.)</p>
Create Channel	<p>Creates an active channel with a filter based on the selected cell in the table result.</p> <p>For example, right-clicking a table cell with an event name and choosing Investigate > Create Channel [EventName] creates an active channel that monitors and filters for occurrences of that event name. The filter is always set to the value of the cell (which in this example would be the event name).</p> <p>For more information about using active channels, see “Viewing and Using Channels” on page 92.</p>
Add Condition	<p>Brings up the Conditions Editor for the selected item, where you can add or modify conditions (filters) on the selected item.</p> <p>Right-click a <i>cell</i> in the query viewer table result to add a filter condition based on the value of the cell.</p> <p>For more information on working with Conditions, see “Common Conditions Editor” on page 616.</p>

Column Sort, Display, and Edit Options

Right click on a column header in a query viewer table result to get various options on that column.



Option	Description
Sort Column	<p>Sorts items in the column in ascending or descending order.</p> <p>Columns that have been sorted after the query viewer run show an up or down arrow next to them to indicate the direction of the sort.</p> <p>You can also sort the column by left-clicking on the column header. Clicking multiple times will toggle the sort between:</p> <ul style="list-style-type: none"> ascending order (indicated by the up arrow next to the header)  <p>Entries shown in descending order show highest numbers or most current time stamps at the top of the list</p> <ul style="list-style-type: none"> descending order (indicated by the down arrow next to the header)  <p>Entries shown in descending order show highest numbers or most current time stamps at the top of the list</p> <p>Notes:</p> <ul style="list-style-type: none"> Sorting on the contents of a column after a query viewer displays its results changes the view of the data provided by the original query. A query sorts during a query run, and then displays the data based on the sorting it did. If you click on columns to re-sort, you are changing the sort order the query gave you. In the cases where the original query used a “single-column” sort, you can “get back” to it in the viewer, but you can’t get back to a multi-column sort because this is offered only in the query sort options, not on the Console UI. Keep in mind that this option sorts on the data result returned by the query. This in combination with query row limits (applied when the query is run) can sometimes yield unexpected results. Example: if the query is defined to run on 2 days’ worth of data but hits the 10,000 row hard limit after processing only 1 day of data, then only 1 day’s worth of data is returned in the result. An “after-query” sort, in this example, is a sort on only 1 day’s worth of data. Sorting at the query viewer level sorts only the data returned by the query to Viewer. Initial sorting is done by the base query, which is responsible for running against the database. If the query level sort is yielding unexpected results, keep in mind that the original base query sort determines how much you can modify the view of the result. <p>See also, “Sort Baseline Data” on page 182.</p>
Remove Sort	<p>Removes a sort on the selected column. You can remove sorting imposed when the query viewer was run or a UI column-click sort that was done on the displayed result.</p>

Option	Description																																				
Show Column	<p>Right-click anywhere on any column header in a table to get a fly-out menu of columns included in the display result.</p> <p>Select columns to hide or show in the result. Columns with no checkmark beside them are hidden.</p> <p>This is the equivalent of hiding or showing a column before the query viewer runs. (However, only columns configured to be included in the original query are available to hide/show after the query is run.)</p> <p>To show a column in the results view that is currently hidden (whether before or after the query ran), right-click again and choose it (checkmark it).</p> <p>See also, “Show or Hide Baseline Columns” on page 182.</p>																																				
Size to Fit	Expands the column, if needed, to accommodate the full width for text in each row of the selected column.																																				
Drag-and-Drop options	<p>Left-click-and-drag on a column header to reposition it in a different horizontal order in the table. For example, if the original query viewer result shows columns in this order:</p> <table><tr><th>TimeStamp</th><th>Name</th><th>Count(Event ID)</th></tr><tr><td>12 May 2008 18:00...</td><td>Monitor Event</td><td>5460</td></tr><tr><td>12 May 2008 18:00...</td><td>Top value count data monitor value current</td><td>807</td></tr><tr><td>12 May 2008 18:00...</td><td>NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...</td><td>661</td></tr><tr><td>12 May 2008 18:00...</td><td>NETBIOS SMB-DS Session Setup AndX req...</td><td>658</td></tr><tr><td>12 May 2008 18:00...</td><td>Task successfully scheduled</td><td>40</td></tr></table> <p>You could click-and-drag “TimeStamp” to the right so that the columns display in this order:</p> <table><tr><th>Name</th><th>TimeStamp</th><th>Count(Event ID)</th></tr><tr><td>Monitor Event</td><td>12 May 2008 18:00...</td><td>5460</td></tr><tr><td>Top value count data monitor value current</td><td>12 May 2008 18:00...</td><td>807</td></tr><tr><td>NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...</td><td>12 May 2008 18:00...</td><td>661</td></tr><tr><td>NETBIOS SMB-DS Session Setup AndX req...</td><td>12 May 2008 18:00...</td><td>658</td></tr><tr><td>Task successfully scheduled</td><td>12 May 2008 18:00...</td><td>40</td></tr></table>	TimeStamp	Name	Count(Event ID)	12 May 2008 18:00...	Monitor Event	5460	12 May 2008 18:00...	Top value count data monitor value current	807	12 May 2008 18:00...	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	661	12 May 2008 18:00...	NETBIOS SMB-DS Session Setup AndX req...	658	12 May 2008 18:00...	Task successfully scheduled	40	Name	TimeStamp	Count(Event ID)	Monitor Event	12 May 2008 18:00...	5460	Top value count data monitor value current	12 May 2008 18:00...	807	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	12 May 2008 18:00...	661	NETBIOS SMB-DS Session Setup AndX req...	12 May 2008 18:00...	658	Task successfully scheduled	12 May 2008 18:00...	40
TimeStamp	Name	Count(Event ID)																																			
12 May 2008 18:00...	Monitor Event	5460																																			
12 May 2008 18:00...	Top value count data monitor value current	807																																			
12 May 2008 18:00...	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	661																																			
12 May 2008 18:00...	NETBIOS SMB-DS Session Setup AndX req...	658																																			
12 May 2008 18:00...	Task successfully scheduled	40																																			
Name	TimeStamp	Count(Event ID)																																			
Monitor Event	12 May 2008 18:00...	5460																																			
Top value count data monitor value current	12 May 2008 18:00...	807																																			
NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	12 May 2008 18:00...	661																																			
NETBIOS SMB-DS Session Setup AndX req...	12 May 2008 18:00...	658																																			
Task successfully scheduled	12 May 2008 18:00...	40																																			

Results in Chart Formats

To get results in Chart format, right-click a query viewer and choose either:

- View Data as > Bar Chart or Horizontal Bar Chart
- View Data as > Pie Chart.

Right-click an item in a chart view to get **Investigate** options for that item (e.g., event)

Investigate menu includes options to:

- create a channel for selected item
- add a condition (filter) to selected item

Table 10-3 Investigate Options for Results in Chart Formats

Option	Description
Drilldowns	<p>Query viewers can provide <i>drilldowns</i> to Active Channels.</p> <p>If there are drill-downs associated with the query viewer, select an item in the first or “key” column, then right-click to get drill-down options in the Investigate menu.</p> <p>For example, an Events query viewer could provides drill-downs to view all source addresses for a selected event. Choosing this drilldown from the Investigate menu on a query result would lead to a table showing source addresses for the selected event.</p> <p>(See “Query Viewer Drilldowns” on page 193 and “Drill-Down Example” on page 200.)</p>
Create Channel	<p>Creates a channel on the selected item. (For example, right-clicking an event and choosing Investigate > Create Channel [EventName] creates an active channel that monitors and filters for occurrences of that event.</p> <p>For more information about using active channels, see “Viewing and Using Channels” on page 92.</p>
Add Condition	<p>Brings up the Conditions Editor for the selected item, where you can add or modify conditions (filters) on the selected item.</p> <p>For more information on working with Conditions, see “Common Conditions Editor” on page 616.</p>

Filtering Query Viewer Results

You can filter query viewer results shown in table and chart formats.

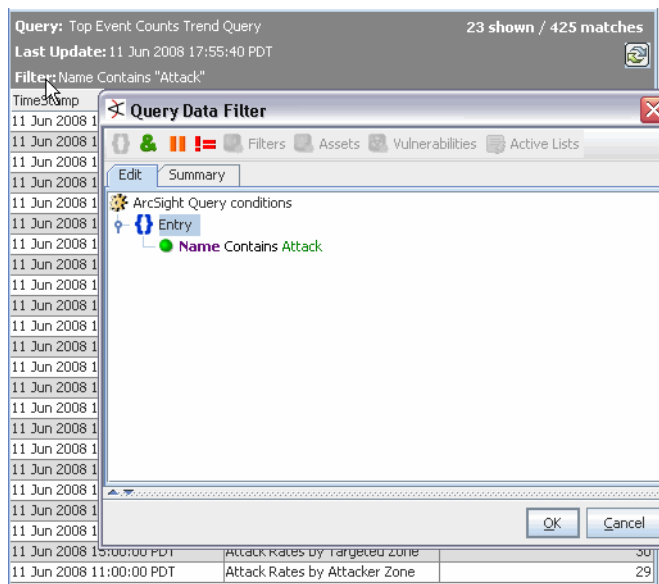
Adding a Filter

To filter query viewer results:

- 1 Click **Filter: No Filter** in the header of a query result view. (You can also right-click the filter name and choose **Edit Filter** from the context menu.)

This brings up the Common Conditions Editor (CCE) dialog.

- 2 Use the CCE dialog to add a filter. (For details on how to use the CCE dialog to create filters, see the topic on the [“Common Conditions Editor” on page 616.](#))



- 3 Click **OK** to save the filter, and filter the current result view.



Filters on query viewer results are locally saved and available only while the current result set is displayed. These filters are not saved as a part of the query viewer. When you close the query viewer result, the filter is no longer available; you will need to recreate it on a new result set.



Filters can also be applied to baseline *delta* columns. (See [“Defining and Using Baselines” on page 177.](#))

Removing a Filter

To remove a filter from a displayed query viewer result, right-click the filter name in the header of the result view and select **Remove Filter** from the context menu.

Adding Query Viewers to Dashboards

You can add a query viewer result to a dashboard as follows:

- 1 Add a dashboard and keep it open in the viewer (or identify and open an existing dashboard to which you want to add query viewer results).

To add a new dashboard:

- a Choose **Dashboards** in the Navigator, click the **Dashboards** tab, right-click on a group, and select **New Dashboard** from the context menu.

This brings up an empty, untitled dashboard in the viewer

- b Right-click on the title bar of the dashboard and choose **Save Dashboard As**.
- c In the popup dialog, navigate to the group where you want to save the dashboard, enter a name for the dashboard, and click **OK**.

Make sure that the dashboard to which you want to add the query viewer result is open and has focus in the viewer.

- 2 Choose **Query Viewers** in the Navigator.
- 3 Select a query viewer, right-click and choose **Add to Dashboard As > <Display Format>**. (Result display formats are Bar Chart, Horizontal Bar Chart, Pie Chart, or Table.)

This runs the query viewer and adds the results to the current dashboard.

You can add multiple query viewer results sets along with other resources to a single dashboard.



Query viewer results on dashboards are accessible from ArcSight Web. For more about ArcSight Web, see ["ArcSight Web" on page 580](#).

For more information about working with dashboards, see ["Using Dashboards" on page 113](#).

Making Query Viewer Results Available to ArcSight Web

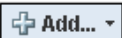
Query viewer results on dashboards are accessible from ArcSight Web. For more about ArcSight Web, see ["ArcSight Web" on page 580](#).

For more information about working with dashboards, see ["Using Dashboards" on page 113](#).

Adding Query Viewers as Startup Views

Query Viewers can be set as the startup view for a group as follows:

- 1 Select **Users** in the Navigator
- 2 Right-click a group and choose **Edit Groups** from the context menu.
- 3 In the editor for the selected group, click **Startup Views** tab, then click **Query Viewers** subtab.

- 4 Click **Add** () to bring up the Query Viewer Selector.

- 5 In the Query Viewer Selector dialog, navigate to and select (checkmark) the query viewer you want as the startup query viewer for this group and click **OK**.

The full path to the query viewer you selected is shown on the Query Viewers tab in Startup Views.

- 6 Click **Apply** to save your changes and leave the group editor open, or click **OK** to save and close the group editor.

For more information on editing groups and startup views, see ["Editing User Groups" on page 442](#) and ["Setting Startup Views" on page 443](#).



Regardless of startup view settings for groups, the Query Viewers you have showing when you close the Console are reloaded when you restart the Console.

Generating Reports from Query Viewers

After you run a query viewer, you can generate a simple report containing the results.



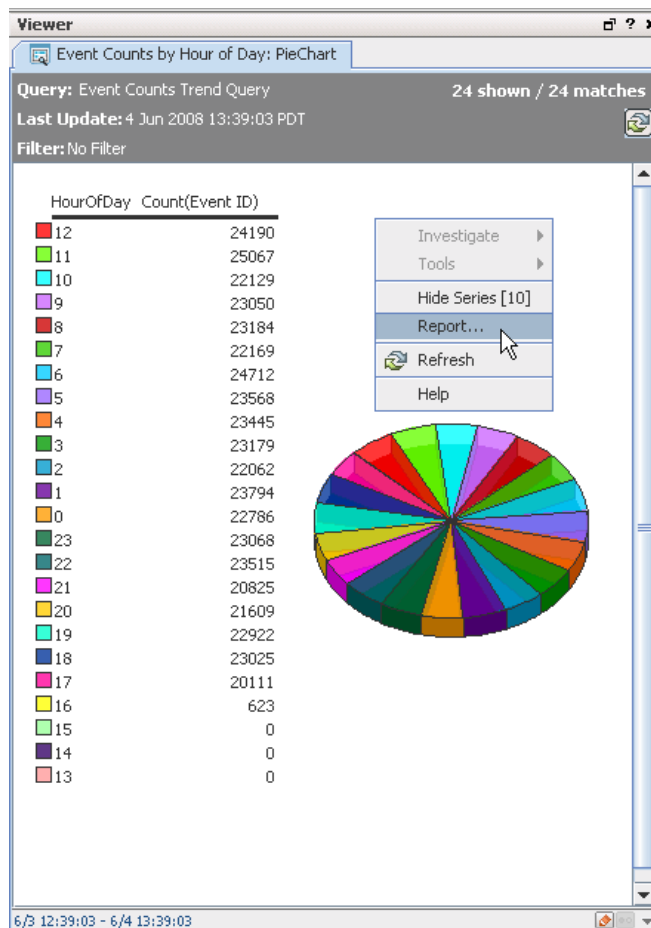
The report display format is based on the query viewer result display. For example, if you chose to view query data as a *pie chart*, the generated report will show the same pie chart view. To generate a report showing results for the same query as a *bar chart* or *table*, you would need to re-run the query viewer (<Query Viewer> > View Data as) in one of those formats, and then generate the report from that view.

The report contents might not include as much data as the query viewer result shown in the Console for these reasons:

- Reports on pie charts and bar charts have a default row limit of 25. This is user-configurable. You can set a higher or lower row limit on the Report Parameters dialog you get when you run the report. (See [Step 2 on page 177](#).)
- Reports on *tables* have no hard limit on number of rows in the table.
- Data viewed in *chart* format has a hard limit of no more than 99 rows, therefore reports on charts have the same hard limit of no more than 99 rows displayed on the Console and Web user interface.

To generate a report on a query viewer:

- 1 Right-click on the query viewer results table or chart (anywhere in the Viewer panel) and click **Report**.



- 2 Specify the options on the Report Parameters dialog (or take the defaults) and click **OK**.

Report Parameters

Set Parameters

Name	Value
Common Parameters	
Report Format	pdf
Page Size	Letter [8.5x11 in]
Email to	
Email Format	Send URL
Email Subject	ReportName
Row Limit	25

Save Output Parameters

Name	Value
Output Parameters	
Archive Report Folder	Select a Archived Report Group
Archive Report Name	{Today}/{ReportName}_{Now}
Archive Report Expiration Time	Now+6M

☒ Save Output

OK Cancel Help



- For more about Report row limits, see these Tips and [related information on page 176](#).
- If you click **Save Output** on the Report Parameters dialog, you get additional options for setting archived report "Save Output Parameters".

For more help on setting report parameters, see ["Report Parameters" on page 289](#).

- 3 When the report is ready, a dialog gives you the option of opening it to view it now or saving it to a location you specify via a file browser.

Choose **Open** to view the report or **Save** to save it in a specified location.



Reports initiated from query viewers are provided for convenience as a quick way to share the result data. Query viewer reports are limited to displaying data from the single query covered by the query viewer and retain the format of the chart or table in which the query viewer results are displayed. For information on creating and publishing richer, highly formatted reports on multiple data sources see [Chapter 11, Building Reports, on page 205](#) and [Chapter 12, Running and Managing Reports, on page 287](#).

Defining and Using Baselines

You can establish a particular set of query results as a **baseline** snapshot against which to compare the results of other runs of the same query. Comparing the results of the same query run at different times and in different contexts highlights the *deltas* (differences) and helps identify areas that vary significantly from normal.

You can define baselines and run comparisons with any query viewer that:

- lends itself well to a table format display
- includes one or more key fields by which to locate matching entries between the baseline and currently displayed information.

For example, suppose you have a query that returns the top 10 event counts by name and you want to compare it against some baseline. A reasonable comparison would be between similarly named events in both sets of data. In this case, the event name would be used as the key field.



- **Baselines are applicable only to table views of result data.** Baselines do not apply to graphical views such as pie charts, bar charts, and so on. You always have the option to view query data from any query viewer as a graphical chart or a table, but the baseline data will only be accessible from the table view of the data.
- **Baselines require one or more key fields** by which to locate matches between the baseline and the displayed data. The key fields must be built into the query viewer to which you want to add a baseline.
- **Values for Key fields must be unique.** When adding baselines, make sure key field(s) in the query viewer have unique values. (See **Fields** tab in query viewer editor.) Also, check the query viewer start and end times (on **Attributes** tab in the query viewer editor) to make sure the time frame over which the query will run makes sense.

You can add one or more baselines to a single query viewer, and delete them as needed.

Why Baselines are Useful

In addition to providing a way to compare result data from different query runs, baselines provide an efficient way to save, annotate, and retrieve data that might otherwise be too difficult to access in any meaningful way.

Once a baseline is defined, it is preserved as a File resource that is associated with the query viewer. In the Navigator, choose **Files** and expand the **Query Viewer Baselines** folder to view the new baseline files.

In **Query Viewers**, you can create, save, and use **Baselines** to compare result data from the same query viewer run at different times and dates.

The screenshot shows the ArcSight Console interface. The main window displays a query viewer titled 'Top Event Counts by Hour of Day: Table'. The query is 'Top Event Counts by Hour of Day: Table'. The results show a table with columns: TimeStamp, Name, Count(Event ID), Count(Event ID - (Typical Weekday Baseline)), and a difference column. The table lists various events like 'Monitor Event', 'Top value count data monitor v...', 'NET 1800S SPM-CIS-OS-Session Setup...', 'AddToAuth: Success', 'Investigate', 'Trade', 'Show Scroll Bar', 'Report...', 'Refresh', 'Help', 'ScheduledTask updated', 'Task successfully removed', 'Task successfully scheduled', 'MS-SQL: Worm propagation atte...', 'MS-SQL: Worm propagation atte...', 'Performance attempt', 'Unreachable H...', 'PSC share un...', 'Unreachable N...', 'CE share unc...', 'ADCP', 'Data monitor v...', and 'Unreachable'. The Navigator pane on the left shows the 'Files' resource expanded, with 'Query Viewer Baselines' highlighted. A callout box points to the 'Add as Baseline' button in the query viewer's context menu.

Baselines created in **Query Viewers** also show up under the **Files** resource in the Navigator.

With Query Viewer baselines, you can:

- Retrieve the snapshot baseline data by running comparisons against it
- Compare current result data against one or multiple baselines
- Get meta-information about the baseline (such as when it was saved, by whom, and comments)
- Sort, show, or hide the baseline comparison columns
- Maintain the baseline data as a Files resource baseline even if the original data is lost or is too performance-intensive to re-generate (for example, an aggregation query). (All baselines are automatically added as Files resources when they are created.)
- Add and remove baselines as needed, and edit some meta-information on baselines (for example, description comments)
- Use filters on the baseline (*delta*) columns. For example, you could filter on a baseline column to find where the current results differ from the baseline by more than some specified value

Planning for Baseline Comparisons

Query viewer baselines might prove most useful if you take a little time to identify some goals for their use or questions you want answered, and then plan how to implement the baselines for those purposes. Here are some suggestions to start off with.

- 1 Establish questions or goals for baseline comparison monitoring and identify the type of data you want to evaluate.

For example, you might want to determine what type of event traffic is at its highest at different times of day or when network attacks tend to increase. Or, you might notice a spike in certain query viewer results (such as more logins from a particular user) and decide to compare the behavior against a sampling of results from subsequent or previous query runs.

- 2 Identify the query viewer (and associated query) appropriate to use. (If the query viewer you need is not provided, you or someone on the team will need to develop it. See [“Customizing Query Viewers” on page 184](#) for more information on this.)

For example, if you want to monitor what type of event traffic is at its highest, you could establish a baseline for a query viewer that returns “Top Event Counts by Hour of Day”. You could also use a query viewer *baseline* to take snapshots of event counts throughout the day, either for record-keeping or to explore and compare later.

- 3 Monitor results for your chosen query (by running the query viewer) to identify a “typical” or “normal” result set to use as a baseline.
- 4 Add (capture) the baseline from the typical/normal result set.
- 5 Monitor subsequent results for variation (spikes, dips) or time periods against which you want to compare with the baseline, and run baseline comparisons on these.

Adding a Baseline

A baseline is a snapshot of the current results that can be used later as a reference point to compare other query result views. Baselines are often added to capture “normal” network behavior, so that when spikes, dips, or other anomalies surface, these can be compared against the baseline.

Baselines can only be defined on numeric data (because they are designed to show *deltas*, the difference or change between two values).

To add a baseline to a query viewer:

- 1 In the Navigator panel, choose the **Query Viewers** resource.
- 2 Select and run the query viewer (containing the query) for which you want to define a baseline.

To do this, right-click on the query viewer and choose **View Data As > Table**.



Baselines are applicable only to table views of result data.

The query viewer result is displayed in the Viewer.

- 3 Right-click anywhere in the results table in the Viewer, and select **Investigate > Add as baseline...** to get the Add a baseline... dialog.

The dialog box titled "Add as baseline..." contains a text input field for "Enter a name for this baseline" with the text "Typical Weekday Baseline" entered. Below it is a "Description:" label followed by a large empty text area. At the bottom are three buttons: "OK", "Cancel", and "Help".

- 4 Enter a name for the baseline, optional description, and click **OK** to add it.

This saves the current query result data as a named baseline for the selected query viewer, and makes it available for use (via "Investigate > Compare with..." against results from other runs of the same query viewer).

The baseline is shown on the Fields tab of the query viewer to which you added it.

The screenshot shows the "Fields" tab of a query viewer. At the top is a "Baselines" section with a "Remove" button. Below it is a list containing "Typical Weekday Baseline". Underneath the list is a "Description" label and an empty text area. At the very bottom, it says "Created by admin at Apr 15, 2008 4:48:28 PM".



If the query viewer editor is not currently displayed, double-click on the same query viewer in the Navigator panel to open it in the editor. Click the query viewer editor **Fields** tab.

Comparing Displayed Results to a Baseline

Once you establish a baseline for a query, you can compare subsequent results for the same query against the baseline.



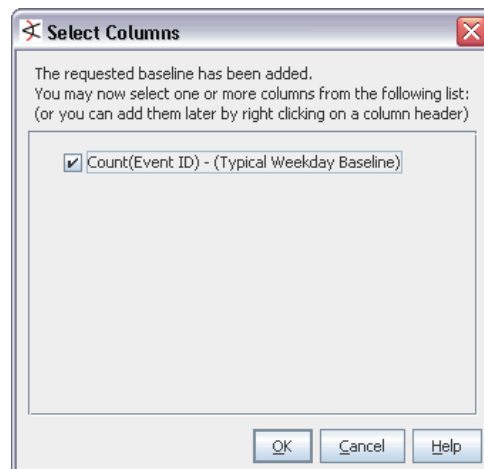
- Baseline comparisons, like baselines, can only be derived from *table* views of the query viewer results. (Select a query and choose View Data as > Table. See ["Results in Table Format" on page 168.](#))
- The query viewer you select for baseline comparison needs to have at least one baseline already added to it. Baselines are shown on the **Fields** tab of the Query Viewer editor.

To run a comparison, do the following:

- 1 If you do not already have a table view of the data you want to compare, right-click the query viewer you want to evaluate against a baseline, and choose **View Data as > Table** from the Navigator menu.
- 2 In the Viewer, right-click anywhere on the table view results and select **Investigate > Compare with: <SomeBaseline>**.

The comparison data is collected and added as a new column. You have the option of hiding or showing it in the table as needed.

- 3 Make your selections on the Select columns table and click **OK**.



If you selected the comparison column, it is displayed on the table next to the original results for that column.

Events: Table		
Query: Events		
Last Update: 1 Aug 2008 16:40:14 PDT		
Filter: No Filter		
10 shown / 10 matches		
Name	COUNT(Events)	COUNT(Events) - (Typical Weekday Baseline)
Monitor Event	14071	-929
Top value count data monitor val...	10209	1209
ICMP PING	976	
ICMP PING *NIX	852	-57
ICMP PING BSDtype	852	-56

Note that differences between the current values and the baseline can be positive or negative, as shown in the example comparison above. A positive value in the baseline comparison indicates more events in your current sample, compared to the baseline. A

negative value in the baseline comparison indicates fewer events in your current sample, compared to the baseline. If the baseline field for a row is null, this indicates that no baseline value was available for that key.



- By the time the Select Columns dialog is displayed, the Baseline comparison is already available. If you select columns, those are displayed in the viewer on the Table result.
- After running a baseline comparison, the right-click over Table **Investigate > Compare with <Baseline>** option for the baseline you just ran will be grayed out (even if you chose not to immediately select any columns or clicked Cancel on the Select Columns dialog). This is because the baseline is already added.
- To show or hide more columns (including baseline columns), right-click the column header, choose **Show Column**, and check (enable) or uncheck (disable) columns. See also, [“Show or Hide Baseline Columns” on page 182](#)

Show or Hide Baseline Columns

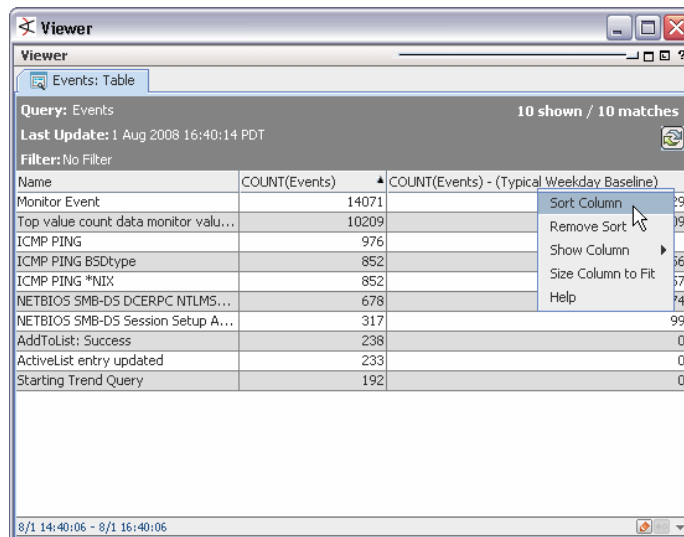
You can always show or hide columns, including baseline columns. To do this right-click anywhere in the table header (on any of the column titles), choose **Show Column > <SomeField>**.

Name	Count(Event ID)	Count(Event ID) - (Typical Weekday Baseline)
Sort Column	6990	6905
Remove Sort	5896	5811
Show Column		5734
Size Column to Fit		5726
Help		5619
Monitor Event		5600
Monitor Event		5545
Monitor Event		5375
Monitor Event		5375

See also [“Column Sort, Display, and Edit Options” on page 170](#).

Sort Baseline Data

You can perform an after-query sort on baseline comparison data by clicking the column headers. A pre-query sort for baseline data is not available. (That is, there is no option to add a sort as a part of the baseline in the query viewer definition.)

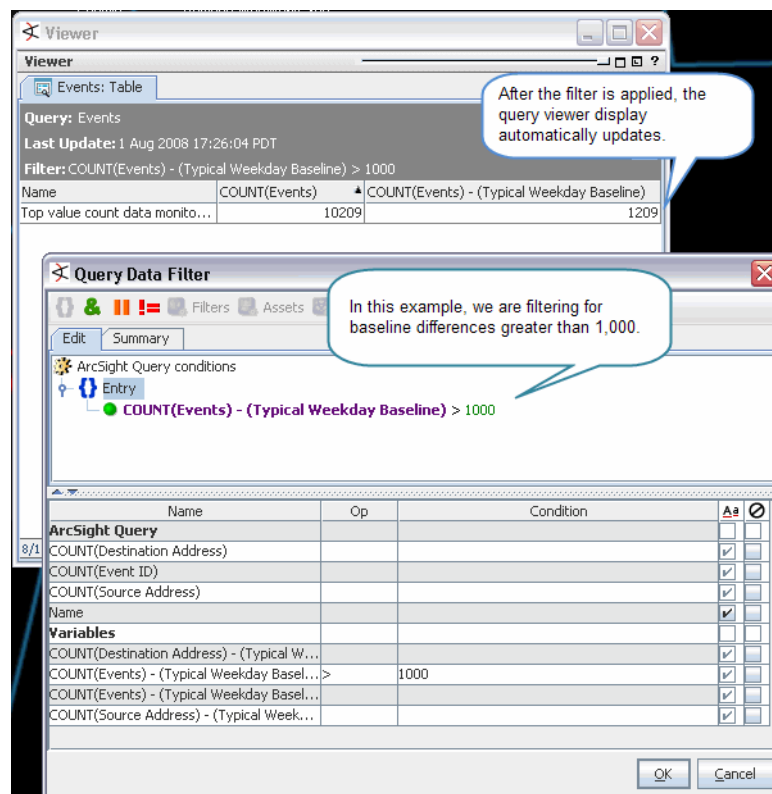


See also [“Column Sort, Display, and Edit Options” on page 170](#).

Filter Baseline Data

You can filter on the baseline comparison column the same way you would filter on any other column. Click the **Filter** in the query viewer header to bring up the Query Data Filter dialog. Enter your filter conditions and click **OK**. After the filter is applied, the query viewer automatically updates.

The Query Data Filter is based on the Common Conditions Editor (CCE). For information about using the CCE to define filters, see [“Common Conditions Editor” on page 616](#).



Removing a Baseline

Baselines, like the queries themselves, are associated with and contained in query viewers. To remove a baseline, you remove it from the list of baselines in the query viewer editor.



Removing a baseline from a query viewer is different from hiding or showing a baseline column in a query result. If all you want to do is temporarily hide a baseline column in a results table, use the right-click “Show Column” option in the Viewer on the results table as described in [“Column Sort, Display, and Edit Options” on page 170](#) in [“Results in Table Format” on page 168](#).

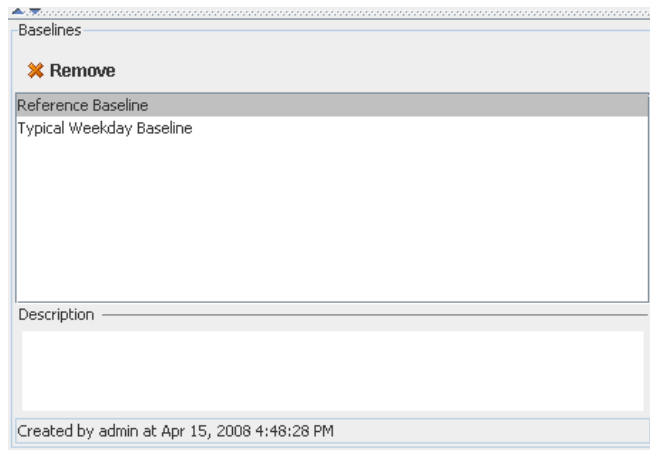
To remove a baseline from a query viewer:

- 1 In the Navigator panel, right-click the query viewer containing the baseline you want to remove and select **Edit Query Viewer**.

This opens the editor for the query viewer in the Inspect/Edit panel.

- 2 In the editor, click the **Fields** tab.

- 3 Under Baselines, select the baseline you want to remove and click **Remove**.



- 4 Click **Apply** to save your changes to the query viewer, or click **OK** to save changes and close the editor.

Note that there is no confirm dialog for this Remove baseline action, but if you do not want to save your changes, click **Cancel** and the baseline will not be removed.

Customizing Query Viewers

Query viewers provide a shortcut alternative to running SQL queries as a part of reporting. Keep in mind that query viewers use base queries, so a first step in creating a query viewer is deciding what SQL query you want to use. If you can't find one that does what you want, you'll need to create one first, before defining your query viewer.

Creating a New Query Viewer

The high-level steps for creating a query viewer are as follows:

- 1 Identify your question(s) and what information you are looking for. (For example, "What types of actions represent the highest volume of events on my network during various times of day?")
- 2 Based on the question you want answered, decide what kind of query you need and determine whether it is available or you have to create it.

If you do not find a suitable query when you browse the choices under Reports/Queries (or on the Query Viewer "Query" field "Select a Query" drop-down menu), you can create one. To get started creating a new query, navigate to **Reports**, and click the **Queries** tab. For more information see ["Building Queries" on page 228](#).

When you know which query you want to use and have either found a pre-built one or created a new one, you are ready to create a query viewer that will use that query.

- 3 Select **Query Viewers** in the Navigator.
- 4 Right-click a group (folder) and select **New Query Viewer**. This launches the Query Viewer Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 5 Define general attributes for the query viewer as described in [“Query Viewer Attributes” on page 185](#). At a minimum, fill in the required values (red asterisks) on the **Attributes** tab (query viewer name and “base query” to use).
- 6 Choose the **Fields** to display for the query viewer as described in [“Query Viewer Fields” on page 189](#). (Fields are inherited from those available in the base query.)
- 7 Define **Variables** for use in the query viewer as described in [“Query Viewer Variables” on page 192](#) (optional).
- 8 Specify any **Drilldowns** you want to make available as described in [“Query Viewer Drilldowns” on page 193](#) (optional).
- 9 Click **Apply** or **OK** to create the new query.



Be sure to click **Apply** or **OK** frequently to save settings periodically as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings via these buttons, your settings will not be saved.

The following sections provide details on defining attributes, fields, variables, and drilldowns for a query viewer.

Defining Query Viewer Settings

Use the Query Viewer Editor to build a new query viewer or edit an existing one. Query viewer settings are defined on multiple sub-tabs.



- To get to the editor for a query viewer, follow the first steps in either [“Creating a New Query Viewer” on page 184](#) or [“Editing a Query Viewer” on page 197](#).)
- If you want to edit more than one query viewer at a time, choose **Edit > Preferences** from the Console menu, then click **Global Options**. On the Global Options panel, check Allow multiple editors of the same type, then click **OK** to save the change and close the Preferences dialog. For more on setting Console preferences, see [“Changing User Preferences” on page 556](#), especially the subtopic [“Changing Global Options Like Panel and Editor Characteristics” on page 558](#).

Query Viewer Attributes

The following fields in the **Query Viewer** section are attributes to specify when creating a new query viewer.

Query Fields	Description
Name	Name for the query viewer. Spaces and special characters are okay. This is a required attribute.

Query Fields	Description
Query	<p>Specifies the base query used in this query viewer. This is a required attribute.</p> <p>If you are creating a new query viewer:</p> <ol style="list-style-type: none"> 1 Click this field to get a drop-down menu showing all available queries on this Manager. You can choose from queries created for reports, for other query viewers, or a new query you created specifically for this query viewer. <p>If you want to create a new query, you need to do this first before creating the query viewer. (See also "Building Queries" on page 228.)</p> <ol style="list-style-type: none"> 2 From the drop-down menu, select the query you want to use. <p>Note: If you are editing an existing query viewer, the Query field is not editable since the base query is set at the time the query viewer is created. If you want to use a different query, create a new query viewer.</p>
Refresh Data After	<p>Sets an amount of time (in minutes or hours) after which the query viewer will automatically re-run and show new data based on that most recent run. This query viewer "refresh" run will repeat, based on the specified refresh time period.</p> <p>The default for this setting is 15 minutes. To change this default:</p> <ol style="list-style-type: none"> 1 Click the field to activate the settings. 2 In the left-hand field, enter a numeral, and in the right-hand drop-down menu, select minute(s) or hour(s).
Query Time Out	<p>Defines a time out limit in which the query must return results. If the query does not complete and send results within the specified time out period, the Manager stops the query run.</p> <p>By default, a time-out of 300 seconds (5 minutes) is configured on the Manager in server.defaults.properties. If you do not specify a Query Time Out in the Attributes tab, this time-out of 5 minutes will apply (even if the Query Time Out field shows "None"). If you specify a time out here, then that one will be used instead of the default.</p> <p>Setting a a time out limit is good practice especially if the event rate (events per second or <i>EPS</i>) is unusually high, start/end time range is large, or the query is complex. Time outs can help guard against infinite or long running queries that impact system performance. Although this is less of an issue with query viewers since they are designed to minimize impact on system performance, this can still be an issue in some scenarios.</p> <p>Setting time outs can be a useful troubleshooting technique for new queries, or existing queries in new scenarios, for example where event counts spike higher.</p>
Default View	<p>The Default View attribute determines how the result data will be displayed when you double-click the query viewer to open the results in the Viewer panel.</p> <p>Define the default (double-click) view format for this query viewer. The choices are to show data as:</p> <ul style="list-style-type: none"> • Table (this is the default) • Pie chart • Bar chart <p>Double-clicking a query viewer in the Navigator will display result data in the format set here.</p> <p>If you choose Pie Chart or Bar Chart as the default view format, choose fields to use for the Values Column (to plot the y axis points on a bar chart or slice sizes on a pie chart) and Points Labels column (to plot the x axis labels on a bar chart or slice labels on a pie chart). The Values Column and Points Labels are also described in Table 10-1, "Configure Chart," on page 166.</p>

Query Fields	Description
Values Column	<p>The Values field applies to bar charts and pie charts. This setting provides fields in the query result that contain data types. The value chosen will be used as the numbers by which to plot the vertical y axis points on a bar chart or the slice sizes on a pie chart.</p> <p>Values typically represent an unknown set of values, like a count. A common example of numeric data appropriate for values is a time like HourOfDay or a count like Count(Event ID).</p>
Point Labels Column	<p>The Point Labels field applies to bar charts and pie charts. This setting provides fields in the query result that contain non-numeric data types. The point labels are used to plot the horizontal x axis labels on a bar chart or the slice labels on a pie chart.</p> <p>Examples of non-numeric data types appropriate for point labels are timestamps, strings such as are used for event names, and different types of addresses such as IP or MAC addresses. Point labels are typically a known set of limited values (like hours in a day denoted by timestamps).</p>
<p>Setting the following attributes (start time, end time, or row limit) in the Query Viewer will override these settings in the base query. (See related information on page 186 about defining the base query in the <i>Query</i> attribute.)</p>	
Start Time	<p>Specifies the starting point for the data gathering.</p> <p>A drop-down menu provides values to select based on Velocity Templates (such as \$Now, \$Now - 1d, and so on). You can also provide a timestamp such as: 27 Jul 2008 16:00:00 PDT.</p> <p>For more on timestamps and timestamp variables, see "Timestamps" on page 779, "Timestamp Variables" on page 780, and "Variables" on page 784.</p>
End Time	<p>Specifies an end point for the data gathering.</p> <p>A drop-down menu provides values to select based on Velocity Templates (such as \$Now, \$Now - 1d, and so on). You can also provide a timestamp such as: 28 Jul 2008 16:00:00 PDT.</p> <p>For more on timestamps and velocity references, see "Timestamps" on page 779, "Timestamp Variables" on page 780, and "Variables" on page 784.</p>
Row Limit	<p>Set the row limit for the data table.</p> <p>The default for all new base queries is the maximum allowable, which is 10,000 rows.</p> <p>If the default is not changed in the base query, and no limit is specified here in the query viewer, the result will show up 10,000 rows of data.</p>

Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes

sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields”](#) on page 552.

Inspect/Edit

Event Inspector | Query Viewer: Event Counts by H...

Attributes | Fields | Variables | Drilldowns | Notes

Query Viewer

Name	Event Counts by Hour of Day
Query	Event Counts Trend Query
Refresh Data After	None
Query Time Out	None
Default View	Table
Values Column	
Point Labels Column	

Common

Resource ID	cFm5wlh8BABCAD-IXWBgdhA==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

Assign

Owner	
Notification Groups	

Creation Information

Created By	admin
Creation Time	20 Feb 2009 17:27:51 PST
Time Since Creation	1 sec(s)

Last Update Information

Last Updated By	admin
Last Update Time	20 Feb 2009 17:27:51 PST
Time Since Last Update	1 sec(s)

Parent Groups

admin's Query Viewers	/All Query Viewers/Personal/admin's Qu...
-----------------------	---

(Name)
(Description)

Name	Value	Use Default
Query Parameters		
Start Time	\$Now - 25h	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Row Limit	10000	<input checked="" type="checkbox"/>

OK Cancel Apply Help

Query Viewer Fields

To define the data display, click the query viewer **Fields** tab.

The screenshot shows the 'Inspect/Edit' dialog box with the 'Fields' tab selected. The dialog has a title bar 'Inspect/Edit' and a subtitle 'Event Inspector' and 'Query Viewer: Event Counts by H...'. The 'Fields' tab is active, showing three sub-sections: 'Data Fields', 'Sort Options', and 'Baselines'.

Data Fields

Name	Alias	Use	Key
HourOfDay	HourOfDay	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Count(Event ID)	Count(Event ID)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TimeStamp	TimeStamp	<input type="checkbox"/>	<input type="checkbox"/>

Sort Options

+ Add... - Remove

Column	Sort Order
TimeStamp	Z-A ↑

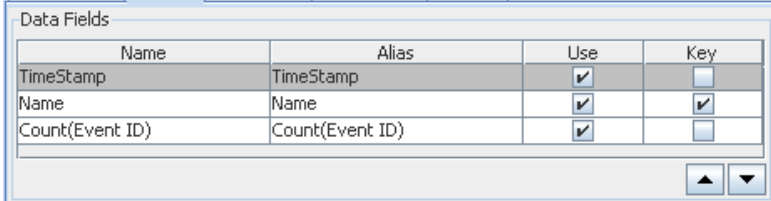
Baselines


- Remove

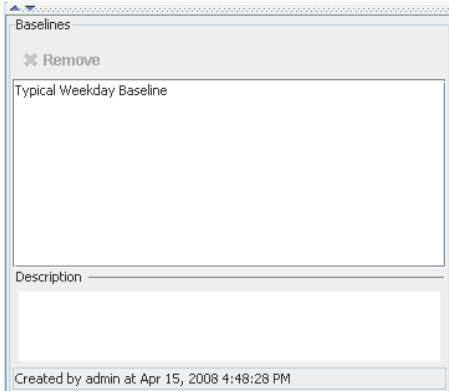

Newest Weekday baseline
WeekDay

Description

OK Cancel Apply Help

Options	Description
Data Fields	<p>The data fields shown on this tab are inherited from the base query. When a query viewer is first created, the data fields are shown here with the same settings they inherited from the base query for "Use" and "Key" fields. So, initially all fields will be enabled for "Use" and fields that are grouped by columns in the base query will show as "Key" fields here.</p> <p>You have the option of overriding the base query settings for "Use" and "Key" settings on inherited data fields in the query viewer. (Settings here do not affect the base query.) You can override these settings when you first create the query viewer, or when you edit it later.</p> <p>Select (checkmark) Use for fields to display in the query viewer results. Fields not selected to "Use" will not show up in the query results.</p> <p>Optionally, you can select one or more fields to use as Key fields. Key fields are columns that can be used to uniquely identify a role in the query. Only the fields selected as keys will be used when doing baseline comparisons.</p>  <p>The query viewer will display results from these columns, showing them from left to right in the order specified. The above settings would result in a query viewer that shows Timestamp as the left-most column, followed by Name, and so forth. You can re-order the columns by selecting a column and clicking the up or down arrow to move it.</p>

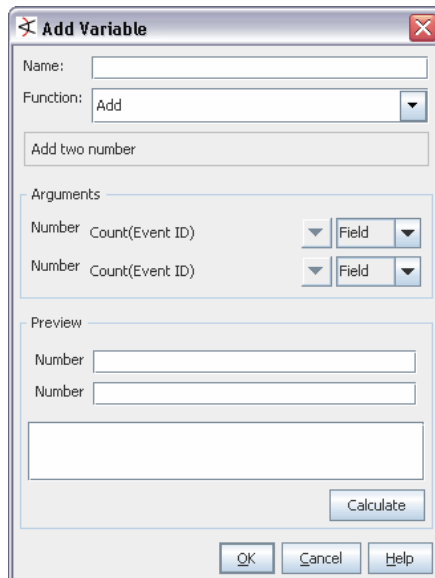
Options	Description						
Sort Options	<p>The query viewer inherits the sort options from the base query, but you can override those sort options here, without affecting the base query.</p> <p>You can add data fields from the base query to sort the query results in the query viewer display.</p> <p>Click Add () to get the list of available fields and select those you want to sort on.</p> <table border="1"> <thead> <tr> <th>Column</th><th>Sort Order</th></tr> </thead> <tbody> <tr> <td>TimeStamp</td><td>Z-A ↑</td></tr> <tr> <td>Count(Event ID)</td><td>A-Z ↓</td></tr> </tbody> </table> <p>In the example above, the Timestamp will be sorted from newest to oldest. Data with the newest Timestamp will show first, at the top of the list. Data with the oldest Timestamp will show last, at the bottom of the list. (This is indicated by the Z-A sort order and up arrow.) In a case where multiple rows have the same Timestamp, these will be sorted by the Count(Event ID) from smallest to largest (as indicated by the A-Z sort order and down arrow).</p> <p>You can change the priority of a column by selecting a column and clicking the up or down arrow to move it.</p> <p>Note: It is possible to sort on fields that you choose not to display in the query result.</p> <p>Suppose you decide to hide the timestamp and count (event ID) columns. In the query viewer Sort Options, you can still sort by Count (Event ID) and Timestamp. The list of event names and results for this query viewer will display in this multi-column sort order by timestamp and count (event ID), but those <i>columns</i> will not show up in the display.</p>	Column	Sort Order	TimeStamp	Z-A ↑	Count(Event ID)	A-Z ↓
Column	Sort Order						
TimeStamp	Z-A ↑						
Count(Event ID)	A-Z ↓						

Options	Description
Baselines	<p>If any baselines have been set on results returned on this query viewer, those are listed in the Baselines area of the Fields tab.</p>  <p>Baselines are created on query results tables via the right-click popup option Investigate > Add as baseline... after a query runs. (See “Defining and Using Baselines” on page 177.)</p> <p>When a query has one or more baselines available, you can compare the current results of a table view with the baseline.</p> <p>To remove baselines from the query viewer, click the Fields tab, select the baseline name, and click Remove ( Remove). Be sure to click OK or Apply on the Query Viewer Editor to save your changes.</p> <p>If you remove the baselines from the query viewer definition, they will not be available on the next run of the query viewer.</p>

Query Viewer Variables

To add a variable, click the **Variables** tab.

- Provide a name for the local variable
- Choose a function from the drop-down Function menu
- Fill in other details as needed and click **OK** to add the variable to the query viewer.



The variable you add here shows up in the following views:

- as a field in the Fields tab in the query viewer editor definition (including the options to **Use** and use as a **Key** field)
- as a column in the query viewer result (If the query viewer result is displayed in the viewer when you add the variable, the variable shows up immediately as a column in the result.)

For example, you can add a Timestamp Function (such as GetHour, GetDayOfWeek, GetDayOfMonth, and so forth).

For more on using variables in resources, see [“Variables” on page 784](#).

Query Viewer Drilldowns

Adding **drilldown** capability to a query viewer provides the user the option of getting more focused views (by means of additional query viewers) on particular aspects of a single item (asset, case, event, and so on) in the query result.

On the Drilldowns tab, you can define one or more drilldowns for a query viewer, along with options for each drilldown.

A drilldown always leads to (is based on) another query viewer. Therefore, the first step in creating drilldown(s) is to define the query viewer(s) that will provide drilldown results. Once the drilldown query viewers are defined, you can add these to the “starting point” query viewer via its Drilldowns tab.

Drilldowns are presented to users on the right-click **Investigate** menu on results displays in the Viewer.

Create Query Viewers for Drilldowns

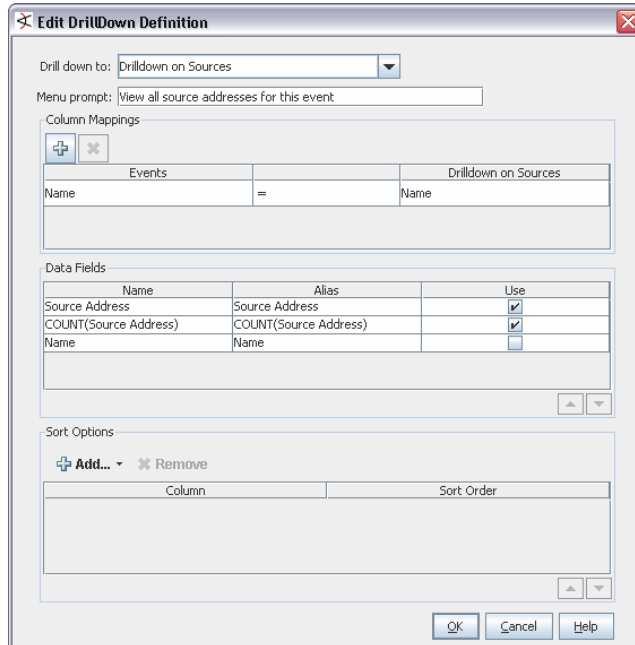
As a first step in adding drilldown capability to a query viewer, decide what kind of information you want the user to be able to focus in on and then create query viewers that get that information.

For example, suppose you have a query viewer that returns the top 10 most frequent events by name. The query viewer might also show timestamps for the events and other information, depending on the base query it leverages and what fields are hidden or shown in the query viewer.

Adding a Drilldown to a Query Viewer

To add a drilldown to a query viewer, click the **Drilldowns** tab.



- 1 Click **Add** () to add a new drilldown definition, mappings, and data fields as described in [Table 10-4, "Add or Edit Drilldown Definition,"](#) on page 194.



- 2 Fill in the fields as described in the following table.

Table 10-4 Add or Edit Drilldown Definition

Option	Description
Drill down to	<p>Select the query viewer to use for the drilldown.</p> <p>This option provides a drop-down menu for navigating the query viewer tree and selecting a query viewer for the drilldown.</p>
Menu prompt	<p>Provide a description of the drilldown for the Investigate menu prompt.</p> <p>The user will see the text you provide here as a drilldown option on the right-click Investigate menu for this query viewer.</p> <p>Note: Drilldowns are available to users only when they view a query viewer result in table format (View Data As > Table).</p>

Option	Description
Column Mappings	<p>The left side of the Column Mappings shows the columns from the source query viewer (the one you are drilling down <i>from</i>).</p> <p>The right side of the Column Mappings shows the columns from the target query viewer (the one you are drilling down <i>to</i>).</p> <p>For example, the Drilldown definition shown in the figure in Step 1 on page 194 maps the source query viewer "Name" column to the target query viewer "Name" column. This will construct the following drilldown filter:</p> <pre><target>.Name = <source>.Name</pre> <p>where <code><source>.Name</code> will be replaced by the actual value from the source query viewer row.</p> <p>You can add or remove column mappings, but your choices are limited to the columns already provided in the query viewer, and field mappings need to be consistent.</p> <p>A field mismatch will trigger an error. For example, mapping a name to an IP address is not allowed.</p> <p>For a summary of usage notes, see "Tips on Drilldown Definitions" on page 195.</p>
Data Fields	<p>Data fields are inherited from the query viewer selected for the drilldown. By setting options here you can choose a subset of columns and/or show them in a different order.</p> <p>Settings on data fields here override other query viewer settings.</p> <ul style="list-style-type: none"> You can choose to show (check Use) or hide (uncheck Use) the data fields in the drilldown query viewer result. You can reorder the data fields. To do this, select a data field, then click the up  or down  arrow buttons. (The buttons are on the right, below the Data Fields list). <p>For a summary of usage notes, see "Tips on Drilldown Definitions" on page 195.</p>
Sort Options	<p>Sort options on a drilldown override other query viewer sort settings, and provide an different way of sorting.</p> <p>Click Add to add a field in the query viewer as a column to sort on before displaying.</p> <ul style="list-style-type: none"> Column Sort Order <p>Only fields available in the query viewer being drilled down to are provided as sort options here.</p> <p>To remove a sort on a field, select a column in the Sort Options list and click Remove.</p>

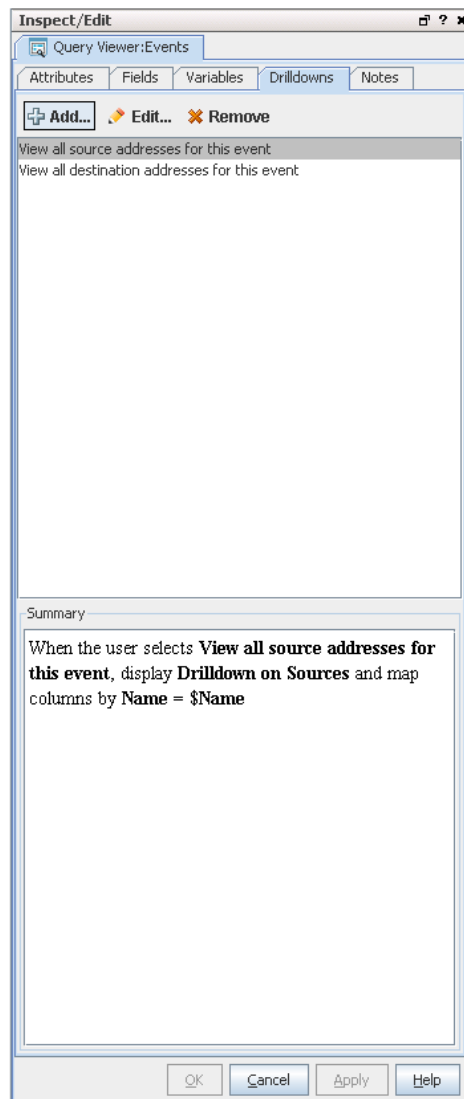
Tips on Drilldown Definitions

- ◆ Drilldowns can be defined for multiple fields of different data types. For example, you could define a drilldown to return a combination of event name and IP

address. The first step would be to define a base query viewer to return these fields in a result (see [“Create Query Viewers for Drilldowns” on page 193](#)), and then, as a next step, add a drilldown and select that query viewer to use as the “Drill down to” query viewer.

- ◆ Drilldowns cannot be defined to go to fields that are SQL functions.
 - ◆ Column and Data Field mappings need to be consistent; a field mismatch will trigger an error. For example, mapping a name to an IP address is not allowed.
- 3 Click **Apply** to save the drilldown and keep the query viewer editor open (or click **OK** to save the drilldown and close the query viewer editor).


The “Drilldown to” description is listed on the Drilldowns tab after you click Apply. You can add multiple drilldowns to the same query viewer. All drilldowns are shown on this tab.



Editing a Drilldown

To edit a drilldown:


- 1 If you have not done so already, open the editor for the query viewer you want to edit. (See [“Editing a Query Viewer” on page 197](#).)
- 2 Click the **Drilldowns** tab.

- 3 Select the drilldown you want to edit and click **Edit** .

The drilldown dialog for this drilldown is displayed. Make changes to the fields and options as described in [“Adding a Drilldown to a Query Viewer” on page 194](#).

Removing a Drilldown


To remove a drilldown from a query viewer:

- 1 If you have not done so already, open the editor for the query viewer you want to edit. (See [“Editing a Query Viewer” on page 197](#).)
- 2 Click the **Drilldowns** tab.
- 3 Select the drilldown you want to edit and click **Edit** .

Editing a Query Viewer

- 1 Navigate to **Query Viewers** in the Navigator panel and select the query viewer you want to modify.
- 2 Right-click the query viewer and select **Edit Query Viewer** from the context menu. This launches the Query Viewer Editor in the Inspect/Edit panel, and shows the definition for the selected query viewer.
- 3 Edit the query viewer definition as needed. (See [“Customizing Query Viewers” on page 184](#) for details.)
- 4 Click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query Viewer editor without saving changes.)



To edit a query viewer for which results are currently displayed in the Viewer, click the Edit Query Viewer button  on the lower right of the Viewer. The results display for the query viewer you want to edit must have focus (i.e., be on top) in the Viewer.

Deleting a Query Viewer

- 1 Navigate to **Query Viewers** in the Navigator panel, right-click the query viewer you want to delete, and select Delete Query Viewer.

A confirmation dialog is displayed.
- 2 Click **Delete** to confirm your choice and delete the query viewer. (Or click **Cancel** if you decide you do not want to delete it.)

Example Queries for Common Scenarios

Query viewers can be used to monitor daily network traffic and get high level summaries of typical activity. Query viewers can also be used drill down on anomalies or other interesting events.

Following is a brief, conceptual scenario of how an *analyst* might use query viewers to *monitor and investigate* certain types of activity.

Also included here is a description of how the *query content developer* might **build and configure** the base query and query viewers that the analyst uses.



In practice, ArcSight ESM ships with pre-built queries and query viewers as standard content. It is likely that the types of resources described here will be provided with ArcSight ESM.

Even so, the configuration of the base query and query viewers is described to illustrate and support this example, and show how a content developer might fine tune these resources to gather the information needed.

Basic Analysis High Level Summaries

A security analyst wants to check if anything unusual is happening on their system. He or she brings up a query viewer called “Events” that shows all events by event name for the last 2 hours. The columns include:

- Event name
- Total count of all events
- Count by unique source address
- Count by unique destination address

Analyst’s First View of Events

The analyst can easily glance at the data and see if anything looks out of the ordinary. Columns can be sorted and filters can be changed to refine the details. The data should come up almost immediately.

Viewer			
Live Events: Table			
Query: Events		114 shown / 114 matches	
Last Update: 18 Jun 2008 10:08:20 PDT			
Filter: No Filter			
Name	COUNT(Events)	COUNT(Source ...)	COUNT(Destina...)
ActiveList entry expired	338	0	1
ActiveList entry updated	2979	0	1
AddToList: Success	3213	0	1
Agent [Nifty Event Player] reconnected	1	1	1
Agent Login	2	1	1
Agent [Nifty Event Player] heartbeat time...	1	0	1
Agent [Nifty Event Player] type [testalert...	1	0	0
Agent updated	2	1	1
Application Event Counts	8	0	0
ArcSight Event Flow Statistics	9	0	0
ArcSight Manager Started	1	0	1
ArcSight User Login	1	1	0
Asset updated	40	0	1
AttachmentOnlyGroup [Package] inserted	1	1	1
Attack From Suspicious Source	2	1	1
Attack Rates by Attacker Zone	2	0	0
Attack Rates by Service	2	0	0
Attack Rates by Targeted Zone	2	0	0
Attacker Zones by Service	2	0	0
Case inserted	2	0	1
Case updated	2	0	1
Channel [Last Hour] got attached	1	1	1
Channel [Last Hour] query completed	2	0	1
Channel [Live] got attached	1	1	1
Channel [Live] query completed	2	0	1
Compromise - Success	2	1	1
Connector Down	1	0	0
Connector Still Down	2	0	0
Connector Up	1	0	0
CreateNewCase: Success	2	0	1
Data Monitor Entry Timeout	1	0	1
6/18 8:08:20 - 6/18 10:08:20			

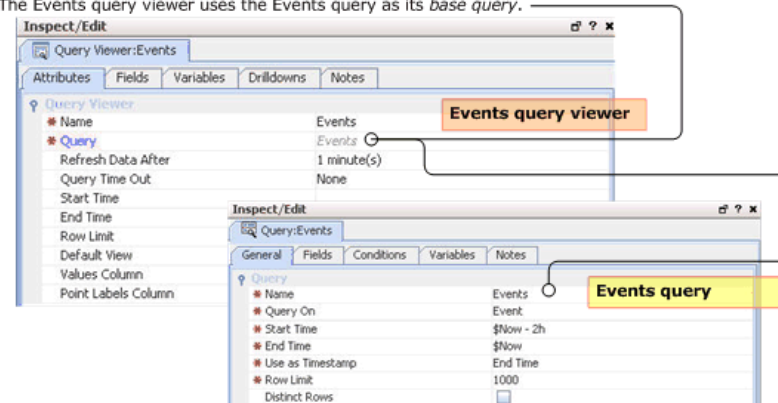
How the Events Query Viewer is Built

The **Events query viewer** described in this example leverages the Events query

Attributes

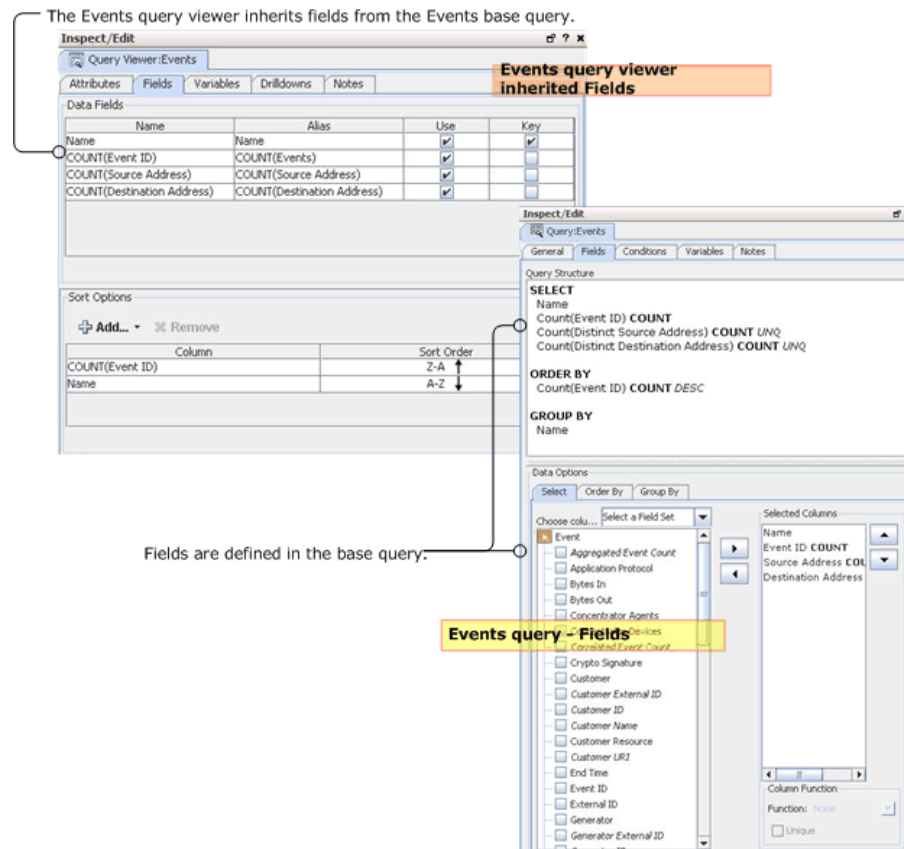
Bringing up the *query viewer editor* for the **Events query viewer** shows that the Events query is used as the base query. Bringing up the **Events query** (base query) in the *query editor* shows that the base query searches on events for the last 2 hours. (Queries are under Reports > Queries in the Navigator.)

The Events query viewer uses the Events query as its *base query*.



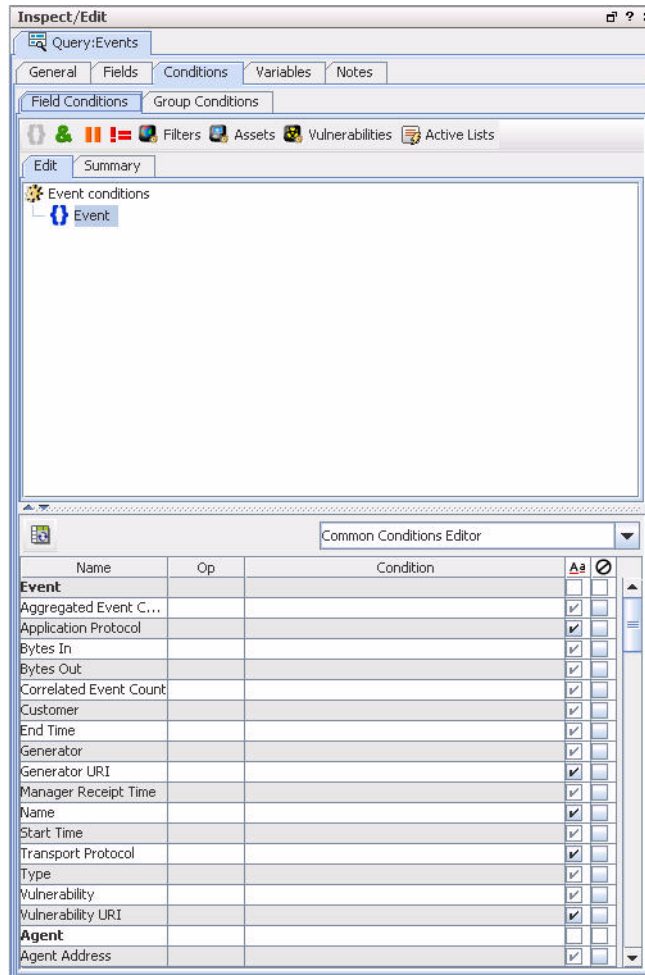
Fields

The fields selection, order by, and group by logic are all defined in the Fields tab for the base query. The Events query viewer inherits the fields from the base query. These show up on the query viewer Fields tab.



Events Base Query Conditions Tab

The condition logic to search on Events is defined in the Conditions tab for the base query.



Drill-Down Example

Continuing with the previous example, the security analyst notes that one of the counts seems troublesome. For example, "Attack from Suspicious Source" is high and showing a lot of unique destination addresses. The analyst would right click on this row and choose **Show Source Addresses**.

The resulting query viewer would show, for this event and time range, the source addresses, as well as other columns of interest (e.g.: destination address). Then by sorting by source address, the analyst could decide if a single source address (probably with the highest count) was the initiator of most of the attacks. This information could also be provided from an appropriate backend trend table (the same one or a different one), and, as a result, the display should come up almost immediately.

The screenshot shows the ArcSight Viewer window with the title bar 'Viewer'. The main content area displays a table titled 'Drilldown on Sources: Table'. The query is 'Drilldown-src' and it shows 13 matches. The last update is '1 Aug 2008 18:24:12 PDT'. The filter is 'Name = "ICMP PING"'. The table has two columns: 'Source Address' and 'COUNT(Source Address)'. The data is as follows:

Source Address	COUNT(Source Address)
4.158.210.103	1
63.193.245.15	482
64.185.36.108	1
81.43.59.4	1
165.247.165.115	2
203.87.70.177	1
203.203.198.49	1
209.179.130.133	1
209.209.220.94	1
209.214.97.116	1
209.240.160.175	1
218.15.205.24	1
218.52.201.132	1

The status bar at the bottom shows the time range '8/1 16:22:58 - 8/1 18:22:58'.

The analyst could also show **destination** addresses for the same event row, if that drilldown is defined as a part of the query viewer.

The screenshot shows the ArcSight Viewer window with the title bar 'Viewer'. The main content area displays a table titled 'Drilldown on Destinations: Table'. The query is 'Drilldown-dst' and it shows 7 matches. The last update is '1 Aug 2008 18:31:53 PDT'. The filter is 'Name = "ICMP PING"'. The table has two columns: 'Destination Address' and 'COUNT(Destination Address)'. The data is as follows:

Destination Address	COUNT(Destination Address)
111.222.101.10	1
111.222.101.20	4
111.222.101.21	3
111.222.101.30	2
111.222.101.140	2
111.222.101.174	1
111.222.121.206	577

The status bar at the bottom shows the time range '8/1 16:31:43 - 8/1 18:31:43'.

How the Drilldowns are Built

The source and destination drilldowns are added to the Events query viewer on the Drilldowns tab at content development time.

Here is the drilldown on sources defined in the Events query viewer example.

The 'Edit DrillDown Definition' dialog box is shown with the title bar 'Edit DrillDown Definition'. It contains the following sections:

- Drill down to:** A dropdown menu set to 'Drilldown on Sources'.
- Menu prompt:** A text box containing 'View all source addresses for this event'.
- Column Mappings:** A section with a '+' and '-' icon. Below it is a table:

Events			Drilldown on Sources	
Name	=		Name	
- Data Fields:** A table with columns 'Name', 'Alias', and 'Use'.

Name	Alias	Use
Source Address	Source Address	<input checked="" type="checkbox"/>
COUNT(Source Address)	COUNT(Source Address)	<input checked="" type="checkbox"/>
Name	Name	<input type="checkbox"/>
- Sort Options:** A section with an 'Add...' button and a 'Remove' button. Below it is a table:

Column	Sort Order
--------	------------

At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Here is the drilldown on destinations defined in Events query viewer example.

The 'Edit DrillDown Definition' dialog box is shown with the title bar 'Edit DrillDown Definition'. It contains the following sections:

- Drill down to:** A dropdown menu set to 'Drilldown on Destinations'.
- Menu prompt:** A text box containing 'View all destination addresses for this event'.
- Column Mappings:** A section with a '+' and '-' icon. Below it is a table:

Events			Drilldown on Destinations	
Name	=		Name	
- Data Fields:** A table with columns 'Name', 'Alias', and 'Use'.

Name	Alias	Use
Destination Address	Destination Address	<input checked="" type="checkbox"/>
COUNT(Destination Address)	COUNT(Destination Address)	<input checked="" type="checkbox"/>
Name	Name	<input type="checkbox"/>
- Sort Options:** A section with an 'Add...' button and a 'Remove' button. Below it is a table:

Column	Sort Order
--------	------------

At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Non-Event Analysis Example

A security analyst wants to examine "Asset Counts by Vulnerability". The analyst selects this viewer and gets the most recent result (from a trend run) and can examine a table containing columns: Vulnerability and Asset Count. Right clicking on a particular vulnerability row would allow drilldown into the assets with that vulnerability.

Baseline Analysis for Data Comparison

Continuing with the previous example, the security analyst notes that one of the counts seems significantly higher than last recalled. The analyst right clicks on the query viewer and selects "Compare with Baseline", from which there are zero or more baselines to choose.

This will make additional columns available to the currently displayed viewer that can be added by the user. For example, a new column could be added next to the current "Count" column showing "Count - <Selected Baseline>". This will be a comparison number showing the difference between the current value of the count and the baselined value for the count. This will be positive, negative, or empty (if a baseline doesn't exist for this vulnerability). The analyst will be able to right click on the new column to sort this column in ascending or descending order.

Other options available to the analyst would be:

- **Add as Baseline...** to save the current values in the display as the new named baseline.
- **Compare with...** to compare to any other set of data available in the trend table.

History Analysis Example

As hinted in the previous example, any previous trend runs can be used for baseline comparison. Similarly, the analyst can change the query viewer to go back into the past to look at previous data. The analyst could use the default baseline and go back in history to see when some count began to significantly differ from the baseline.

Chapter 11

Building Reports

These topics describe how you use ArcSight to monitor enterprise security.

[“Understanding Reporting Workflow” on page 205](#)

[“Using Report Templates” on page 209](#)

[“Building Queries” on page 228](#)

[“Building Trends” on page 241](#)

[“Creating Reports” on page 251](#)

[“End-to-End Reporting Examples” on page 272](#)

Reports are captured views or summaries of data that can be viewed in the ArcSight Console or exported for sharing in a variety of file formats. Reporting is an essential tool for communicating the state of your enterprise security to internal and external stakeholders. ArcSight ESM 4.0 introduces a whole new architecture for how reports are designed, created, and maintained.

Reporting is a broad subject in ArcSight. Because it can use all the scheduling, conditional logic, resource- and rules-based filtering capabilities of the system, the possibilities can take some time to explore. Creating a report is a multi-step process that can involve steps using several different resources.

Understanding Reporting Workflow

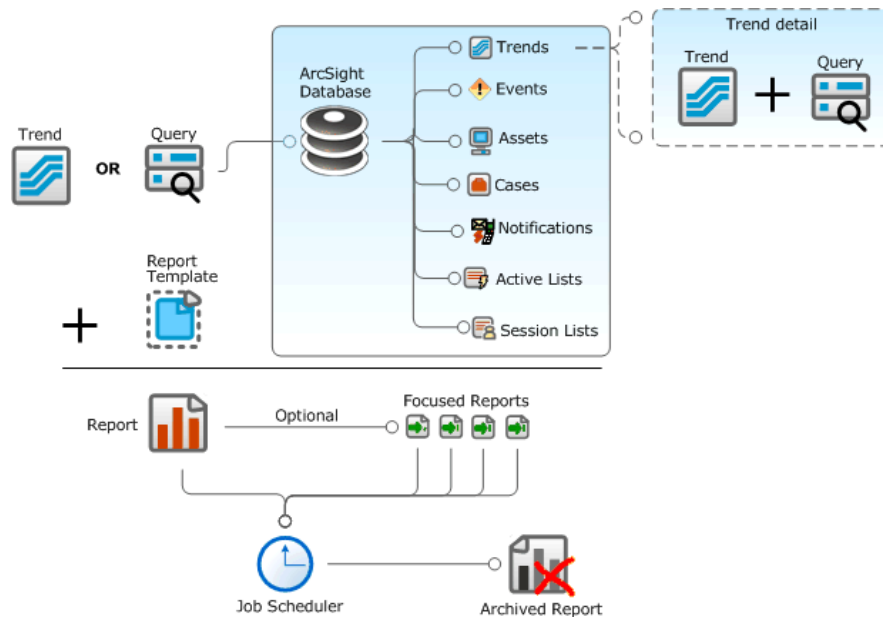
Building Reports is a multi-step process that involves use of a few different data gathering and reporting tools. ArcSight Enterprise Security Management (ESM) can gather report data using standard queries or trends.



Reports can be relatively simple (you can create a report with the Report Wizard based on the results of a single query) or complex (you can create a report based on the results of layers of queries and trends that feed data results up the chain as the basis for new queries). See [“End-to-End Reporting Examples” on page 272](#) for examples of both basic and complex reports.

Following is a quick overview of reporting workflow tasks and tools, along with a reminder about dependencies among reporting resources.

For a more in-depth description of how these elements build on each other to create various views of the data, see also [“Query-Trend Relationships in Reporting” on page 242](#).



1. Build a Query

A query is an ArcSight resource that defines the parameters of data you want to gather from an ArcSight data source. The results of the query then become the basis for one or more ArcSight report(s) and/or trend(s). As a data source, queries can use the ArcSight database of events, assets, cases, notifications, active lists, session lists, or data gathered from a trend.

Queries are described in [“Building Queries” on page 228](#).



If all you want to do is build a report based on a single query, at this point you can skip to step 4 and select a template. (See [“4. Select or Design a Report Template” on page 207](#).)



Queries built for reports can be used in query viewers also.

And if you want to run quick SQL queries for monitoring and analysis outside of the reporting resource, you can use query viewers, a new feature in ArcSight ESM 4.5. You can add query viewers to dashboards and generate simple reports on query viewer results.

For information on query viewers, see [Chapter 10, Query Viewers, on page 161](#).

2. Build a Trend (Based on a Query)

A trend is an ArcSight resource that defines how and over what time period data will be evaluated for trends. A trend is always based on a query. The trend results are stored in a trend table in the ArcSight database, and are themselves queryable. Trends can also be used as the primary data source for a report.

Trends are described in [“Building Trends” on page 241](#).





If you want a report based on a single trend-query, at this point you can skip to step 4 and select a template. (See [“4. Select or Design a Report Template” on page 207](#).)

3. Build a Query (Based on a Trend)

At this point you have the option of using a simple query or trend in a report, or you can further refine query results by using a trend in another query.


See the [“Building Queries” on page 228](#) and [“Building Trends” on page 241](#) for more information on how to do this.

<p>Data Gathering: Query Building</p>  <p>Query source data</p> <ul style="list-style-type: none"> Specify the data you want to work with Narrow the results by setting conditions and variables 	<p>Data Gathering: Trend Defining</p>  <p>Is data a trend?</p> <ul style="list-style-type: none"> Design interval trend to operate on events Design snapshot trend to operate on assets, network model, cases, and notifications
---	--

4. Select or Design a Report Template

Use an existing report template layout or create your own using the new Report Designer tool. For information on working with templates, see [“Using Report Templates” on page 209](#).

Layout Designing



Design report template

- Using a stock template?
- Design your own: chart, table, combination

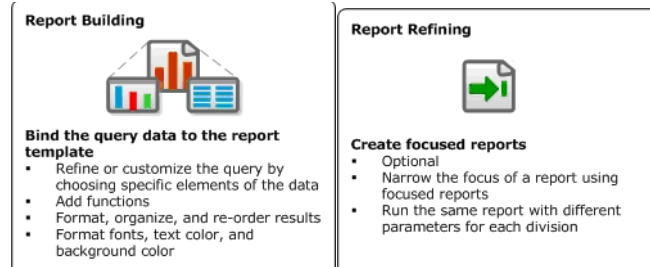
5. Create a Report

A report is an ArcSight resource that binds data from a query or trend to an existing report template. Once run, the results of a report can be viewed in the Console Viewer panel, saved (archived), and/or exported in a variety of formats. Reports can be scheduled to run at regular intervals, and also can be run on demand as needed.

Reports are described in [“Creating Reports” on page 251](#), and an overview of the whole topic is provided in [Chapter 11, Building Reports, on page 205](#).

Focused reports enable you to run the same report definition on different subdivisions of the data without having to copy and modify the master report every time. For example, you can run an individual Top 10 Infected Systems report for each of your business divisions.

The job scheduler enables you to schedule reports and focused reports to run automatically at specific time intervals. (The job scheduler is also used as a part of building trends which, by nature, involve scheduling.)



Queries and trends are intended to capture data. Reports are used to display the data from queries and trends. For example, if you wanted to run monthly or quarterly reports on VPN login statistics, you would first create one or more queries to capture the data, then create trends (based on the queries) to define a schedule for running the queries and storing the results, and finally create and run reports on the trends. For a full walk-through of this process, see [“End-to-End Reporting Examples” on page 272](#).

6. Run a Report

ArcSight ESM ships with a set of ready-made reports available under the Reports resource. (For example, on the Navigator panel under the Reports resource look in /Reports/Shared/All Reports/ ArcSight Solutions/. Open the sub-groups (folders) to see provided reports.)

For information on how to run an existing report, see [“Running Reports” on page 287](#) and [Running a New or Archived Report](#).

7. Archive and Maintain Reports

After running a report, you can elect to save (archive) the report results. This enables you to retrieve a particular report for immediate viewing without having to regenerate the report. Reports that are run on demand are saved on the Archives tab just like scheduled reports. If the Save Output option is chosen for an on-demand report, the archived report has an expiration date of 6 months from the time it was run (by default). If the Save Output option is not chosen for an on-demand report, the report is maintained in the archive for one day only.

Archived reports can also be sent to a notification group after the scheduled report is run.

For information on how to archive and maintain reports, see [“Archiving Reports” on page 294](#) and [“Managing Reports” on page 291](#).



Managing Dependencies for Reports Resources

As you work with these resources, please keep in mind that queries, trends, and reports generally have multiple dependencies upon each other. Modifying some elements within one resource can affect another. If modifications to a resource impact another to the extent that the dependent resource is rendered unusable, errors will be reflected in the Console. ArcSight ESM manages and updates most of these resources and dependencies automatically, but not all.

For example, a trend built on a query relies on a set of fields (columns) contained in the base query. If you modify fields in the base query that are used in the trend, the trend will be disabled. (The proper approach for modifying a query used in a trend is to create a new trend.) Similarly removing a resource (like a query) that another resource (like a report) depends on will generate error messages on the Console.

Using Report Templates

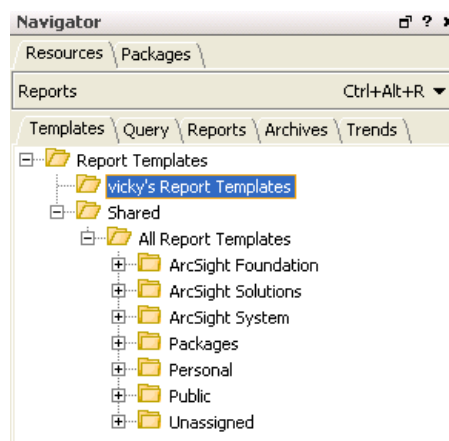
To provide more flexibility in reporting, ArcSight now offers powerful report template tools including a rich offering of ready-made templates and a template design wizard for more customized reports. Template definitions determine how query and trend data are displayed in a report. You can create and adjust templates to specify which data is displayed, what visual elements are used (variations on tables, charts, graphs, and so on), the layout of those elements, the report output file format, and much more. A template consists of report design elements, such as headers, footers, title bars, charts, and tables, arranged on a page according to a layout specification.

Templates can accommodate input from multiple queries and show multiple visual elements, such as three charts and a table each pulling from a different data source, in a single report.

You can use the templates provided or create custom templates with the report template designer.

Navigating to Templates

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Templates** tab.



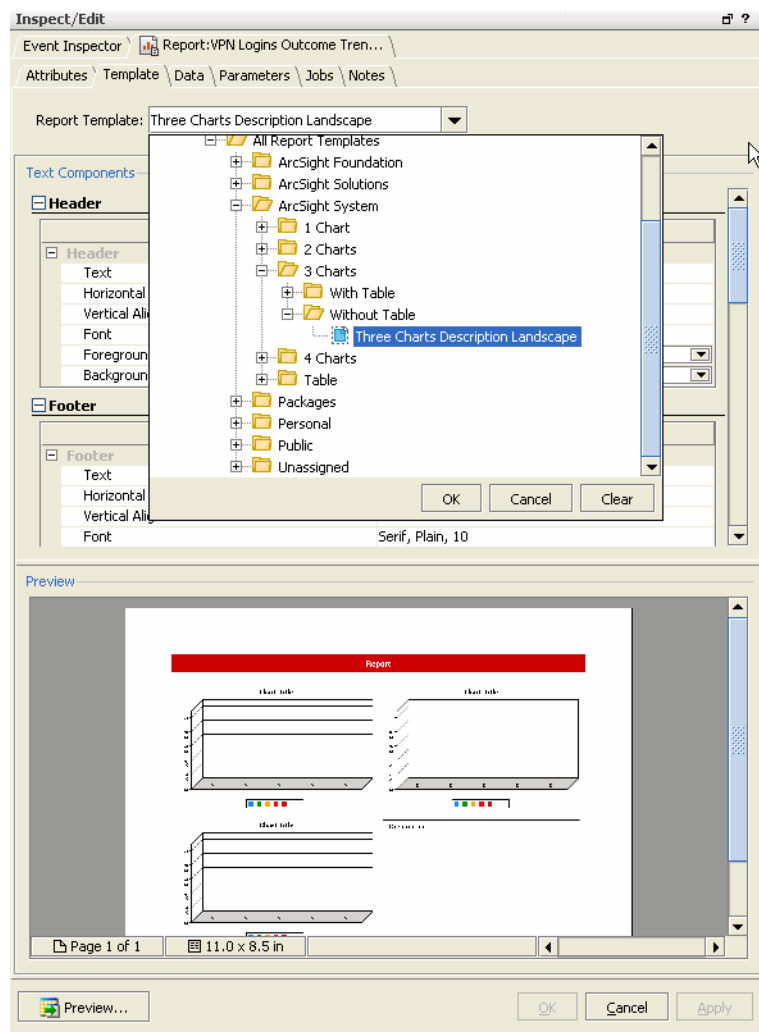
Report templates are a component of ArcSight Reporting resource tools. Be sure to see [“Building Reports” on page 205](#) for an overview of all reporting tasks and tools.

Using Standard Templates

To get you started, ArcSight provides a rich set of templates you can use as-is or copy to use as a starting point for your own template layouts. There are two ways to use standard templates for reports. You can apply a template to an existing report, or you can create a new report based on a template.

Applying a Template to an Existing Report

- 1 With the **Reports** resource selected in the Navigator panel, click the **Reports** tab.
- 2 If Reports groups (folders) are collapsed, click **+** to expand user and Shared folders and view reports.
- 3 Double-click the report to which you want to apply a template. (Alternatively, you can select the report, right-click and select **Edit Report** from the context menu.) This brings up the Report editor in the Inspect/Edit panel.
- 4 In the Report editor, click the **Templates** tab for the selected report.
- 5 In the **Report Template** field drop-down menu, select a template.
- 6 Click **OK** to apply the template and close the file browser.
- 7 Click **Apply** or **OK** to verify and save the template choice for the selected report.



Creating a New Report Based on a Template

- 1 With the **Reports** resource selected in the Navigator panel, click the **Templates** tab.
- 2 Right-click your user folder (group) and select **New Report from Template**. This launches the Reports Editor in the Inspect/Edit panel with the chosen template.
- 3 See [“Creating Reports” on page 251](#) for details on how to define data for your report and fine-tune the template by means of the Template tab in the Report editor for this report.

Copying a Template

An easy way to get started customizing a template is to copy an existing template and modify it to suit your needs. To copy a template:

- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Open the All Report Templates folder, navigate to a template you want to copy, and select it.
- 4 Left-click, and drag and drop the selected template into your user folder.
- 5 Select **Copy** from the Drag & Drop Options dialog. A copy of the template is dropped into your user folder.

Alternatively, you can select the template you want to copy in the Navigator and choose **Edit > Copy** from the menus. Then select your user folder and click paste to drop the template into the folder.

Opening the Designer to Edit a Template

- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Right-click a template and choose **Open in Designer**, or choose **Edit Template** and click the **Open in Designer** button on the Attributes tab for the template editor.

For more about using the template Designer, see [“Designing Custom Templates” on page 211](#).

Designing Custom Templates

You can use the report template designer to create report templates specific to the needs of your organization. This can be useful, for example, if you need to customize reports per corporate branding, policy requirements, or standards compliance. This can be useful, for example, if you need to customize reports per corporate branding, policy requirements, or standards compliance. (You can also copy the stock templates and use the Designer to modify these templates to suit your needs.)

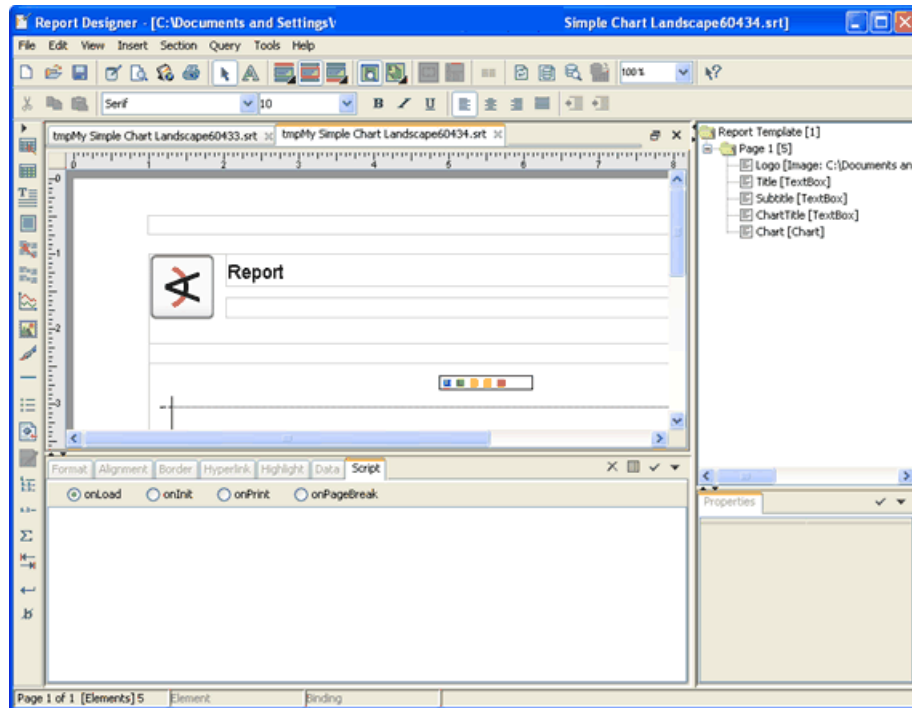
Opening the Template Designer to Edit Existing Templates

- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Right-click a template and choose **Open in Designer**, or choose **Edit Template** and click the **Open in Designer** button on the Attributes tab for the template editor.

Creating a New Template

To design a custom template, you need to first create a new template then launch the report designer wizard:

- 1 With the Reports resource selected in the Navigator panel, click the **Templates** tab.
- 2 Select the template group (folder) where you want to store your new template. (We suggest that you create new content in your user folder. The name of this folder depends on the user name with which you logged into the Console.)
- 3 Right-click and select **New Template** from the context menu. This brings up the Template editor in the Inspect/Edit panel.
- 4 Provide a **Name** for the new template in the Template Editor and click **OK**. (Your new template is now displayed in the group you selected in the Navigator.)
- 5 In the Navigator panel, select the template you just created, right-click, and select **Launch Designer** from the context menu. This starts the Report Designer, as shown below. Use the Report Designer to create custom templates.



From the Report Designer menus, you can launch wizards for building common report elements such as **Section > Section Wizard** and **Query > Table Wizard**.

Template Designer User Interface

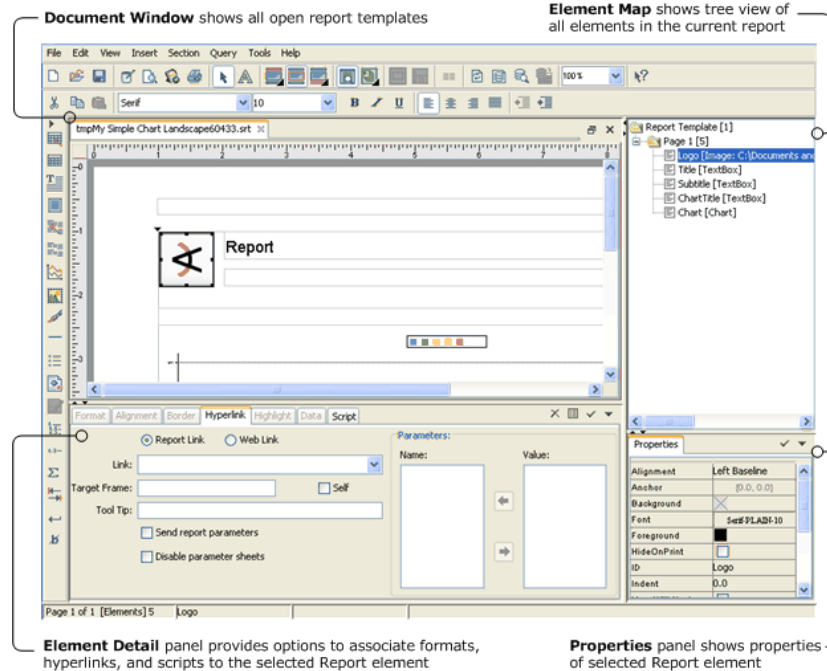
The Report Template Designer provides options for creating fully customized report templates. These topics introduce the Designer features and functions, and provide a quick tour of the user interface (UI).

Tour of Designer UI

The Report Template Designer user interface (UI) consists of the following panels and tools. See also [“Menus” on page 214](#) and [“Toolbars” on page 217](#) for detailed descriptions of those options.

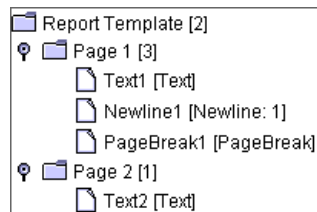
Overview Diagram

Report Template Designer: You can use the Report Designer to create custom templates. To launch the Report Template Designer, right-click a template in the Navigator and choose Open in Designer, or choose Edit Template and click the Open in Designer button on the Attributes tab for the template editor.



Element Map

The element map displays a hierarchical tree view of all elements in the current report. The element map appears in a frame between the report element toolbar and the document window, and looks like this:



Selecting an element on the element map will cause that element to be selected in the report.

To display the element map, click **Element Map** on the **View** menu.

Document Window

The document window is the largest window on the Report Designer screen and contains all the currently opened report templates. Reports can be minimized, maximized, resized and moved within the document window.

- To arrange open report templates, click **Cascade** on the **Window** menu.
- To change the active report template, click the template's file name on the **Window** menu.

Status Bar

The status bar appears at the very bottom of the Report Designer application window and looks like this:



The information displayed on the status bar, from left to right, is as follows:

- Current page number
- The number of elements in the current page
- The ID of the currently selected report element
- Information about the currently selected report element: ID and element type

Change the Report View

Normal View

Click the **View** menu
Check the checkbox button to the left of **Layout View**

or

Click the **Layout**  toolbar button when the report is in page layout view



Page Layout View

Click the View menu
Uncheck the checkbox button to the left of **Layout View Change the Editing Mode**


or

Click the **Layout**  toolbar button when the report is in normal view.

Change the Editing Mode

- To switch to Element Selection Mode, click the **Selection Mode (Pick Tool)**  toolbar button.
- To switch to Text Mode, click the **Text Mode (Text Tool)**  toolbar button.

Change the Report Magnification

To increase or decrease the display size of the report (zoom in or zoom out), select the magnification percentage from the drop-down list  on the toolbar.

Menus

The Report Template Designer menus are described in the following tables.

Table 11-1 File Menu

Menu item	Description
New	Creates a new Style Report template.
Save	Saves the current report template.
Export	Exports the current report in one of the following formats: PDF, HTML, Excel, RTF, SVG, CSV, or Text.
Preview	Displays a preview of the generated report in a new window.

Menu item	Description
Print	Prints the current report.
Page Setup	Sets the current report's page format properties.
Most recently used file list	These menu items display the most recently opened reports. Clicking one of these items will open the corresponding report template in a new window.
Exit	Exits the Report Designer.

Table 11-2 Edit Menu

Menu item	Description
Undo	Reverses, one at a time, a series of editor actions.
Copy	Copies the current selection to the clipboard.
Cut	Deletes the selection from the report and copies it to the clipboard.
Paste >> Into Page	Inserts the contents of the clipboard into the current document.
Paste >> Into Section	Inserts the contents of the clipboard into selected Section element.

Table 11-3 View Menu

Menu item	Description
Layout View	Sets the report view to either Normal view or Layout view.
Element Map	Displays a tree mapping all report elements on the page in a frame to the left.
Ruler	Sets the visibility of the ruler.
Grid	Sets the visibility of the grid.
Snap To Grid	Sets whether inserted report elements should be placed at the nearest grid vertex or not.
Properties	Displays the properties dialog for the selected report element.
Console	Displays the error console.

Table 11-4 Insert Menu

Menu item	Description
Header	Elements will be inserted into the page header.
Body	Elements will be inserted into the page body.
Footer	Elements will be inserted into the page footer.
Basic Element >> Table	Inserts a table.

Menu item	Description
Basic Element >> Text	Inserts a text element.
Basic Element >> Textbox	Inserts a text box.
Basic Element >> Image	Inserts an image.
Basic Element >> Chart	Inserts a chart.
Basic Element >> Tab	Moves the insertion point to the next tab stop.
Basic Element >> Bullet	Inserts a bulleted item.
Basic Element >> Separator	Inserts a horizontal line across the page.
Spacing Element >> Newline	Inserts a newline.
Spacing Element >> Break	Inserts a line break.
Spacing Element >> Space	Inserts a non-breaking space.
Spacing Element >> Page Break	Inserts a page break.
Spacing Element >> Conditional Page Break	Inserts a page break that only occurs when the specified condition(s) is met.
Spacing Element >> Area Break	Inserts an area break.
Special Field >> Table of Contents	Inserts a table of contents.
Special Field >> Page Number	Inserts a text element displaying the current page number into the header or footer.
Special Field >> Page Count	Inserts a text element displaying the page count into the header or footer.
Special Field >> Date	Inserts a text element displaying the current date into the header or footer.

Table 11-5 Format Menu

Menu item	Description
Preference	Displays the formatting preferences dialog.
Draw Area	Inserts a new page area into the report template.
Order Area	Changes the flow order of the page areas in the report template.

Table 11-6 Window Menu

Menu item	Description
Cascade	Places all document windows in a cascading arrangement.
Close All	Closes all document windows.
Window list	This list contains a menu item for each open document window. Clicking on one of these items will bring the corresponding window to the foreground.

Toolbars

The Report Template Designer toolbars are described in following tables.

Table 11-7 Standard Toolbar











Toolbar button	Description
 Save	Saves the current report template.
 Preview Report	Displays a preview of the generated report in a new window.
 Print	Displays the print dialog, allowing the user to print the active document.
 Selection Mode (Pick Tool)	Switches to element selection mode.
 Text Mode (Text Tool)	Switches to text editing mode.
 Cut	Copies the current selection to the clipboard and deletes the selection from the report.
 Copy	Copies the current selection to the clipboard.
 Paste	Inserts the contents of the clipboard into the current document.
 What's This	Clicking on this item and then on a menu item, toolbar button or window region will display help information on what was clicked.

Table 11-8 Layout Toolbar

Toolbar button	Description
 Header	Elements will be inserted into the page header.










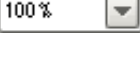







Toolbar button	Description
 Body	Elements will be inserted into the page body.
 Footer	Elements will be inserted into the page footer.
 Element Map	Sets the report view to Normal Layout view, with a tree mapping all report elements on the page in a frame to the left (in Report Designer).
 Layout View	Switches between Normal and Layout views, and displays the page layout properties dialog.
 Draw Area	Inserts a new page area into the report template.
 Order Area	Changes the flow order of the page areas in the report template.
 Columns	Places two page areas side-by-side on the page to split the report into columns. The areas flow from left to right.

Table 11-9 Format Toolbar

Toolbar button	Description
 Font	Sets the current font.
 Font Size	Sets the current font size.
 Zoom	Zooms in and out according to the percentage selected.
 Bold	Makes text boldface.
 Italic	Renders the current text in italics.
 Underline	Underlines the current text.
 Left Justify	Changes the alignment to left justification.
 Center	Changes the alignment to center justification.
 Right Justify	Changes the alignment to right justification.
 Fill	Changes the alignment to fill justification.













Toolbar button	Description
 Decrease Indent	Decreases the current indentation.
 Increase Indent	Increases the current indentation.

Table 11-10 Report Element Toolbar

Toolbar button	Description
 Table	Inserts a table.
 Text	Inserts a text element.
 Text Box	Inserts a text box.
 Chart	Inserts a chart.
 Image	Inserts an image.
 Separator	Draws a horizontal line across the page.
 Table of Contents	Inserts a table of contents.
 Tab	Moves the insertion point to the next tab stop.
 Newline	Inserts a newline.
 Space	Inserts a non-breaking space.

Setting Report Page Options

As a part of your report template designs, you can set page options such as page size, orientation, margins, and so forth. The page settings you define at template design time will be built into the “deployed” template as defaults.

Setting the Page Size

- 1 Select the **File > Page Setup** from the menus.
- 2 Select a page size from the drop-down list, or enter the size and units of measurement for non-standard page sizes.
- 3 Click the **OK** button.

Setting the Page Orientation

- 1 Select the **File > Page Setup** from the menus.
- 2 Select either **Portrait** or **Landscape**.
- 3 Click the **OK** button.

Setting the Page Margins

- 1 Select the **File > Page Setup** from the menus.
- 2 Set the distance, in inches, from the edge of the page for the **Left**, **Top**, **Right**, and **Bottom** fields
- 3 Set the distance, in inches, from the edge of the page to the top of the page header and footer in the **Header** and **Footer** fields.
- 4 Click the **OK** button.

Setting the Page Background

Select the **File > Page Setup** from the menus, and click the **Background** tab.


Setting a Background Color

- 1 Select the **Color** option.
- 2 Select a color from the drop-down list.
- 3 Click the **OK** button.


Setting a Background Image

- 1 Select the **Image** option.
- 2 Enter the path to the image.
- 3 Select the loading method.
- 4 To embed the image in the template file, check the **Embed** option.
- 5 Select either **Tile** or **Center** positioning option.
- 6 Enter preferred size of image or leave unspecified for actual image size.
- 7 Click the **OK** button.

Editing the Page Header

- 1 Click the Header  toolbar button or select the **Header** item from the **Insert** menu.
- 2 Insert and edit report elements as you would normally.


Editing the Page Footer

- 1 Click the Header  toolbar button or select the **Header** item from the **Insert** menu.
- 2 Insert and edit report elements as you would normally.


Designing Report Flow Layout

With the Report Template Designer, you can design the flow layout for a report template that specifies layout of the report content on the page.

Drawing a Page Area

- 1 Change the report view to **Layout**.
- 2 Click the **Draw Area**  toolbar button.
- 3 Click and hold the left mouse button where you want the upper-left corner of the page area to be placed.
- 4 Continue holding the left mouse button and drag the cursor to the location you want for the lower-right-hand corner of the page area.
- 5 Release the mouse button.


Changing the Order of Page Areas

- 1 Set the report view to **Page Layout**.
- 2 Click the **Order Areas**  toolbar button.
- 3 Move the mouse over the area you want to receive the flow first. The cursor should turn into a hand.
- 4 Click the left mouse button. The number in the corner of the page area should now be "1".
- 5 Repeat steps 3 and 4 for each page area, in the order you want to flow.

Inserting an Area Break

- 1 Click the cursor on the location where you want the break.
- 2 Select the **Area Break** from the **Insert»Spacing Element** menu.


Creating a Non-flow Area

- 1 Set the report view to **Page Layout**.
- 2 Click the **Draw Area**  toolbar button.
- 3 Click and hold the left mouse button where you want the upper-left corner of the page area to be placed.
- 4 Continue holding the left mouse button and drag the cursor to the location you want for the lower-right corner of the page area.
- 5 Release the mouse button.
- 6 Right-click on the page area you just created.
- 7 Click **Properties** on the popup menu.
- 8 Disable (uncheck) the **Flow Area** property.
- 9 Click the **OK** button.

Creating a Fixed Position Element

- 1 Set the report view to **Page Layout**.
- 2 Click on a non-flow area.
- 3 Set the report view to **Normal**.
- 4 Insert the element into the non-flow area as you would a normal page area.

Creating an Element Associated Area

- 1 Set the report view to **Page Layout**.
- 2 Click the small arrow in the corner of the **Layout**  toolbar button.
- 3 Click the **Edit** item on the drop-down menu.
- 4 From the drop-down list on the dialog, select the report element you want to associate with the page layout.
- 5 Click the **New** button.
- 6 Click the **OK** button.

Creating Parallel Report Flows

- 1 Set the report view to **Page Layout**.
- 2 Create a non-flow area to one side of the report.
- 3 Create normal report areas in the remaining page area however you want.
- 4 Right-click the non-flow area.
- 5 Click the **Properties** item on the popup menu.
- 6 Deselect (uncheck) the **Repeat Contents** property.
- 7 Set the report view to **Normal**.
- 8 Place report elements in the non-flow area for one part of the parallel report flow.
- 9 Place report elements in the other page areas for the other part of the parallel report flow.

Designing Report Tabular Layout

Using the Report Template Designer, you can define the default layout for tables in a report template.

Inserting a Row

- 1 Set the report view to **Page Layout**.
- 2 Click the row you want to insert the new row before.
- 3 Right-click the row.
- 4 Click **Insert Row** on the popup menu.

Inserting a Column

- 1 Set the report view to **Page Layout**.
- 2 Click the column you want to insert the new column before.
- 3 Right-click the column.
- 4 Click **Insert Column** on the popup menu.

Deleting a Row

- 1 Set the report view to **Page Layout**.
- 2 Click the row you want to delete.
- 3 Right-click the row.

- 4 Click the **Delete Row** item from the popup menu.


Deleting a Column

- 1 Set the report view to **Page Layout**.
- 2 Click the column you want to delete.
- 3 Right-click the column.
- 4 Click the **Delete Column** item from the popup menu.

Splitting a Cell

- 1 Set the report view to **Page Layout**.
- 2 Click the cell you want to split.
- 3 Right-click the cell.
- 4 Select the **Split Cell** item on the popup menu.
- 5 To split the cell horizontally select **Rows**; to split the cell vertically select **Columns**.
- 6 Enter the number of cells to split the current cell into.
- 7 Click the **OK** button.

Resizing a Cell

- 1 Set the report view to **Page Layout**.
- 2 Move your mouse over the cell's edge until the cursor changes to the resize cursor. 
- 3 Press and hold the left mouse button.
- 4 Drag the mouse until the cell is the desired size.
- 5 Release the mouse button.


Building Report Elements into a Template

The following topics describe how to use the Report Template Designer to include different types of report elements into a template.

Inline Elements

Inline elements include options for inserting text, text formatting, working with tabs, and spaces.

Inserting Text

- 1 Click the report at the location you want to insert the text.
- 2 Click the Text  toolbar button or select the **Text** item from the **Insert>>Basic Element** menu.
- 3 Type the text to display.


Formatting text

- 1 Right-click the text or textbox element.
- 2 Select the format to apply from the **Format** submenu on the popup menu.

These formats are available in the Report Designer:

Format Type	Description
Date format	Specifies conversion for date/time values.
Decimal format	Specifies conversion for numeric values.
Currency format	Specifies formatting of numbers as currency (with a currency symbol).
Percent format	Specifies formatting of numbers as percentages.

Inserting a Tab

To insert a tab, press the **Tab** key or click the Tab  toolbar button.

Setting the Tab Stops

Select the **Format > Preferences** item from the menus, and click the **Tab Stops** tab.

Adding a Tab Stop


- 1 Enter the distance, in inches, from the left margin to position the tab stop in the text field.
- 2 Click the **Set** button.

Removing a Tab Stop

- 1 Select the tab stop from the list.
- 2 Click the **Clear** button.

To apply the changes, click the **OK** button.

Inserting a Space

To insert a space, press the **Space** key or click the Space  toolbar button.

Setting a Space's Width

- 1 Click the space element to format.
- 2 Right-click the element.
- 3 Select the **Properties** item from the popup menu.
- 4 Enter the width, in points, of the space in the **Number of Points** field.
- 5 Click the **OK** button.

Float Elements

Float elements include options for setting anchors, working with text wrap, setting margins, working with charts and text boxes, and inserting images.

Setting the Anchor

- 1 Move the mouse over the float element.
- 2 Click and hold the left mouse button.
- 3 Drag the element to the desired position.

- 4 Release the mouse button.

If a float element's anchor is not set, it is laid out as an inline element.

Setting the Text Wrapping

When one or more anchored elements exist on a line, other flow elements could wrap around the anchored elements. To set the wrapping:

- 1 Click the element to edit.
- 2 Right-click the element.
- 3 Select the **Properties** item from the popup menu.
- 4 Click the **Layout** tab.
- 5 Select the wrapping style to apply to this element.

The Report Designer offers these wrapping styles:



No wrapping; the flow overlaps the float element.



Wraps around the left side of the float element.



Wraps around the right side of the float element.



Wraps around both sides of the float element.




No contents allowed on either side of the float element.

Setting the Margins


- 1 Click the element to edit.
- 2 Right-click the element.
- 3 Select the **Properties** item from the popup menu.
- 4 Click the **Layout** tab.
- 5 Enter the size, in points, in the **Left**, **Top**, **Right**, and **Bottom** fields.
- 6 Click the **OK** button.

Inserting a Chart


- 1 Click on the report at the location you want to insert the report.
- 2 Click the Chart  toolbar button or select the **Chart** item from the **Insert >>Basic Element** menu.
- 3 Select the chart type from the drop-down list that appears.

Inserting a Text Box

- 1 Click the report at the location to insert the element.

- 2 Click the Text Box  toolbar button or select the **Text Box** item from the **Insert>>Basic Element** menu.
- 3 Type the text to display.
- 4 Right-click the text box and select the **Properties** item from the popup menu to apply formatting.

Inserting an Image


- 1 Click on the report at the location you want to insert the image.
- 2 Click the Image  toolbar button or select the **Image** item from the **Insert>>Basic Element** menu.
- 3 Enter the path to the image in the text field.
- 4 Check the **Embed** option if you want to embed the image data in the report template.
- 5 Select the loading option (see below) to use.
- 6 Click the **OK** button.

The loading options supported by the report designer are:

Loading Option	Description
Resource	Loads the image as a resource. The path to the image must be relative to the class path.
URL	Loads the image from the specified URL.
Relative path	The path to the image is relative to the location of the report template in the local file system.
Full path	The path to the image is the full path on the local file system.

Block Elements

Inserting a Table


- 1 Click the report at the location you want to insert the table
- 2 Click the Table  toolbar button
- 3 Select the number of rows and columns for the table

Or

- 1 Click the report at the location you want to insert the table
- 2 Select the **Table** item from the **Insert>>Basic Element** menu
- 3 Edit the number of rows and columns for the table by selecting the table element
- 4 Right-click and select **Properties**
- 5 Select **Headers and Data** tab and modify rows and columns fields and click **OK**

Inserting a Bullet


- 1 Click the report at the location you want to insert the bullet

- 2 Click the Bullet  toolbar button or select the **Bullet** item from the **Insert>>Basic Element** menu
- 3 Type the text to appear next to the bullet




The bullet and the text are separate elements.

Inserting a Separator Change a Separator's Line Style

- 1 Click the report at the location you want to insert the separator.
- 2 Click the Separator  toolbar button or select the **Separator** item from the **Insert>>Basic Element** menu.

Inserting a Newline

- 1 Click the report at the location to insert the newline.
- 2 Click the Newline toolbar  button or press the **Enter** key.

Changing a Newline's Height

- 1 Click the newline element to edit.
- 2 Right-click the element and select the **Properties** item from the popup menu.
- 3 Enter the number of lines in the **Number of Newlines** field.
- 4 Enter the height, in points, of each newline in the **Newline Size** field.
- 5 Click the **OK** button.

Inserting a Page Break

- 1 Click the report at the location to insert the page break
- 2 Select the **Page Break** item from the **Insert>>Spacing Element** menu

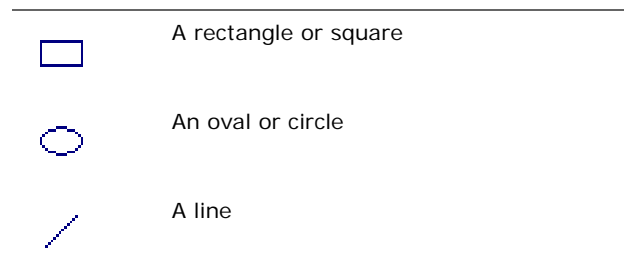
Inserting an Area Break

- 1 Click the location in a page area to insert the break
- 2 Select the **Area Break** item from the **Insert>>Spacing Elements** menu


Drawing a Freehand Shape

- 1 Change the report view to **Page Layout**
- 2 Click one of the shape buttons on the report element toolbar
- 3 Press and hold the left mouse button at the location of the upper-left corner of the shape
- 4 To constrain a rectangle to a square, or an oval to a circle, hold down the **Shift** key
- 5 Drag the mouse to the location of the lower-right corner of the shape
- 6 Release the mouse button


You can draw these freehand shapes:



Inserting a Numbered Heading






- 1 Click the report at the location to insert the heading
- 2 Click the Heading  toolbar button
- 3 Select the heading level from the drop-down list
- 4 Type the text for the heading

Inserting a Table of Contents

- 1 Click the report at the location to insert the table of contents
- 2 Click the Table of Contents  toolbar button or select the **Table of Contents** item from the **Insert>>Special Field** menu
- 3 Select the style for the table of contents from the drop-down list
- 4 Click the **OK** button

The table of contents will be generated automatically, based on the numbered headings in the report.

Changing an Element's Font

- 1 Click the element whose font you want to modify
- 2 Select the font's name  from the drop-down list on toolbar
- 3 Select the font size  from the drop-down list on the toolbar
- 4 To make the font bold, click the Bold  toolbar button
- 5 For an italic font, click the Italic  toolbar button
- 6 To underline the font, click the Underline  toolbar button

Building Queries

A query is an ArcSight resource that defines the parameters of the data you want to report on derived from an ArcSight data source. The result of the query then becomes the basis for one or more ArcSight report and/or trend. The Query Editor is a component of ArcSight Reporting resource tools. Be sure to see [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools.



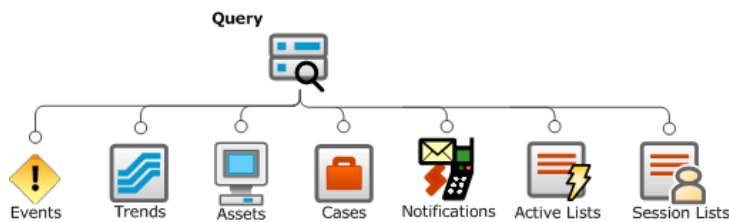
Queries built for reports can be used in query viewers also.

And if you want to run quick SQL queries for monitoring and analysis outside of the reporting resource, you can use query viewers, a new feature in ArcSight ESM 4.5. You can add query viewers to dashboards and generate simple reports on query viewer results.

For information on query viewers, see [Chapter 10, Query Viewers, on page 161](#).

How Queries Work

As a data source, queries can use the ArcSight database of events, modeled network objects (assets), cases, notifications, session lists, or active lists, or data gathered from a trend.



In a query, you select the data fields you want to report on, specify any additional functions you want run on them (such as sum, average, and so on), and any sort or group-by conditions you want to add, such as grouping results by source address, zone, or priority.

Using Queries and Trends Together for Reports

A query can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.

For a more detailed description of the relationships you can build between queries and trends for reporting, see the [“Query-Trend Relationships in Reporting” on page 242](#).

Using Queries in Query Viewers

You can use queries built for reports in *query viewers*, outside of the reporting paradigm. Query viewers provide a “channel-style” view of SQL query results but are not limited to events in terms of scope. They provide high-level summaries to monitor system health, reveal trends, and allow for drill-down and investigation of all types of resources across time. Query viewers are performance-tuned to work with trend tables rather than event tables, and so can return results much faster than active channels.

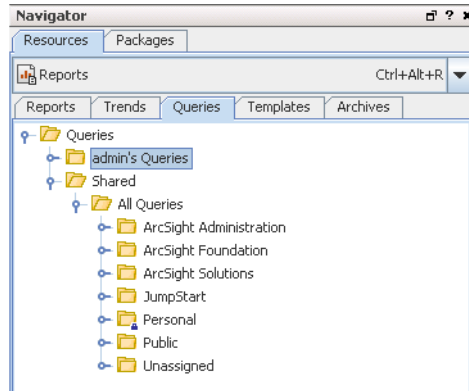
Query viewers include their own simple reporting option by which you can initiate a report on the query results from the query viewer.

For more on using query viewers, see [Chapter 10, Query Viewers, on page 161](#).

Building a Query

Navigating to Queries

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Queries** tab.



Creating a New Query

The high-level steps for creating a query are as follows:

- 1 Right-click a group (folder) and select **New Query**. This launches the Query Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 2 Define General Attributes. At a minimum, fill in the required values (red asterisks) on the General tab.
- 3 Define a schema for Query Fields.
- 4 Create Query Conditions.
- 5 Define Query Variables (optional).
- 6 Click **Apply** or **OK** to create the new query.



Be sure to click **Apply** or **OK** frequently to save settings intermittently as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings via these buttons, your settings will not be saved.

The following sections provide details on how to use the Query editor to define query attributes, fields, conditions, and variables.

Defining Query Settings

Use the Query Editor to build a new trend or edit an existing one. Query settings are defined on multiple sub-tabs.

General Attributes

The following fields in the **Query** section are required attributes that must be specified when creating a new query.

Query Fields	Description
Name	Name for the query. Spaces and special characters are OK. This is an alias for the query that will appear in pick lists in other editors.
Query on	<p>From the drop-down menu, select one of the following data sources:</p> <ul style="list-style-type: none"> • Event - Select Event if you want to report or calculate a trend on event activity. • Case - Select Case if you want to report or calculate a trend on the status of cases, such as number of cases opened and resolved. • Notification - Select Notification if you want to report or calculate a trend on the status of events sent out in the notification workflow, such as number of events in the Investigate stage. • Asset - Select Asset if you want to report or calculate a trend on statistics about the assets on your network, such as a list or count of assets categorized in a particular asset category, or the zone a particular asset is in at a particular time. • Trend - Select Trend if you want to report or calculate a trend on the data gathered in an existing trend. For instructions about how to build a trend, see "Building Trends" on page 241.
Start Time	<p>This field only appears if you selected Event or Trend in the Query On field. Enter values depending on the data source you selected:</p> <ul style="list-style-type: none"> • Event - Specify the starting point for the data gathering from the events database. Event data is generally kept unarchived for 30 days by default, so specify a start time within that time frame. • Trend - Specify the starting point for the data gathering from the trends database. Be sure to specify a timeframe within the lifecycle of the trend (otherwise, the query will return an empty result set). <p>Tip: If the query is used as a base query in a trend, the trend start time overwrites the start time set here. See "Trend Parameters" on page 249.</p>
End Time	<p>This field only appears if you selected Event or Trend in the Query On field. Enter an end time depending on the type of source data you selected:</p> <ul style="list-style-type: none"> • Event - Specify the ending point for the data gathering that is some time after the starting point. Keep in mind that large time spans can mean large amounts of data, which can affect system performance. • Trend - Specify the end point for the data gathering that is some time after the starting point. <p>Tip: If the query is used as a base query in a trend, the trend end time overwrites the end time set here. See "Trend Parameters" on page 249.</p>

Query Fields	Description
Use as Timestamp	<p>This field only appears if you selected Event or Trend in the Query On field. This field indicates which value to use as the timestamp for the report itself. This value helps with sorting and scheduling.</p> <ul style="list-style-type: none"> • End Time - Select End Time if you want to use the event or trend end-time you specified in the End Time field. The timestamp will reflect the event end time. (If you are querying on a trend, select this option.) • Manager Receipt Time - Select Manager Receipt Time to use the time the event was received at the Manager. (If you are querying on a trend, this is probably not an appropriate option to choose because in that case "Manager Receipt Time" would indicate when the trend is run, rather than when events are received by the manager.)
Row Limit	<p>Set the row limit for the data table. (The default is 1000 rows.)</p> <p>Tip: If the query is used as a base query in a trend, the trend row limit overwrites the row limit set here. See "Trend Parameters" on page 249.</p>

The example below shows a query called *VPN Logins Outcome - Hourly* that will return VPN login attempts over a one day period each time it is run (Start Time is \$Now - 1d and End Time is \$Now).

Name	Value
Query	
* Name	VPN Logins Outcome - Hourly
* Query On	Event
* Start Time	\$Now - 1d
* End Time	\$Now
* Use as Timestamp	End Time
Common	
Resource ID	[3DGNGA0BABCAM1IXCsqAw==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	
Parent Groups	
vicky's Queries	/All Queries/Personal/vicky's Queries
Creation Information	
Created By	vicky
Creation Time	16 Aug 2006 12:55:04 PDT
Time Since Creation	5 min(s) 58 sec(s)
Last Update Information	
Last Updated By	vicky
Last Update Time	16 Aug 2006 12:56:56 PDT
Time Since Last Update	4 min(s) 5 sec(s)



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 552](#).

Query Fields

The Query **Fields** tab contains three sub-tabs. Select the data you want to include in your query and any optional functions, order by, and group by settings you want to apply as described in detail below.

Query Fields: Select

The **Select** tab is where you select the data for the query. Data selected enters one big bucket, and any functions set for any of the data fields is performed on the entire bucket of data.

Query Structure: Shows a summary of selected data and any optional functions and/or order-by and group-by conditions.

Query Columns: Shows data selected for the query.

Column Function: As an option, select a query column, then select a function to perform on it. Click Unique to perform the function on unique values only.

Choose Columns: Select one or more data fields, then click the arrow to move it to the Query Columns area.

Select a Field Set: Narrow the list of data fields to one designed for a particular use case.

The screenshot shows the 'Inspect/Edit' dialog box with the 'Query Fields' tab selected. The 'Select' sub-tab is active. The 'Query Structure' panel shows a SELECT statement: `Count(Category Outcome) COUNT`, `Category Outcome`, and `Hour`. The 'GROUP BY' section shows `Category Outcome` and `Hour`. The 'Data Options' panel shows the 'Select' sub-tab. The 'Choose columns...' list includes fields like *Event*, *Additional Data*, *Aggregated Event Count*, *Application Protocol*, *Base Event Ids*, *Bytes In*, *Bytes Out*, *Concentrator Agents*, *Concentrator Devices*, *Correlated Event Count*, *Crypto Signature*, *Customer*, *Customer External ID*, *Customer ID*, *Customer Name*, *Customer Resource*, *Customer URI*, *End Time*, *Event ID*, *External ID*, *Generator*, *Generator External ID*, *Generator ID*, *Generator Name*, *Generator Resource*, and *Generator URI*. The 'Query Columns' panel shows `Category Outcome COUNT`, `Category Outcome`, and `Hour`. The 'Column Function' panel shows 'Function: None' and a 'Unique' checkbox.

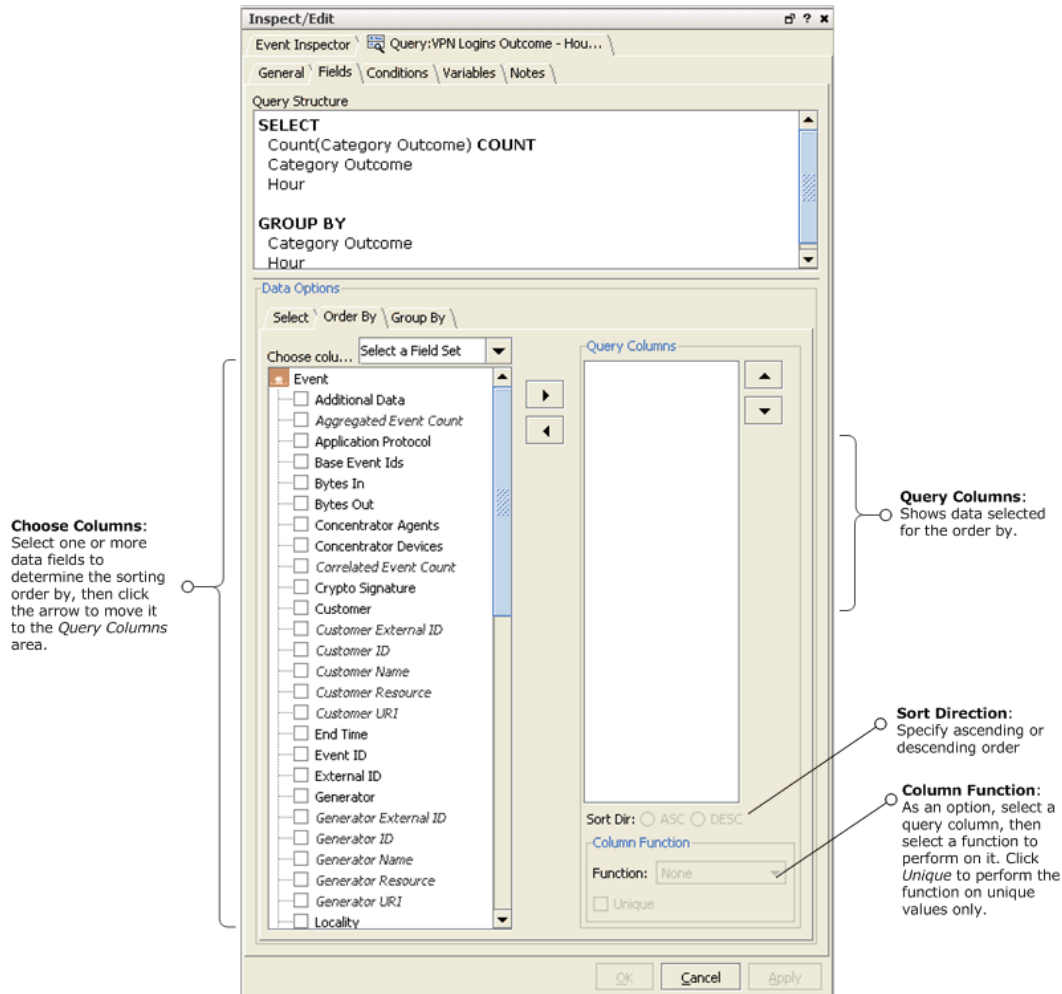


Fields shown in *italics* on the Data Options panel are derived, referenced, or side table fields (rather than “hard event data” in the main database tables). See also, [“Data Fields” on page 633](#) and [“Variables” on page 784](#).

Query Fields: Order By

Options	Description
Query Structure	<p>The Query Structure section at the top provides a summary of the fields selected in the Data Options section at the bottom.</p> <p>The Query Structure example in above shows the Count() function applied to the "Target User Name" field.</p>
Choose Columns	<p>Select (checkmark) one or more data fields you want to use in your query. Click the right arrow to move selected fields into the Query Columns section.</p> <p>As selections are made, they populate the Query Columns section and appear in the Query Structure summary at the top.</p>
Select a Field Set	<p>Field sets are named subsets chosen from the available data fields. By default, all fields are listed as options to use for populating "columns" in the result data.</p> <p>If you want to narrow the list of fields you have to choose from here, you can choose a standard field set to start with. This is just a "view" option you can use as needed to reduce the long list of data fields showing.</p>
Query Columns	<p>Selected fields are shown on this panel to the right of the list of available fields.</p> <ul style="list-style-type: none"> To add field(s) to the schema for this query, select them under "Choose Columns" and click the right arrow. To remove field(s) from the schema, select them under "Query Columns" and click the left arrow.
Column Function	<p>Optionally, you can specify an aggregate function on a particular column of data, such as a line item count, or in the case of numeric data, a sum or average</p> <p>If the query is not grouped by one or more columns in the Group By tab, then aggregate functions added here are applied to the whole result set</p> <p>If the query is grouped by one or more columns in the Group By tab, then the aggregate function is performed on each group individually</p> <p>Adding a function adds a data field to the query schema that provides the results of the function, which can later be displayed in the report.</p> <p>To specify a function for column data, select a data field in the Query Columns section then select a Function (from the drop-down menu) to apply to the column data:</p> <ul style="list-style-type: none"> Count - Count the number of line items returned in this column. Max - Calculate the top values of the items returned in this column. Min - Calculate the lowest values of the items returned in this column. Average - Calculate the average of all numerical data in a column, such as aggregated event count. Sum - Add all numerical data in a column, such as aggregated event count. <p>Click the Unique checkbox to apply the function only to unique values in the column. (For example, the target address column may have 50 items in it, but only three are unique. To get a count of unique target addresses, check the Unique box.)</p>

The **Order By** tab is where you specify the order in which you want the data in your buckets sorted. For example, you might "order by" if you were interested in the numeric value of the items in your bucket such as the top 10 logins.



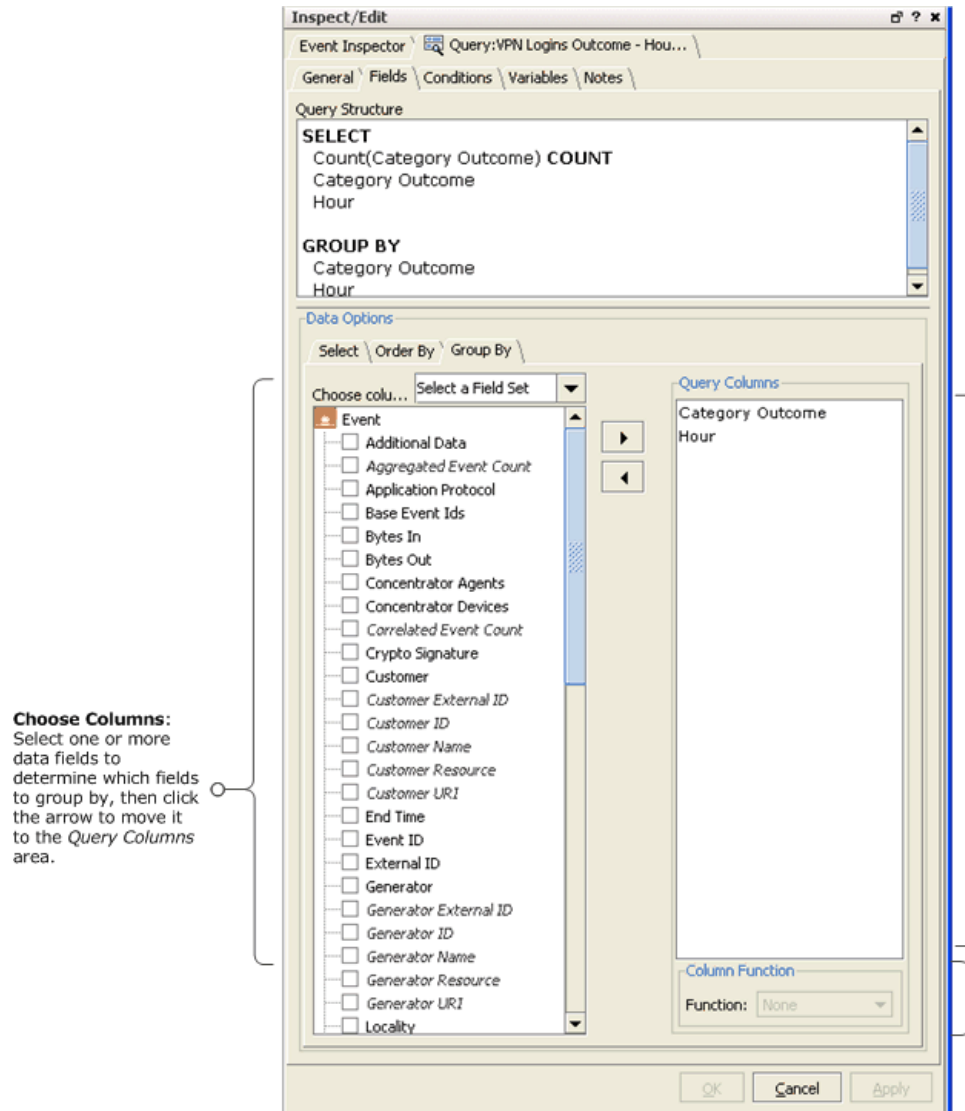
Fields in shown in italics on the Data Options panel are derived, referenced, or side table fields (rather than "hard event data" in the main database tables). See also, ["Data Fields" on page 633](#) and ["Variables" on page 784](#).

Options	Description
Query Structure	<p>The Query Structure section at the top provides a summary of the fields selected in the Data Options section at the bottom. If you add "Order By" settings, these show up here also.</p> <p>The example above shows "Event ID" selected, so the query results will be ordered by event ID. (Even if Event ID is not one of the fields chosen on the Select tab and therefore not visible as a column in the query result, events will still be ordered by event ID in the result.)</p>

Options	Description
Choose Columns	<p>Select (checkmark) one or more data fields you want to order by. Click the right arrow to move selected fields into the Query Columns section.</p> <p>As selections are made, they populate the Query Columns section and appear in the Query Structure summary at the top.</p> <p>The Order By columns can be different than the ones you chose for the query data on the Select tab.</p>
Select a Field Set	You can narrow the list of data fields shown here to a pre-defined field set from the Select a Field Set drop-down menu.
Query Columns	<p>Selected Order By fields are shown on this panel to the right of the list of available fields.</p> <ul style="list-style-type: none"> To add field(s) to the schema for this query, select them under "Choose Columns" and click the right arrow. To remove field(s) from the schema, select them under "Query Columns" and click the left arrow.
Sort Direction	By default, the sort order is ascending. To change the sort order, select the item in the Query Columns area to activate the Sort Direction radio buttons.
Column Function	Optionally, you can specify a function on the Order By data, such as a line item count, or in the case of numeric data, a sum or average. This works similarly to the column function feature on the first tab (Fields). For more information, see the detail about Column Function above.

Query Fields: Group By

The **Group By** tab is where you divide the query results into separate buckets. For example, you could do a "group by" if you are interested in sorting items by timestamp, such as log-ins between 3 and 5 p.m. Functions applied to data on the **Group By** tab only apply to timestamp-based fields.



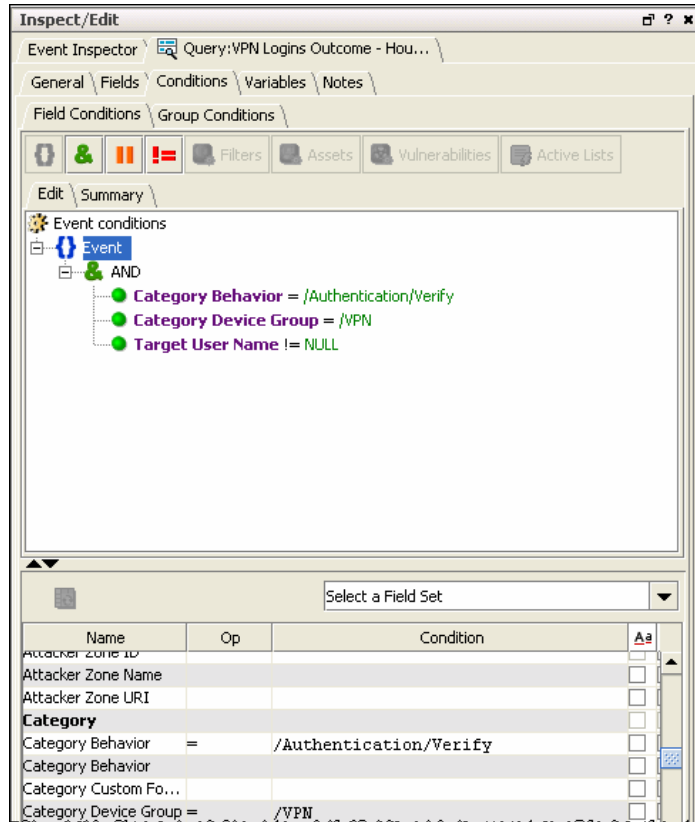
Fields shown in italics on the Data Options panel are derived, referenced, or side table fields (rather than "hard event data" in the main database tables). See also, ["Data Fields" on page 633](#) and ["Variables" on page 784](#).

Options	Description
Query Structure	<p>The Query Structure section at the top provides a summary of the fields selected in the Data Options section at the bottom. If you add "Group By" settings, these show up here also.</p> <p>The example above shows event "End Time" selected with the function Day() applied, so the query results will be grouped by end times within the same day.</p>
Choose Columns	<p>As an option, you can specify a time-based function on the group by column of data. Because these are time-based functions, they apply only to time-based fields, such as event end time.</p> <p>Functions on items in the Group By tab create a separate bucket of data for each time function specified. Adding a function adds a data field to the query schema that provides the results of the function, which can later be displayed in the report.</p> <p>Select (checkmark) one or more data fields you want to group by. Click the right arrow to move selected fields into the Query Columns section.</p> <p>As selections are made, they populate the Query Columns section and appear in the Query Structure summary at the top.</p>
Select a Field Set	<p>You can narrow the list of data fields shown here to a pre-defined field set from the Select a Field Set drop-down menu.</p>
Column Function	<p>Optionally, you can specify a function on the Order By data, such as a line item count, or in the case of numeric data, a sum or average. This works similarly to the column function feature on the first tab (Fields). For more information, see the detail about Column Function above.</p> <p>To specify a function for column data, select a data field in the Query Columns section then select a Function (from the drop-down menu) to apply to the column data:</p> <ul style="list-style-type: none"> • Second - This creates a new bucket for all events that occur in the same second. • Minute - This creates a new bucket for all events that occur in the same 60-second period. • Hour - This creates a new bucket for all events that occur in the same 60-minute period. • Day - This creates a new bucket for all events that occur in the same 24-hour period. • DayofWeek - This creates a new bucket for all events that occur on the different days of the week, such as Monday, Tuesday, and Wednesday. • DayofMonth - This creates a new bucket for all events that occur on various days of the month, such as the first, second, and third.

Query Conditions

Optionally, you can create conditions on individual fields or on groups as part of the query. You can add filters, and conditions based on assets, vulnerabilities, and active lists.

Use the [Common Conditions Editor](#) (CCE) within the query editor to create query conditions as described below.



The Common Conditions Editor is used throughout the Console for various resources. In addition to the topics that follow on defining conditions for a report query, see also [“Common Conditions Editor” on page 616](#), [“Conditional Statements” on page 625](#), and [“Conditions” on page 626](#).

Creating Conditions on a Field

- 1 Click the **Conditions** tab and select data fields from the fields below list to build a condition statement in the display area at the top of the Edit sub-tab.

The data field table displays a **Name**, **Operator**, and **Condition** column. These three columns are combined to create <data field> <logic operator> <data field value> condition statements. For example, if monitoring a Cisco Router, you could define a condition statement to specify `Device Product = Cisco Router: Device Product` as the data field, `equals (=)` as the logic operator, and `Cisco Router` as the data field value.

- 2 In the Op column, double-click the cell and select a logic operator from the drop-down menu.
- 3 In the Condition column, type a data field value or double-click the cell and select a value from the drop-down menu. Press **Enter** to add the condition to the statement above.

- 4 Repeat this process to add more statements to the condition.
- 5 Click **Apply** or **OK** to save your changes and create the condition.

Here is some guidance on creating conditions.

- Drop-down menus appear if the selected data field has a set of value options.
- For example, if the Category Behavior data field is selected, a drop-down menu appears with the value options of `/Access`, `/Access/Start`, `Access/Stop/` and so on. One of the choices in this menu is `/Authentication/Verify`, which is the condition we selected for Category Behavior in our example condition.
- For date and time data fields, such as Detect Time, you can type an actual date value, such as `10/12/2002 8:54:00 AM`, or you can use special Time variables.
- The condition statement appears as a branch under the logical operator.
- To add a condition to an event field, click in its condition box and click the ellipses icon.
- To activate all operands on the top, select an item in the editor view, as shown above.

Creating Group Conditions

Creating a group condition is similar to creating a normal condition, except you pick an aggregate function to perform on the group.

You would use it if, for example, to group by event name and when you want to get only the events with more than 100 occurrences in the query. In this case, you would add a `Count()` aggregate function to the eventID field, for example, `count(eventId) > 100` to eliminate the events that have occurred less than 100 times.

Query Variables

Variables are run-time information derived from the source data (event, asset, case, notification, or trend, depending on the schema) that can be used in the query wherever normal fields can be used.

To set a variable:

- 1 Click the **Variables** tab.
- 2 Click **Add** to launch the Variables dialog.
- 3 The Variables dialog displays different values depending on the function you choose. In the Variables dialog, enter the following values and click **OK**.

Options	Description
Name	Enter a name for the variable. This is the alias that will appear in the Conditions editor when you can use the variable. Spaces and special characters are OK.
Function	From the drop-down menu, select a function. For a description of each function, click Help in the lower right corner.
Arguments	The arguments section contains a series of fields where you set the parameters for the variable. The available fields vary with the function you select.
Preview	The preview area provides an interface where you can enter values for the key variable fields so you can verify that the parameters you specified return the expected results. Enter test values and click Calculate .

Editing a Query

- 1 Navigate to **Reports** in the Navigator panel, select the **Queries** tab, and select the query you want to modify.
- 2 Double-click the query, or right-click and select **Edit Query** from the context menu. This launches the Query Editor in the Inspect/Edit panel, and shows the definition for the selected query.
- 3 Edit the query definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)



If the query is used in a trend, the query and associated schema referenced in the trend are set at the time the trend was created. After the trend is created, you can add columns to the base query, but columns added to the query after the trend is created will not be used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to add or remove columns (data fields) in the query that are used in the trend, you will need to create a new trend and select that modified query.

Building Trends

A trend is an ArcSight resource that defines how and over what time period data will be aggregated and evaluated for trends. A trend executes a specified query on a defined schedule and time duration.

The ArcSight trends engine evaluates source data for trends based on event conditions (such as number of worm outbreaks, incident time-to-close, or number of cases closed) or common network elements (such as operating system, business role, or regulatory compliance relevance).

Trends can be used as the primary data source for a report, or used as the data source input to another query which is then used in a report (perhaps along with other queries or trends).

Building trends is a component of ArcSight Reporting resource tools. Be sure to start with [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools, and ["Understanding Reporting Workflow" on page 205](#) to see how Trends fit in to the process of creating a report.

How Trends Work

A trend references a query, specifies a schedule on which the query automatically triggers, and provides mechanisms for efficiently storing, viewing, and leveraging the trend results for reporting. The trend results are stored in a trend table in the ArcSight database, and are themselves queryable.

Trends can be set to run indefinitely or to end at a specified date and time. A trend can be configured to start retrieving historical data from logs, start with current events, or at some specified time in the future. (You can also specify advanced options on how and when to build tables, store data, and partition it.)

Once trend data is collected, you can view the results in the Data Viewer table and generate a trend report that displays the results in tables and graphs.



Depending on the data gathered by the base query, the trend will either be a *snapshot trend* or an *interval trend*.

Snapshot Trend

A *snapshot trend* uses a query that operates on a fixed moment in time, for example, to gather information about assets on your network. Snapshot trends are built from queries based on assets, cases, or notifications. For example, snapshot queries and the trends built from them would be used to determine metrics such as current number of assets, number of systems with a particular operating system, or number of systems with particular vulnerabilities. A snapshot trend operates on data in the current moment in time, and only collects data going forward. Thus, trends cannot be used to answer the question, "how many assets were there in this zone a month ago?" You can use trends to collect data from this point forward, however, and in a month from now, you will have a month's worth of data that will tell you how many assets were in this zone at regular intervals over the last month.

Interval Trend

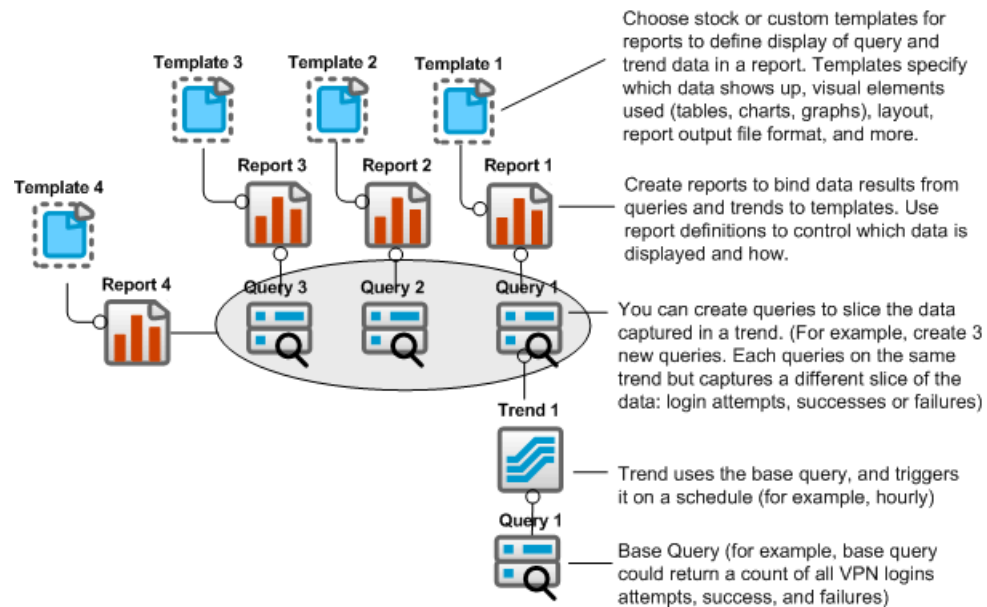
An *interval trend* uses a query that operates on events that happen over a specified time window, for example, to gather information about how many events of a particular description occurred daily over a 6-month period. Interval trends are event-based. For example, an interval trend using a base query with a time window could gather information to determine the number of login attempts in the past hour. You can "refresh" an interval trend manually as needed (by selecting the trend in the Navigator and clicking **Refresh** on right-click context menu). Interval trends are typically event-based.

Query-Trend Relationships in Reporting



Note that for a query used in a trend, the query and associated schema referenced in the trend are set at the time the trend was created. After the trend is created, you can modify some elements of the query if they do not affect the trend. For example, you can add or remove columns in the query if the related trend does not depend on them. Such modifications made to a referenced query will not be reflected in the trend. If you modify aspects of the query that a trend depends on, the trend will be disabled.

A base trend is made up of one query. Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.



For example, you could create a trend called "VPN Logins Outcome - Hourly" that references a query that returns all VPN login attempts, successful logins, and failed attempts. (You could schedule the trend to run hourly.) You can use this base trend directly in a report.

However, a more powerful approach would be to further refine the data results by creating three new trend queries, each of which takes the base trend as its data source but then sets further conditions on the query data to return one specialized slice of the results. One query could return only login attempts, another only successful attempts, and another only failed attempts. You could then draw on four queries in a single or multiple reports to show different views of the data. (The base query would show all types of login events, and the other three would show the focused views.)

Multiple reports can be generated from a single query or trend, and a single report can capture data from multiple queries and trends.

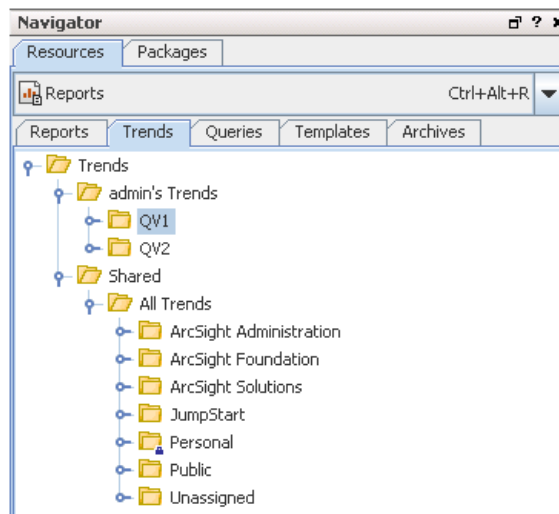
The ability to automate and refine queries by feeding them into trends and vice versa, along with the flexibility in populating reports solves many typical enterprise security reporting challenges. You can build a trend that gets a daily event count, feed the trend into a query that sums up the daily counts to get a monthly event count, and even feed that monthly count query into another trend and so forth. Managed Security Service Providers (MSSP) can use slicing and dicing query-trend approaches to create focused reports for multiple customers built from what are initially broad range queries.

Building a Trend

Before you begin building a trend, make sure that you have a query defined that captures the data you want to build a trend on. (See ["Building Queries" on page 228](#) if you need more information.)

Navigating to Trends

In the Navigator panel, select the **Reports** resource from the drop-down menu and click the **Trends** tab.



Creating a New Trend

The high-level steps for creating a trend are as follows:

- 1 Right-click a trend group (folder) and select **New Trend**. This launches the Trend Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 2 Define Trend attributes. At a minimum, fill in the required values (red asterisks) on the Attributes tab as described in the Trend Attributes topic below.
- 3 Verify the trend schema represented by the selected Data Fields is appropriate.
- 4 Test the trend schema to make sure it is returning the expected data as described in Testing a Trend.
- 5 Define a Trend schedule as described in Trend Schedule.
- 6 Click **Apply** or **OK** to create the new trend.



Do not click **Apply** or **OK** until you have defined the required values in the Trend section (trend name and query to use) and the trend schema in the Data Fields section of Trend Attributes. When you commit changes to the trend, the query and the schema are set and cannot be edited. If you decide to use a different base query or need to make a change to the schema, delete the trend and start fresh



A trend uses a "snapshot" version of the query as its data source. After you have used a query in a trend, you can modify some elements of the query if they do not affect the trend. For example, you can add or remove columns in the query if the related trend does not depend on them. Such modifications made to a referenced query will not be reflected in the trend. If you modify aspects of the query that a trend depends on, the trend will be disabled.

Defining Trend Settings

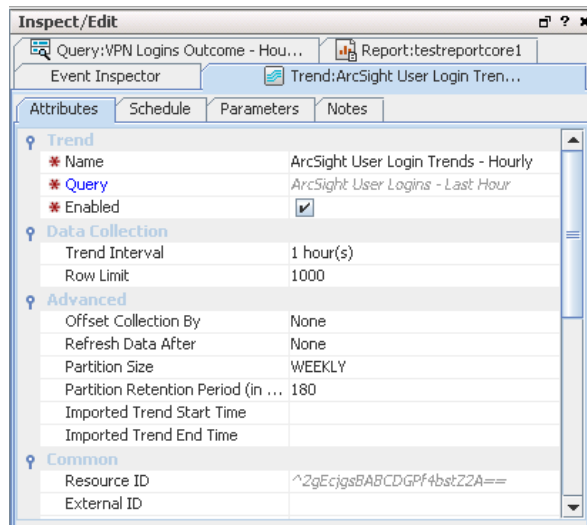
Use the Trend Editor to build a new trend or edit an existing one.

Trend Attributes

The following fields in the Trend section are required attributes to specify when creating a new trend.

Trend Fields	Description
Name	Name for the trend. Spaces and special characters are OK. The name you enter here is the alias that will appear in data source pick lists in other editors.
Query	Specifies the query that this trend uses If you are creating a new trend, use the Query drop-down menu to select a query as the source data for your trend. Caution: Once the trend is created, you can add columns to the base query, but columns added to the query after the trend is created will not be used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to remove columns (data fields) in the query that are used in the trend, you will need to create a new trend and select that modified query.
Enabled	By default, the Enabled checkbox is checked. This activates the trend to begin working on live data as soon as the trend is created. Uncheck this box if you want to experiment with the trend before pushing it live.

The example below shows a trend that uses the "VPN Login Outcome - Hourly" query as its basis.



The **Data Collection** section provides default values for row limit and query duration. You can keep the defaults or modify as needed.

Data Collection Fields	Description
Trend Interval	Time span over which the trend will operate. The default is one hour. For example, if the query counts the number of logins, this setting will count the number of logins every hour.
Row Limit	Maximum number of rows of data the trend will capture. The default number is 1000.

The **Advanced** section provides optional settings to offset trend data collection and refresh trend data at a specified point in the future. By default, the offset and refresh values are set to "None". The Advanced section also specifies default values for data storage partitions. You can keep the defaults or modify as needed.

Advanced Fields	Description
Offset Collection By	<p>Delays trend data collection by the time period specified. Offsetting trend data collection time enables you to compensate for events that arrive to the Manager late, either from a time zone lag or other data collection lag. Trend data collection will start after the time delay entered here.</p> <p>Enter a time delay and select Hours or Minutes from the drop-down menu. The default offset is None.</p>
Refresh Data After	<p>Triggers the system to automatically re-evaluate the query data at a later time to capture any additional events that may have come in late.</p> <p>Enter a refresh interval and select Hours or Minutes from the drop-down menu. The default refresh is None.</p> <p>Note: The Manager supports late arrival of events. For example, a SmartConnector can send a batch of events later if it is falling behind. You need to explicitly schedule a refresh of trend data only if SmartConnectors frequently lag behind in sending events to the Manager. If SmartConnectors rarely go down and are generally on time delivering events, there is no need to set this option.</p>
Partition Size	<p>Specifies the time range of the database partitions for this trend data, which in effect determines the partition size.</p> <p>The default "time slice" for trend tables is WEEKLY. That is, if the default setting is used, each partition would contain a week's worth of data. Partition size can be set to daily, weekly, or monthly. (You can always modify the Partition size as needed by editing the trend definition.</p> <p>Database partitioning is for space and archive management purposes (keeping trend data organized for long term storage. It can also help to improve query performance.</p> <p>The Partition Size works in concert with the Partition Retention Period, described below.</p>

Advanced Fields	Description
Partition Retention Period (in days)	<p>Specifies the number of days to retain the partitions from this trend as active in the ArcSight database. The default is 180 days. (You can always modify the Partition Retention Period as needed by editing the trend definition.)</p> <p>Note: The Partition Retention Period works in combination with the Partition Size. The system makes sure you always have as much data, if not more, than you specified in the configuration of these two settings. Similarly for factors such as time zones and daylight savings time, more data (never less) is retained. For example, if the Partition Size is set to MONTHLY and the Partition Retention Period is 45 days, the system will store two month's worth of data. If the Partition Retention Period is set to 0 days, the data collected from one run of the trend will be retained until the next partition is started. For example, if the Partition Size is MONTHLY and the Partition Retention Period is 0 days, then you will keep one month's worth of data. Make sure that the trend start date is appropriate; a trend with a MONTHLY partition size, 0 days retention, and a start date near the end of the month would not maintain data for very long.</p>
Imported Trend Start Time	<p>If the trend is exported without schedule start and end times, the trend start time specified here will be used when the trend is imported.</p> <p>If the trend is exported without Schedule start and end times and no value is specified for Imported Trend Start Time, then when the trend is imported it will default to use \$CurrentDate as the start time. (With this setting, the trend will capture data starting from 12:00:00 AM of the current day.)</p> <p>Note: The imported trend start time takes effect only if the trend is exported without Schedule start time. To exclude the Schedule start time from a trend upon export, you must set the package "Format" option to "export". For information on this, see the description of the package "Format" options in "Creating Packages" on page 492.</p>
Imported Trend End Time	<p>If the trend is exported without schedule start and end times, the trend end time specified here will be used when the trend is imported.</p> <p>If the trend is exported without Schedule end time and no value is specified for Imported Trend End Time, then when the trend is imported it will default to using no end time. (With this setting, the trend will run indefinitely until it is manually disabled or edited to include an end time.)</p> <p>Note: The imported trend end time takes effect only if the trend is exported without Schedule end time. To exclude the Schedule end time from a trend upon export, you must set the package "Format" option to "export". For information on this, see the description of the package "Format" options in "Creating Packages" on page 492.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 552](#).

The **Data Fields** section is where you build the trend schema. This is populated automatically when you first select the query to use in this trend. The list shows the data fields collected by the query you chose. By default, all the query fields are selected for use

in the trend. If you do not want to use a particular data field, uncheck the Use box for that item. Also, you can select which fields you also want to index. Indexing is done mostly for query efficiency. It is helpful if the query you are using returns a large amount of data, and you want to run sub-queries on the data.

Data Fields

Name	Use	Index
Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of Logins	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Category Outcome	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hour	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The **Summary** box at the bottom displays a summary of the query interval and the schedule on which it runs.

Trend Schedule

Click the **Trend Schedule** tab to review or modify settings for the following parameters:

- **Schedule Frequency** - Specifies how often the query will run and gather data. The default is to run once every hour on the hour.
- **Schedule Range** - Specifies the timeframe (start and end date/time) during which the trend will collect data at the scheduled collection times. By default, the date and time the trend was created is used as the trend schedule start time. The default is indefinitely; that is, No End date.

With the default settings, this trend would collect data once every hour on the hour until it is disabled manually.

A Summary of the configured schedule is shown at the bottom of the tab.

Inspect/Edit

Event Inspector \ Trend:VPN Logins Outcome - Hou...

Attributes \ Schedule \ Parameters \ Notes

Query Data Source: VPN Logins Outcome - Hourly

Query Duration: 1 hours

Next Run: 1 Aug 2006 13:00:26 PDT

Schedule Frequency

☒ Hourly Every 1 hour(s) at 0 minutes after

☐ Daily

Schedule Range

Start: 7/26/06 10:48:26 AM

End: ☒ No End date

☐ End on 8/1/06 12:46:10 PM

Summary

Occurs **Hourly**.
Schedule will start on **Wed Jul 26 10:48:26 PDT 2006**.

Refresh Trend Runs Test OK Cancel Apply

Trend Parameters

The Parameters tab lets you further refine the query results in terms of row limits, time zone restraints, filters, and start and end times. If you set parameters in the base query used by this trend, those parameters show up on the Trend Parameters tab. In the Trend, you can specify default parameters.

Then at Report building time, you can opt to run the report with the default parameters or "all parameters". You can also further refine parameter details for a specific run of a report. For more information on specifying parameters in reports, see ["Report Parameters" on page 267 in Creating Reports](#).



Trend start/end times and row limits are used for gathering the data, and overwrite the start/end times and row limits set in the base query. If you do not customize the Trend Parameters, the defaults on this tab are used (not the start/end times and row limit on the Query General Attributes tab).

For reporting on the data (once it is collected), you can set new start/end times and row limit in the **Report Parameters** tab. The report parameters prescribe only the "outbound" or publishing data derived from the data already collected, not the how the data is gathered. (See ["Report Parameters" on page 267 in Creating Reports](#) and ["Running Reports" on page 287](#) for more information.)

Testing a Trend

When you are creating a new trend or modifying an existing one, you might want to test it first to determine if you have defined the trend properly to return the data you want. To test the results of the schema you selected, make sure you are on the Schedule tab for the trend you want to test and click **Test**. Here are navigation instructions in case you are not already on that tab:

- 1 Navigate to Reports Trends in the Navigator panel, and select the trend you want to test.
- 2 Do one of the following:
 - ◆ Right-click and choose **Test** from the context menu

Or

 - ◆ Click Edit Trend to bring up the Trend editor in the Inspect/Edit panel. Within the editor for the selected trend, click the Test button at the bottom of any of the editor tabs (Attributes, Schedule, Parameters, and so forth).

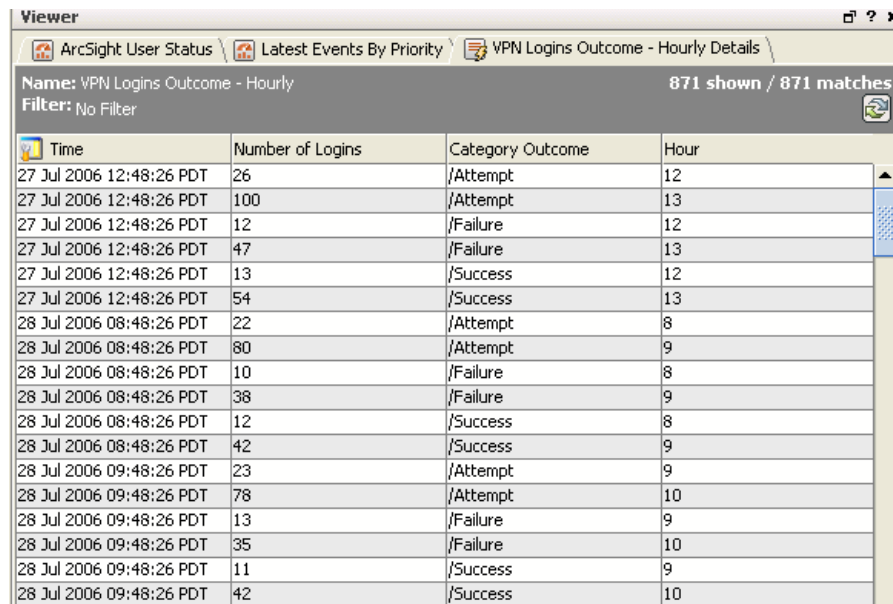
This will evaluate the current event stream for matching events and populate the Test Trend pop-up dialog. The message "Success: x rows" at the bottom of the dialog will tell you how many rows your trend returned.

The Test Trend sample will show a maximum of 25 rows. For interval queries, the sample also shows data from, at most, the last hour. If there is no match for the data, the trend will return 0 rows. This may mean that your current event query data contains no matching events or resources, or it may mean that your query needs to be refined.

Viewing Trend Data

- 1 Navigate to Reports Trends in the Navigator panel, and select the trend for which you want to view the data.
- 2 Right-click and select **Data Viewer** from the context menu. This launches the Trend Data Viewer in the Viewer panel and shows the query results. As with other ArcSight

event viewers, you can select an event or group of events, right-mouse click, and access various tools from the context menu to use for further investigation.



Time	Number of Logins	Category Outcome	Hour
27 Jul 2006 12:48:26 PDT	26	/Attempt	12
27 Jul 2006 12:48:26 PDT	100	/Attempt	13
27 Jul 2006 12:48:26 PDT	12	/Failure	12
27 Jul 2006 12:48:26 PDT	47	/Failure	13
27 Jul 2006 12:48:26 PDT	13	/Success	12
27 Jul 2006 12:48:26 PDT	54	/Success	13
28 Jul 2006 08:48:26 PDT	22	/Attempt	8
28 Jul 2006 08:48:26 PDT	80	/Attempt	9
28 Jul 2006 08:48:26 PDT	10	/Failure	8
28 Jul 2006 08:48:26 PDT	38	/Failure	9
28 Jul 2006 08:48:26 PDT	12	/Success	8
28 Jul 2006 08:48:26 PDT	42	/Success	9
28 Jul 2006 09:48:26 PDT	23	/Attempt	9
28 Jul 2006 09:48:26 PDT	78	/Attempt	10
28 Jul 2006 09:48:26 PDT	13	/Failure	9
28 Jul 2006 09:48:26 PDT	35	/Failure	10
28 Jul 2006 09:48:26 PDT	11	/Success	9
28 Jul 2006 09:48:26 PDT	42	/Success	10

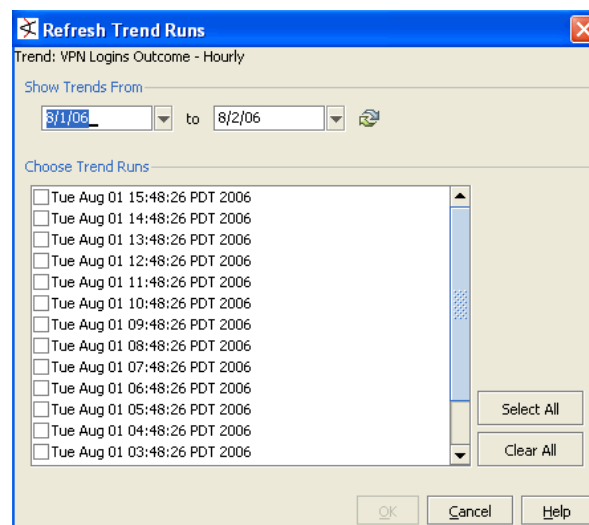
Refreshing Trend Data

In addition to relying on the scheduled execution of a query per its interval trend schedule, you can manually refresh the trend data at any time by using the trend refresh feature.

To manually refresh a trend table:

- 1 Do either of the following:
 - ◆ Click the **Refresh Trend Runs** button on the Trends Attributes tab for the selected trend
 - ◆ In the Navigator, select a Trend you want to refresh, right-mouse click and select **Refresh trend runs...** from the context menu.

This brings up the **Refresh Trends** dialog which displays execution times of the selected trend.



- 2 Select a timeframe under **Show Trends From**, select one or more of the Trend Runs under **Choose Trend Runs**, and click **OK** to refresh the selected trend run(s).

This executes the base query and refreshes the trend table on the selected run(s). Trend refresh allows you to manually re-run a trend to compensate for events that arrive to the Manager late, either from a time zone lag or other data collection lag.



Also, you can configure data collection to be offset by some time period to compensate for late arrival of events. For more information, see [Advanced settings for trends](#) in this Help topic.

Editing or Viewing a Trend Definition

- 1 Navigate to **Reports** in the Navigator panel, select the **Trends** tab, and select the trend you want to modify.
- 2 Double-click the trend, or right-click and select **Edit Trend** from the context menu. This launches the Trend Editor in the Inspect/Edit panel, and shows the definition for the selected trend.
- 3 Edit the schedule, advanced settings, and so forth as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Trend editor without saving changes.)



The query used for a trend and the schema are set at the time the trend was created, and cannot be edited later. If you decide to use a different base query or need to make a change to the schema, delete the trend and start fresh. You can edit the base query by adding columns to it, but columns added to the query after the trend is created will not be used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to add or remove columns (data fields) in the query that are used in the trend, you will need to create a new trend and select that modified query.

Using a Trend in a Query or Report

Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result.

For more information on next steps, see [Building Queries](#) and [“Creating Reports” on page 251](#).

Creating Reports

Reports are captured views or summaries of data that can be viewed in the ArcSight Console or exported for sharing in a variety of file formats. You can create reports by pulling together the result sets from one or more queries or trends.

For information on how to run an existing report, see [“Running Reports” on page 287](#).

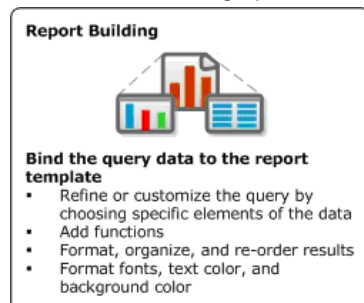
Creating Reports is a component of ArcSight Reporting resource tools. See also [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools, including how to build queries or trends and how to use a provided or custom template.

How Reports Work

When you have source data defined in queries and/or trends, you can design reports to present the data in charts and tables. You can use one of the templates provided with

ArcSight or design your own template using the Template Designer. This topic explains how to create a report that binds result data from queries and trends to a template, once you have one. (For information on accessing stock report templates or designing custom templates, see [“Using Report Templates” on page 209.](#))

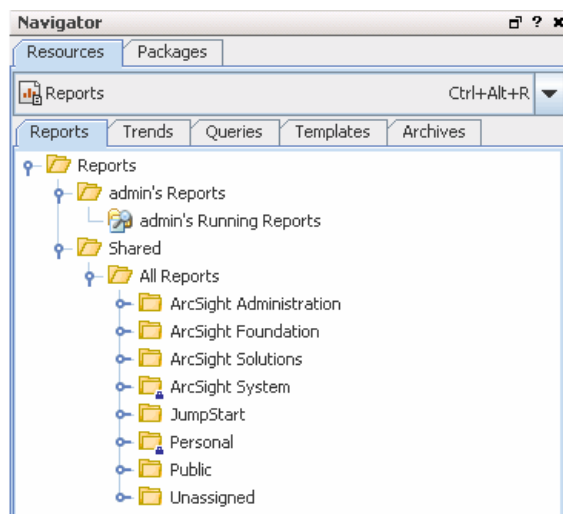
The reports resource defines how query data is bound to a report template. Depending on the report template you use, the reports editor exposes different parameters, variables, and conditions that enable you to choose which elements of the query data you want to show in the report. You can also apply additional functions to run on the data, and set numerous formatting options.



Building a Report

Navigating to Reports

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Reports** tab.



Creating a New Report

The high-level steps for creating a report are as follows:

- 1 Right-click a reports group (folder) and select **New Report** (or **New Report from Template** to start with a base template that you can refine later). This launches the Reports Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 2 Define Report Attributes such as report name, and optional aliases and owner/notification details.
- 3 Select the Report Template you want to use.
- 4 Choose Report Data by specifying what parts of the query data you want to use for each report element. Optionally, apply legends and top/bottom functions.
- 5 Specify Report Parameters output details, such as file format, paper size, and routing instructions. You can also set limits on the query return, such as row limits, time zone restraints, apply filters, and specify report start and end times.
- 6 Click **Apply** or **OK** to save settings and create the new report.



Be sure to click **Apply** or **OK** frequently to save settings intermittently as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings via these buttons, your settings will not be saved.

- 7 Run the report to test it as described in Running a New or Archived Report.

The following sections provide details on how to use the Report editor to define report attributes, apply a template, choose report data, and specify report parameters.

Defining Report Settings

Report Attributes

The **Report Attributes** tab is where you define a report name, set alias report name and notification options, and view tracking details such as when the report was created and last updated.

The following fields in the **Report** section are required attributes that must be specified when creating a new query.

Report Field	Description
Name	Name for the report. Spaces and special characters are OK.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

The following example shows the Report Attributes for our VPN Logins Outcome report

Name	Value
Report	
Name	VPN Logins Outcome Trend Report
Common	
Resource ID	9RHoDVw0BABCfk2z4e1RyNA==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	
Parent Groups	
vicky's Reports	/All Reports/Personal/vicky's Reports
Creation Information	
Created By	vicky
Creation Time	28 Aug 2006 16:00:50 PDT
Time Since Creation	1 hour(s) 5 min(s) 57 sec(s)
Last Update Information	
Last Updated By	vicky
Last Update Time	28 Aug 2006 16:00:50 PDT
Time Since Last Update	1 hour(s) 5 min(s) 57 sec(s)

Preview... OK Cancel Apply

Report Templates

The **Templates** tab is where you specify the template for the report. You can specify fonts, colors, page headers and footers, and the chart and table combinations and layout you want to use.

Report Template Selection

To populate the editor, select a template from the **Report Template** drop-down menu. ArcSight comes with six stock templates in the System templates folder, or you can navigate to your own template.

The example below shows the system template Three Charts Description Landscape.

Inspect/Edit

Report Editor

Attributes | Template | Data | Parameters | Jobs | Notes

Report Template: Three Charts Description Landscape

Text Components

Header

Name	Value
Header	
Text	
Horizontal Alignment	left
Vertical Alignment	vertical center
Font	Serif, Plain, 10
Foreground Color	0, 0, 0
Background Color	255, 255, 255

Footer

Name	Value
Footer	
Text	
Horizontal Alignment	left
Vertical Alignment	vertical center
Font	Serif, Plain, 10
Foreground Color	0, 0, 0
Background Color	255, 255, 255

Preview

Page 1 of 1 11.0 x 8.5 in

Preview... OK Cancel Apply

Report Template:
Choose a template.
(Arcsight-provided or
custom template)

Text Components:
Specify Header,
Footer, and Text
formatting options for
the report.

Preview Area:
Shows the layout of
the Report Template
you chose.

Text Components

Text Components areas for Header, Footer, and Text sections provides fields to specify values for each of those sections of the report page.

	Attribute	Description
Header	Text	Type in the text you want to use as the header of your the pages in your report, such as the name of your department, or the series of reports to which it belongs. Note: You can use Velocity template references for fields that accept text, as described in “Velocity References for Reports” on page 796 .
	Horizontal Alignment	From the drop-down menu, select where you want the header to appear in the header area: left, right or center.
	Vertical Alignment	From the drop-down menu, select where you want the header to appear in the header area: top, center, or bottom.
	Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
	Foreground Color	From the drop-down dialog, select a foreground color. This will be the color of the lettering.
	Background Color	From the drop-down dialog, select a background color. This color will fill the header box.
Footer	Text	Type in the text you want to use as the footer of your the pages in your report, such as the name of your company, a confidentiality statement, or the date. You can use the variables provided (such as \$currentpagenumber and \$totalpagenumber for page numbers). These are evaluated when you run the report to populate report output with appropriate numbering. Note: You can use Velocity template references for fields that accept text, as described in “Velocity References for Reports” on page 796 .
	Horizontal Alignment	From the drop-down menu, select where you want the footer to appear in the footer area: left, right or center.
	Vertical Alignment	From the drop-down menu, select where you want the footer to appear in the footer area: top, center, or bottom.
	Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
	Foreground Color	From the drop-down dialog, select a foreground color. This will be the color of the lettering.
	Background Color	From the drop-down dialog, select a background color. This color will fill the footer box.

	Attribute	Description
Text	Text	Type in the text you want to use as the title of your report, such as Top 10 Attacks per Zone.
	Horizontal Alignment	From the drop-down menu, select where you want the title to appear in the title area: left, right or center.
	Vertical Alignment	From the drop-down menu, select where you want the title to appear in the title area: top, center, or bottom.
	Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
	Foreground Color	From the drop-down dialog, select a foreground color. This will be the color of the lettering.
	Background Color	From the drop-down dialog, select a background color. This color will fill the title box.

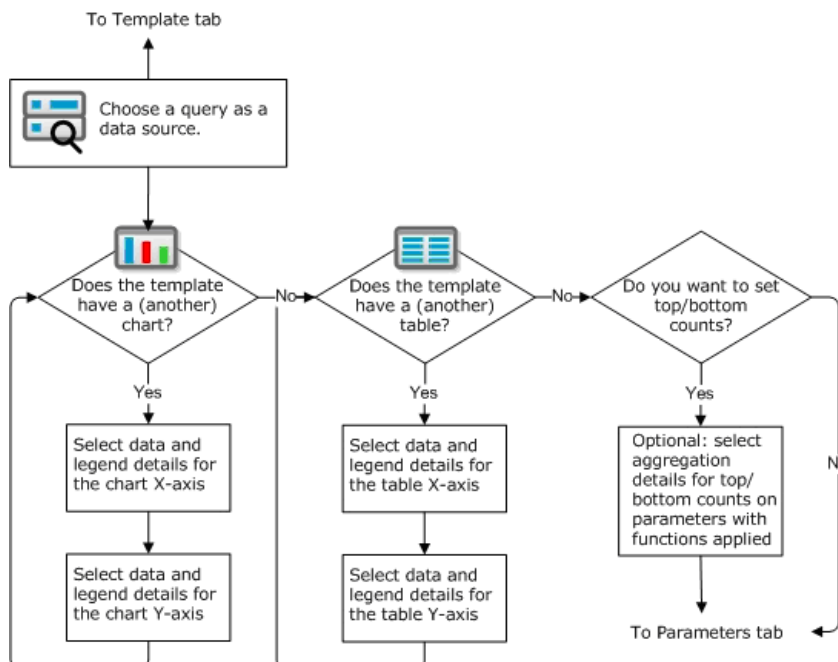
Preview Area

The Preview Area shows the layout of the report, and does not show the formatting updates as you go along. If you have designed other text boxes for your template, the attributes for those text boxes will be displayed here using the same format as those shown above.

Report Data

Once the template is chosen and formatted, you are ready to populate the elements of the report with data.

The **Data** tab is where you choose which parts of the query or filter result data you want to use for each report element, apply legends and, optionally, top/bottom functions.



Use these options to select the data source (query or trend), chart and table type to use for the report, columns to include, and details on how the chart will present of data.

Binding Data to Charts in Reports

Chart Data	Description
Data Source	<p>From the drop-down menu, select an existing data source you want to use for the char part of your report.</p> <p>The data source drop-down menu provides a list of existing resources based on the resource type you selected in the accompanying drop-down. You can report on queries, trends, active lists, or session lists.</p> <p>When the data source is selected, the remaining elements of the Data tab populate with the data available in the selected resource.</p>
Chart Type	<p>From the drop-down menu, select the type of chart you want to use for the chart part of the report. Depending on the template you use, you may have are several types of bar charts available as well as line charts, pie charts, and so forth. The data source and chart type you choose apply to both the X and Y axes.</p>

Selecting Data for the X-Axis on a Chart

Data Source: Choose an existing resource on which to run the report. (Available sources will depend on which resource type is selected.) Data selected here apply to both X and Y axes.

Resource Type: Choose the resource type. You can report on queries, trends, active lists, or session lists.

Chart Type: Choose a chart type. (Bar chart, line chart, pie chart, and so on.)

X, Y Axis Tabs: Indicates which aspect of Data details you are working on. Optionally, you can Aggregate on one of the columns for this Report.

X-Axis Details: Choose and order the data you want to use on the X axis. Optionally, create and position a label for the data.

Display Options and Scale Format: Values set here apply to both X and Y axis data, and appear the same on both tabs.

If the report template you selected contains a **Chart**, bind your result data to the chart as described below.

	X-Axis Data Attribute	Description
Columns and Label	Available Columns	<p>Select the data field(s) from the query you want to show in the X-axis and use the right-hand arrow to move it to the Selected Columns area. The data you select here should be the item(s) you want to count</p> <p>For example, to build a trend report showing number of events over time, use a trend that captures the number of events per day. Add the end time to the X-axis to represent the day and add the count gathered for that day to the Y-axis. In this case, the X-axis is the data label, and the Y-axis is the count.</p>
	Selected Columns	The Selected Columns area shows which data fields you have selected for the X-axis, and provides the opportunity to change the sort order of the data. To change the sort order, select an item to activate the Sort checkbox. Select A-Z to sort data in ascending order; select Z-A to sort data in descending order.
	X-Axis Title	Specify a title for the X-axis.
	Label Rotation	<p>Select a rotation angle for the by entering a digit between 0 and 360.</p> <p>Labels refer to the individual X-axis data points, which are automatically derived from the data. The Label Rotation controls the angle of these labels.</p>
Display Options	Font	From the drop-down menu, select a font for the X and Y-axis text.
	Show Legend	Select this box to show a legend of the data elements. Keep in mind the number of different data elements your query may return. If the data you selected contains many elements, the legend may be large, which will reduce the available space for the chart itself. If you choose to display the legend, you can move its location from choices in the Placement drop-down menu.
	Show Axis Grid	This setting will display the chart results in a table format along side the chart.
Scale and Format	Font	From the drop-down menu, select a font for the X and Y-axis text.
	Show Legend	Select this box to show a legend of the data elements. Keep in mind the number of different data elements your query may return. If the data you selected contains many elements, the legend may be large, which will reduce the available space for the chart itself. If you choose to display the legend, you can move its location from choices in the Placement drop-down menu.

X-Axis Data Attribute	Description
Show Axis Grid	This setting will display the chart results in a table format along side the chart.

Selecting Data for the Y-Axis on a Chart

Y-Axis Details: Choose and order the data you want to use on the Y axis. Optionally, create and position a label for the data.

Summary Function: Optionally, you can enter a Summary Function on one of the columns and aggregate on that data for the Report.

Y-axis data should be numeric. If the data you select is a non-numeric data type, such as a string, apply a numeric *summary function* to it, such as **Count** or **Count distinct**.

Y-Axis Data Attribute	Description
Available Columns	Select the data field(s) from the query you want to show in the Y-axis and use the right-hand arrow to move it to the Selected Columns area. The data you select here should be the item you want to count by. For example, to show how many addresses each of your attacker zones have, you would select the attacker address.

Y-Axis Data Attribute	Description
Summary Function	<p>You can assign a summary function to one or more column of data:</p> <ul style="list-style-type: none"> • Count - Provides a count of all line-items returned by the query. • Count distinct - Provides a count of how many items are unique. For example, if there are 100 IP addresses but only 5 of them are unique, the system will count 5. • Average - Adds the results of numeric data and divides by the number of line items. • Sum - Adds the results of numeric data. • Max - For numeric data, Max calculates the line item with the highest value. • Min - For numeric data, Min calculates the line item with the lowest value. • Median - For numeric data, Median calculates the line item with the value closest to the middle between high and low. • Standard Deviation - For numeric data, measures the dispersion of the values in the data set (how spread out they are). If the data points are all close to the mean, then the standard deviation will be close to zero. If many of the data points are far from the mean, then the standard deviation will be further from zero. If all the data values are equal, then the standard deviation will be zero. The Standard Deviation is the square root of the variance. • Variance - For numeric data, measures how spread out the distribution of data is. The variance is computed as the average squared deviation of each number from its mean. The variance and the standard deviation are closely related measures of dispersion and variability. <p>Selecting one of these functions activates the Aggregation tab, where you can set further parameters on these functions. To set a function, select a column, and choose a function from the Summary Function drop-down menu.</p>
Y-Axis Title	Type in a title for the Y-axis. Select a rotation angle by entering a digit between 0 and 360.
Label Rotation	<p>Select a rotation angle for the by entering a digit between 0 and 360.</p> <p>Labels refer to the individual Y-axis data points, which are automatically derived from the data. The Label Rotation controls the angle of these labels.</p>
Sort by	Optionally, choose a sorting order for the data on the Y axis. You can display data alphabetically (the default), reverse alphabetical, or sort by count.

Specifying Top/Bottom Filters Aggregation Filters for a Chart (Optional)

You can also set **Top/Bottom Counts** for a chart. This tab only becomes active when a summary function is applied to data in the Y axis. Settings in the **Aggregation** tab set top/bottom counts to data with summary functions applied. This is an optional step.

Inspect/Edit

Report: VPN Logins Outcome Tren...

Attributes Template **Data** Parameters Jobs Notes

Chart3 Chart2 Chart1

Data Source: s Outcome Trend Query - Attempt Queries

Chart Type: Line chart 2 sets of data (Z-axis)

Data (X-Axis) Value (Y-Axis) **Aggregation**

Set a top or bottom filter for the chart (optional)

How do you want to filter the chart data?

☒ None (Show all)

☐ Top 10 by means of Number of Logins

☐ Bottom by means of Number of Logins

Top Bottom Filter: Optionally, use aggregation to set top/bottom counts for Y-axis numeric functions.

Display Options

Font: Verdana, Plain, 8 Show X-axis grid Show Y-axis grid

☒ Show Legend Placement: Bottom

Scale and Format

Data (y-axis): ☐ Logarithmic Scale ☒ Show Value

Min Max Incr

Preview... OK Cancel Apply

On the Chart Aggregation tab, set the top or bottom filter for the chart. If there are more charts in your report, repeat these processes until data is bound to all the charts and laid out in your report template.

Aggregation Top/Bottom Filter

Description

None (Show all)

By default, no top/bottom filter is set.

Top

Select **Top** if you want to show the a certain number of entries with the highest values. Enter a digit in the text box, and from the drop-down list, select an appropriate Y-axis data column with a function applied.

Aggregation Top/Bottom Filter	Description
----------------------------------	-------------

Bottom	Select Bottom if you want to show a certain number of entries with the lowest values. Enter a digit in the text box, and from the drop-down list, select an appropriate Y-axis data column with a function applied.
--------	--

Binding Data to Tables in Reports

If the template you selected contains a table, use the Table **Fields** tab to build a visual representation of a table in which to display the query result. You can choose the type of data source (trend, query, active list or session list) and the particular data source (which query, trend, etc.) to report on. Then you can select which fields from the data result you want to show up in your report (with the "Use" checkbox). Use Groups to combine fields into a single column in your Report table (drag and drop or menu commands).

Table Data	Description
------------	-------------

Data Source	From the drop-down menu, select an existing data source you want to use for the table part of your report.
--------------------	--

The **data source** drop-down menu provides a list of existing resources based on the resource type you selected in the accompanying drop-down. You can report on queries, trends, active lists, or session lists.

When the data source is selected, the remaining elements of the Data tab populate with the data available in the selected resource.

Data Source: Choose an existing resource on which to run the report. (Available sources will depend on which resource type is selected.)

Resource Type: Choose the resource type. You can report on queries, trends, active lists, or session lists.


Fields and Groups: Select the data fields you want to display in the table (by enabling **Use** for a field you want to show).
Provide a display name alias and specify data sort order in the column by dragging and dropping fields to desired location in column order.
Group multiple fields in a single column by dragging fields into Groups.

Display Options: Select a column or group to set font, foreground, and background display options.

Global Options: Global options apply to the whole table.

Specifying Fields for a Table

In the **Available Columns** area, you can select the fields you want to display in the table, group multiple fields into a single column as needed, assign Alias names for column headings, specify a data sort order, and set column size and alignment options.

Attribute	Description
Groups	<p>Optionally, you can sort data results from queries by grouping two or more fields into a single column.</p> <p>To create a group: Right-click in the Groups row for a column and choose Make Group. This brings up a dialog where you can name a new group and add the selected field.</p> <p>To add fields to a group: Drag fields from the Fields row to the Groups row. Alternatively, right-click a field and choose Add to Group. This brings up a dialog where you can name the group to which you want to add the selected field.</p>
Function	<p>To set a function on a field, right-click in the Function row for that field's column. Select the function you want to apply to the column from the Function drop-down menu. Once the function is set, the field will be displayed with the function icon (). When you apply a function to a column, the Aggregation tab</p>
Use	<p>By default, all data entries are selected for use in the table. If you do not want to use all the available columns, uncheck the corresponding checkbox.</p> <p>Caution: If you de-select a data entry to indicate you do not want to use that column in report, the column is automatically pushed to the far right (the end of the table) to move it out of the way so that you can focus on the columns you are using. If you then select "Use" again for that same data entry, its column is inserted back into its original position along with the other columns you have selected to use.</p>
Field	This displays the name of the field as it is referred to in the ArcSight database. This field is not editable.
Alias	Enter a display name alias for the data column. For example, if the column is referred to as Source Translated Zone Name in the ArcSight database, this name can be shortened to Zone Name or Src Zone for display in the report table. In our example, we provide the aliases Time instead of Timestamp and Number of Logins for Category Outcome (Count).
Width	<p>Set column Width to either of the following options:</p> <ul style="list-style-type: none"> Auto - Automatically divides column width evenly among the selected columns User Specified Layout - This option requires that you enter numbers to specify percentage widths for individual columns.
Sort	Indicate the sort order for the data in each column.
H Align	Right-click in the H Align row to get a drop-down menu for specifying horizontal alignment of text in a given column. You can select for left- aligned, centered, or right-aligned text in the corresponding column.
V Align	Right-click in the V Align row to get a drop-down menu for specifying vertical alignment of text in a given column. You can select for top, bottom, middle, or baseline text in the corresponding column.

Attribute	Description
Page Break	Right-click in the Page Break row in a column to get options for specifying a page break before or after the that column.
Re-order Column Arrows	To specify a different order for how the columns are displayed, select a column and use the up/down arrows to move it up or down in the order.

With the **Custom Layout** options, you can specify custom column widths for the data in the table. By default, the **Custom Layout drop-down** menu shows User Specified Layout, which enables you to enter a numeral to specify a percentage for individual columns. Select one of the following:

- **Fit content** - Adjusts the column width to accommodate its content without wrapping. If the content is wider than the table, the table is extended to multiple pages.
- **Fit content one table area per page** - Adjusts the column width to accommodate its content without wrapping, and breaks each column onto its own page.
- **Fit content to page** - Adjusts the column width to accommodate its content without wrapping, and stretches the last column to fill the page.
- **Equal width columns** - Each column receives the same width to fit across a single page.
- **User specified layout** - Enables you to enter a numeral that represents a percentage of the overall page width. You can set a percentage for each column that totals 100%, or enter a percentage for one column, and the others selected will receive an even percentage of the space remaining.

The **Display Options** area provides format options for each individual data column. This enables you to set different font style, size, and color and column background colors for each data column. To activate the display options, select one or more data columns:

- **To select one field:** click the field.
- **To select one or more contiguous fields:** click a field, hold down the Shift key, and select the remaining fields.
- **To select one or more non-contiguous fields:** click a field, hold down the Ctrl key and select the remaining fields

Attribute	Description
Font	From the drop-down menu, choose a font for the selected column(s).
Foreground Color	Foreground color for text, any visible lines that describe rows/columns, and other elements in the foreground. The example above shows all columns using black (RGB 0,0,0).
Background Color	Background (field) color for the data column. The example above shows the Count line with a pale yellow background (RGB 255, 255, 153).

In the **Global Options** area, you can set formatting options that apply to the whole table (not just one column).

Attribute	Description
Merge cells	Indicates whether to merge cells for grouped columns. When this option is enabled, identical values in grouped columns will show only once. When this option is disabled, identical values will show as many times as they occur (regardless of whether they are grouped).
Show group header	Indicates whether to show a group header row. This is a group label for when you have a summary function that adds one more rows at the end of the section. If this option is enabled, the table will include an extra column with a header derived from the content by which the section is grouped.
Show group columns	Enable this option to populate the grouped columns with data. (If this option is disabled, grouped columns will have empty contents.)
Grand total	If you want to provide a grand total of all the sections, check the Show grand total box.
Label	If you selected a grand total, you can apply a label for the grand total. (For example, Total VPN Login Attempts.)

Click the **Preview...** button to preview the report table with the current configuration.

Set Top/Bottom Counts in Table Aggregation Tab (Optional)

This tab only becomes active when a function is applied to a column on the **Fields** tab. Settings in the Aggregation tab set optional top/bottom counts to data with summary functions applied to individual fields.

Report Parameters

The **Parameters** tab is where you set report output details such as file format, paper size, and routing instructions. From here you can also set limits on the query return such as row limits and time zone restraints, apply filters, and specify report start and end times.

Inspect/Edit
Report:VPN Logins Outcome Tren...

Attributes Template Data **Parameters** Jobs Notes

Report Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input type="checkbox"/>
Run as User	Select a User	<input type="checkbox"/>
Email to		<input type="checkbox"/>
Email Format	Send URL	<input type="checkbox"/>

Query Parameters

Name	Value	Use Default
Table		
Row Limit	10000	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart2		
Row Limit	50	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart1		
Row Limit	50	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>

Report Parameters: Set Report output details.

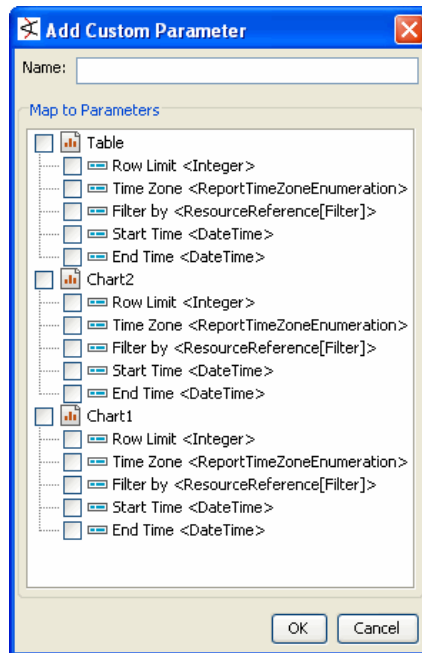
Add Custom Parameters: Add and Edit custom parameters.

Query Parameters: Set override parameters for query data selected for each element of the report.

In the **Report Parameters** area, enter the following values. The Use Default checkboxes to not apply to these items.

Common Parameters	Description
Report Format	<p>From the drop-down menu, select one of the following report output formats:</p> <ul style="list-style-type: none"> • pdf - Outputs the report as an Adobe PDF file. • xls - Generates a Microsoft Excel file for tables and charts. • rtf - Produces a rich-text format document. • csv - Creates tabular data as a list of comma-separated values. (See note below.) • html - Generates the report in a Web page displayed by the default web browser. <p>Notes: Reports generated in CSV format are not the full equivalent of exports to other formats like PDF or HTML. CSV format is useful for loading report data into a spreadsheet for further manipulation. Since CSV is meant to contain tabular data, only the table data of a report is normally useful. Therefore, ArcSight ESM exports only the table data portion of a report to CSV format, ignoring any other report information such as charts or text, including report titles</p>
Page Size	From the drop-down menu, select a paper size.
Run as User	<p>Run the report as a particular user. From the drop-down menu, select the user name by which you would like to run the report.</p> <p>For example, this option would allow an administrator for an Managed Security Service Provider (MSSP) to run report for a customer. The administrator would need write permissions to the user.</p>
Email to	<p>You can have the report sent as email to one or more users.</p> <p>From the drop-down menu, select the users to whom the report should be emailed.</p>
Email Format	<p>You can e-mail a link (URL) to the report or send it directly as an e-mail attachment.</p> <ul style="list-style-type: none"> • If the report is large and is saved (archived) to a network-accessible location, you may want to select Send URL to point users to the report. • If you want to send the report directly to the user's email box, select Attach Report.
Row Limit	You have the option of setting a row limit (for example, 1,000) if you think the generated table could exceed a manageable size.

To add a custom parameter that applies to the Report data, click the **Add** button. Parameters added here override those set in the query. For example, if you want all the report elements to report on events for the past 2 hours, you can create a start-time parameter of \$Now-2h, which will set both table and chart start times to \$Now-2h. Custom parameters are saved locally to the report definition, and are not persisted back in the query.



Set parameters and click **OK** to apply them to the report definition.

Back in the **Parameters** tab in the **Custom Parameters** section, enter an override parameter for the field(s) you selected from the Add Custom Parameters dialog.

In the **Query Parameters** area, enter any override values for the parameters in your query data. The Use Default checkboxes are only activated for items where default parameters exist and override values can be entered.

Enter these override parameters as needed for each chart and table.

Query Parameters	Description
Row Limit	You can limit the number of rows in the table to a number specified. Select a row limit value from the drop-down list.
Time Zone	By default, the Manager time zone is used. Choose the Console time zone, or another of the time zones from the drop-down list.
Filter By	Set a filter to operate on the query conditions.
Start Time	<p>To set a start time that overrides the one set in the query, disable Use Default for this field and specify a start time here.</p> <p>For example, if you want all the report elements to report on events for the past 2 hours, you can create a start-time parameter of \$Now-2h, which will set both table and chart start times to \$Now-2h.</p> <p>This setting is saved locally as part of the report definition, not as part of the original query upon which the report is based.</p>
End Time	<p>To set an end time that overrides the one set in the query, disable Use Default for this field and specify an end time here.</p> <p>This setting is saved locally as part of the report definition, not as part of the original query or trend upon which the report is based.</p>

Be sure to click **Apply** to save settings or **OK** to save settings and close the Inspect/Edit details for this report.

Setting Special Parameters for Running Large or Complex Reports

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the ArcSight Manager to crash and re-start. To prevent this scenario, you can set up the Manager to expose a special report parameter for generating the report in a separate process. The separate process has its own VM and heap, so the report is more likely to finish. Even if the memory allocated is still not enough, the report failure will not crash the Manager. This option must be set up on the Manager to expose it in the Console report parameters list. The steps are as follows:

- 1 On the ArcSight Manager in the `server.properties` file, set `report.canarchiveportinseparateprocess=true`. (This will make a new report parameter available on the Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight ESM Console, open the report that you want to run in a separate process in the Report **Editor**, and click the **Parameters** tab. Set the parameter **Generate Report In Separate Process** to **true**.
- 4 Run the report. The report should run like a normal report, but it will not consume the resources of the Manager VM. See notes below for more information.



Tips:

- If a report is saved with the parameter set to "**true**", the report is archived as a separate process even if the property `report.canarchiveportinseparateprocess` in `server.properties` is set back to **false** later on.
- This property indicates whether reports are allowed to be archived in a separate process. When this property is set to "**true**", the option to run and archive the report in a separate process is available in the common properties in the Report Editor. Setting the value of the property to true will cause the report to be archived in a separate process. The main benefit of archiving a report in a separate process is to avoid consuming Manager resources and potentially crashing the Manager.
- Refer to the ArcSight ESM Administrator's Guide for more information on setting server properties on the Manager. The property `Canarchiveportinseparateprocess` is also documented in the `server.defaults.properties` file.
- Use this parameter only in special circumstances as needed. For example, if archiving a report is causing the manager to crash then you might apply this solution. Generally, if a report contains tables that have more than 500,000 rows with 4 or 5 columns per row it is likely that the report is large enough over-tax the Manager VM memory. However, the tipping point may vary depending on the Manager heap size and the details and data in the tables so it is best to only resort to this solution if you encounter problems archiving a particular report.

Reports that query over a large time range with complex joins run much faster if the query contains a full scan database hint. This option must be set up on the Manager to expose it in the Console report parameters list. The steps are as follows:

- 1 In the ArcSight ESM Manager in the `server.properties` file, set `report.canquerywithfullscanhint=true`. (This will make a new report parameter available on the Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ArcSight ESM Console, open the report that you want to contain the full scan hint in the Report **Editor**, and click the **Parameters** tab. Set the parameter **Query with Full Scan Hint** to **true**.
- 4 Run the report.



If a report is saved with the parameter set to **"true"**, the full database optimization hint is applied even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to **false** later on.

When the property `report.canquerywithfullscanhint` is set to **"true"**, the report uses the FULL_SCAN hint in the SQL queries it generates to query the database. The content of the report does not change, but the queries logged in `server.report.log` contain the hint. The main benefit of querying the database with the FULL_SCAN hint is that it can significantly reduce the runtime for SQL queries that query over events within a large time range and contain complex joins.

Refer to the ArcSight ESM Administrator's Guide for more information on setting server properties on the Manager. The property `report.canquerywithfullscanhint` is also documented in the `server.defaults.properties` file.

Use this parameter only in special circumstances if your organization has determined with the help of ArcSight support or professional services that it is appropriate.

Setup and Parameters to Generate PDF Reports with Asian Fonts

To generate reports in PDF with Asian fonts, the appropriately localized Adobe Reader 8.0 (for the language of your platform) must be installed on the ArcSight Manager with the OpenType fonts for Asian languages. (The font files you need are included as part of the localized Adobe Reader 8.0 installation.)

Additionally, font paths in `server.properties` need to map to the Adobe Reader 8.0 fonts. On the Manager edit `server.properties` as follows:

- Set `report.font.trueType.path` property to point to the directories that contain the TrueType and OpenType fonts. On Windows systems, these paths are typically `"C:\\WINNT\\fonts;C:\\Program Files\\Adobe\\Reader 8.0\\Resource\\CIDFont"`, where ";" is used as a path separator to separate the multiple paths. (In the properties file, use backslashes as shown to escape the backslashes for the Windows-style path separators.) On UNIX systems, these paths are typically `"/usr/lib/font:<Adobe_Reader_Directory>/Resource/CIDFont"` where ":" is used as the path separator.
- Set `report.font.cmap.path` property to point to Adobe Reader's CMap directory. On Windows systems, this is typically `"C:\\Program Files\\Adobe\\Reader 8.0\\Resource\\CMap"`. (In the properties file, use backslashes as shown to escape the backslashes for the Windows-style path separators.) On UNIX systems, the path is typically `"/usr/lib/font:<Adobe_Reader_Directory>/Resource/CMap"`.

Since the Adobe Reader supports OpenType fonts but does not directly support TrueType fonts, the ArcSight Manager provides default mappings between TrueType and OpenType fonts in

`<arcsight_home>\il8n\server\reportpdf_config_<locale>.properties` file. Generally, the default mappings will suit your purpose but if not, you can edit the `reportpdf_config_<locale>.properties` file to change mapping of any TrueType font to a different OpenType font.

After making these configuration updates, save the `server.properties` and `reportpdf_config_<locale>.properties` files, and restart the Manager. (Be sure to download and install the Adobe Reader and font files first, then change and save the settings in the properties files based on installed font paths, and restart the Manager.)

If you try to generate PDF reports with Asian fonts without the above setup, the Asian language strings will appear mangled. For more information, see the *ArcSight ESM Administrator's Guide* "Troubleshooting" section.

Editing a Report

- 1 Navigate to **Reports** in the Navigator panel, select the **Report** tab, and select the report you want to modify.
- 2 Double-click the report, or right-click and select **Edit Report** from the context menu. This launches the Report Editor in the Inspect/Edit panel, and shows the definition for the selected report.
- 3 Edit the report definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)

End-to-End Reporting Examples

This topic includes two examples:

Quick-start example with Report Wizard - An introductory example of how to create a simple report on the results of a single, stock query with the Report Wizard.

Advanced example - A more in-depth example reporting on the results of several trend-queries and using a heavily-modified 3-charts template. This example walks you through creating the following resources for example queries, trend, and report:

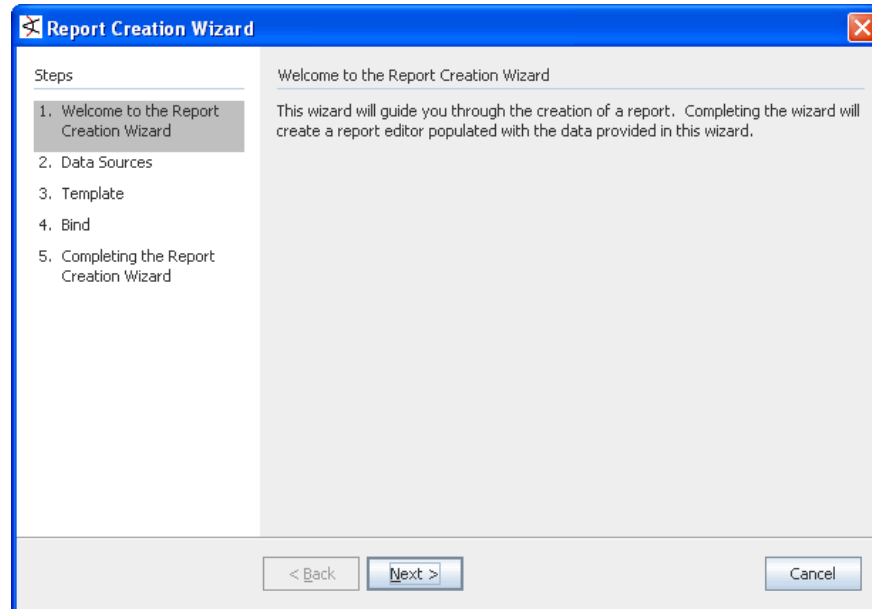
- A base query that captures data about number of VPN login attempts per hour
- A trend that takes the base query as input, executes it, and stores captured data per a schedule you define
- Queries that build on the trend to filter on various VPN login outcomes
- A report that uses the complex queries as data sources and provides visual representations of query results in charts and tables based on an ArcSight provided template

Even if you do not anticipate immediately having to create these elements from scratch (ArcSight provides a starter set of stock reporting content), we suggest working through both the simple example and the more complex one to gain an understanding of how queries, trends, and templates work together in the context of reporting.

Refer also to other topics in [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools.

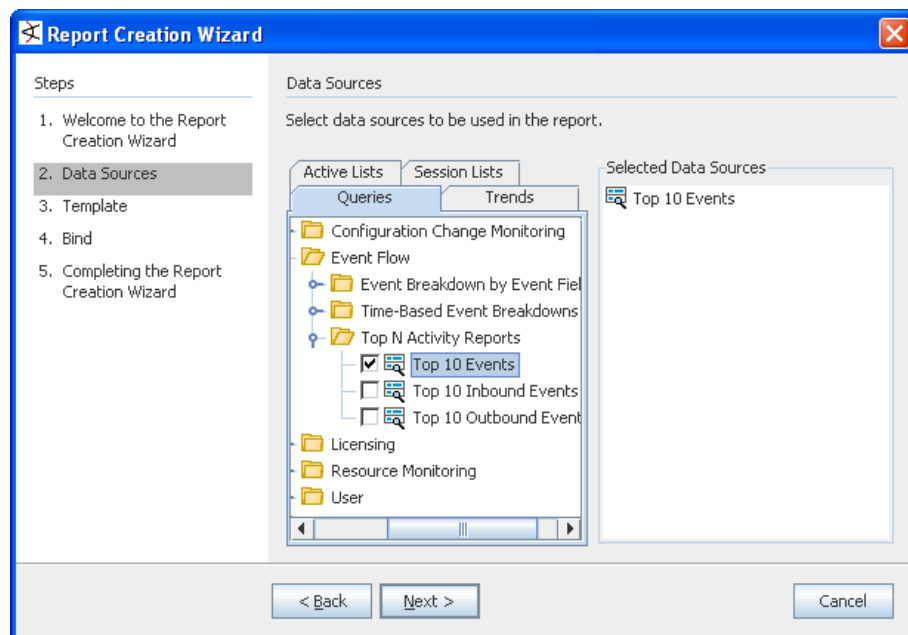
Quick Start Example of Creating a Simple Report with the Wizard

- 1 Navigate to the Reports resource in the Navigator panel and click the **Reports** tab. Right-click your user folder and choose **Start Report Wizard**.



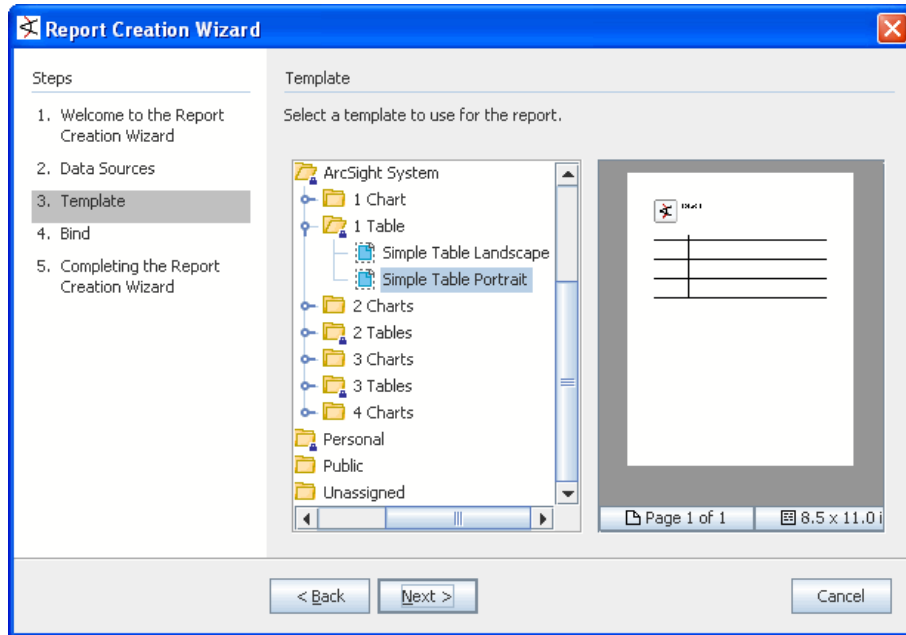
Click **Next**.

- 2 On the **Data Sources** page, select the **Queries** tab (if not already selected, and navigate the Queries tree to choose an existing query. For this example, we select the **Top 10 Events query**, which you can find in Queries/Shared/All Queries/ArcSight Administration/Event Flow/Top N Activity Reports/.



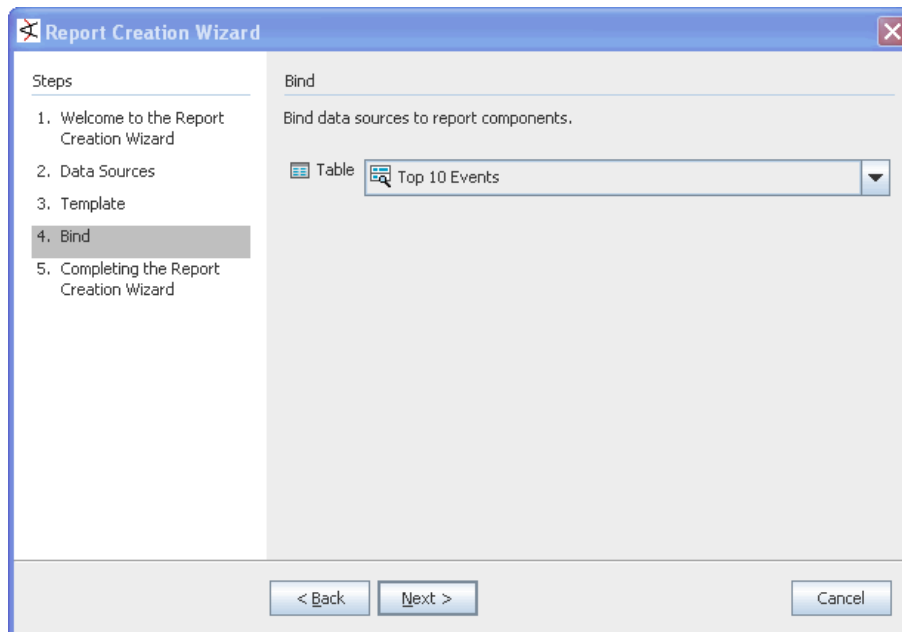
Click **Next**.

- 3 On the **Template** page, select a template. For this example, select the **Simple Table Portrait** template under /Report Templates Shared/All Report Templates/ArcSight System/.



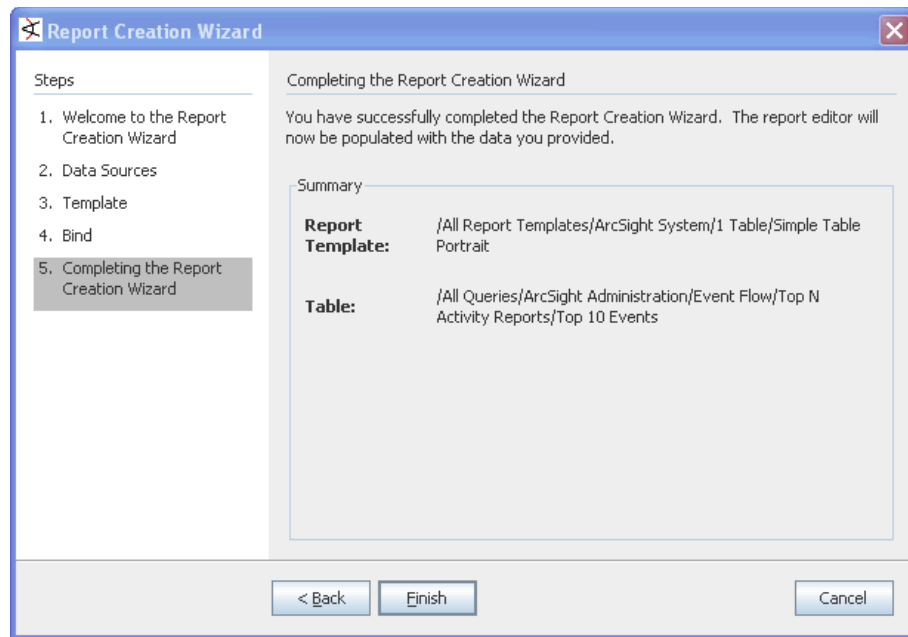
Click **Next**.

- 4 On the **Bind** page, select a template. For this example, select the **Simple Table Portrait** template under /Report Templates Shared/All Report Templates/ArcSight System/.



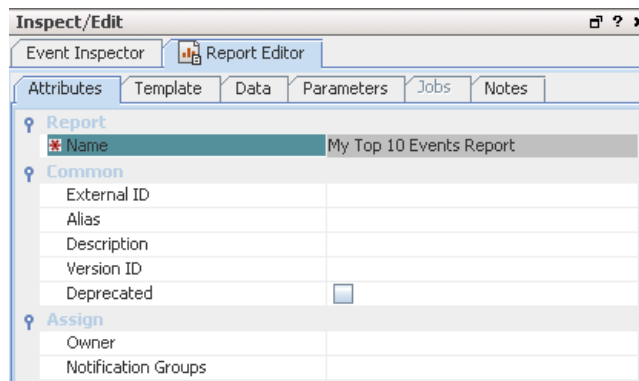
Click **Next**.

- 5 Review the report configuration summary.



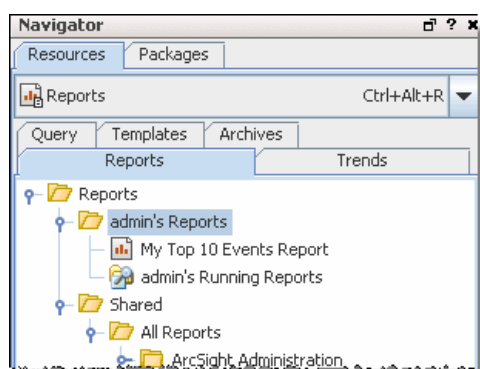
When you are satisfied with the report configuration, click **Finish** on the last page of the Report Wizard.

- 6 On the **Report Editor Attributes** tab (which is automatically displayed), enter a **Name** for the report. For this example, we name the report "My Top 10 Events Report".



Click **Apply** or **OK** on the Report editor to apply the report name and create the report.

- 7 The new report is added to your Reports folder shown in the Navigator.



- 8 On the Navigator panel Reports tree, open your Reports folder, right-click on the new report and select **Run > Report with defaults**.

Advanced Reporting Example Overview

We build an example query that shows the number of login attempts on a virtual private network (VPN). Then, we use the query in a trend to collect data on VPN login attempts on an hourly basis. Next, we build several more focused queries on top of the trend to get views into particular slices of the data (all login attempts, successful logins, and failed logins).

Finally, we use the data results from the queries and trends to create a report. To format the report, we use one of the ArcSight provided templates.

Start by navigating to the Reports resource in the Navigator panel, then follow these steps to build the example report:



You will need a set of canned VPN login events to properly verify the query and trend resources created for this example.

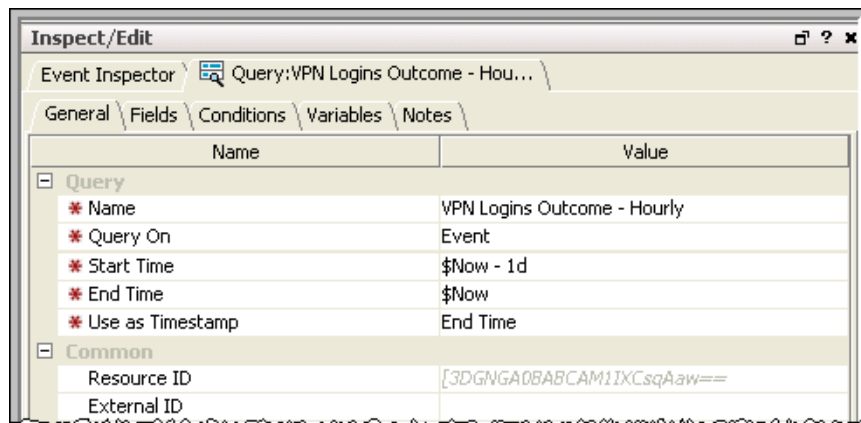
1. Build the VPN Logins Outcome Query

Start by building a base query that captures VPN Login Data to return a count of hourly VPN login attempts. Following is a summary of configuration details you can use to create this query. (If you need more general help on creating queries in ArcSight ESM, refer to Building Queries.)

Query Name and Other General Attributes

Create a new query, name it, and set general attributes for it on the Query **General** tab as shown.

Query Attributes	Value
Name	VPN Logins Outcome - Hourly
Query on	Event
Start Time	\$Now - 1d
End Time	\$Now
Use as Timestamp	End Time

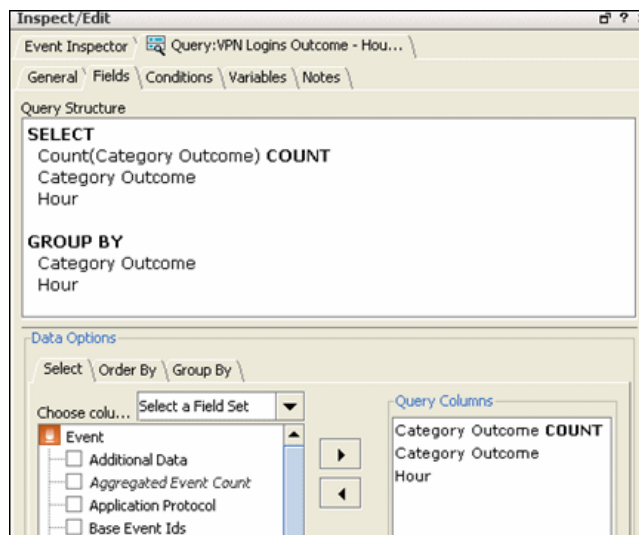


Fields to Include in Query Result

On the Query **Fields** tab, select fields and apply functions as shown to populate columns in the table of result data.

Selected Fields	Description
Category Outcome (COUNT)	To get this, first add Category Outcome to the Query Columns list. Then select it from the Query Columns list and use the Function drop-down menu to apply the COUNT function to it.
Category Outcome	Add the Category Outcome field to the Query Columns list again, but do not apply any function to it. This column will simply contain the outcome of each login attempt (success or failure).
Hour	To get this, define a variable called Hour and assign the GetHour function to it, which will return the hour value based on the end time of the event. (Click the Variables tab to define the Hour variable first. Then you can return to the Select tab to add the Hour variable to the Query Column list.) This column will contain the date and time of the login attempt.

Group by Category Outcome and Hour.



Query Conditions

On the Query **Conditions** tab, define some logical conditions for the login data that narrow the query result to return only the data you are interested in. Filter on VPN Logins by specifying that each login attempt must be categorized in a specific event category and device group:

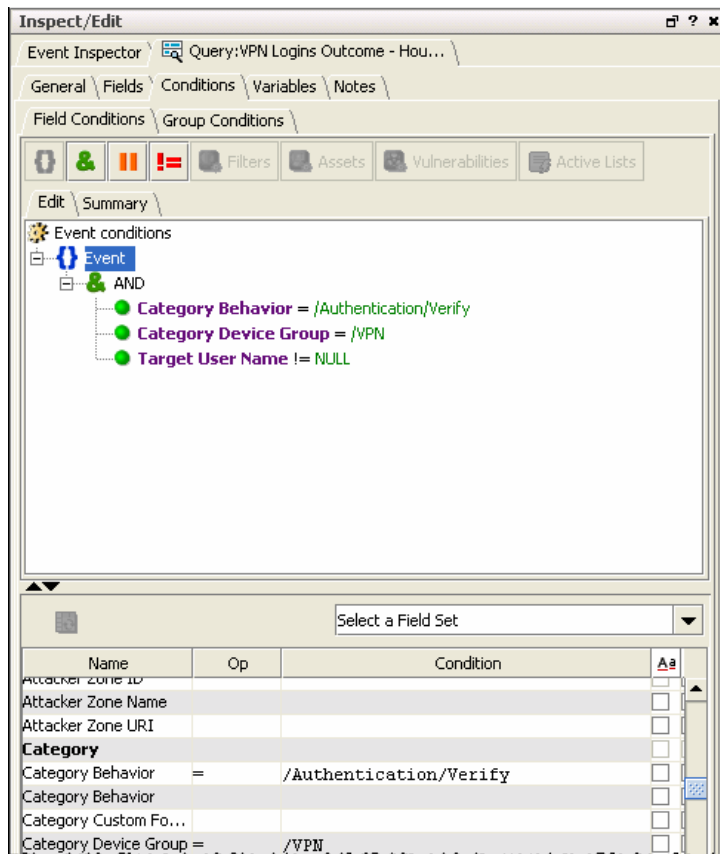
Category Behavior = /Authentication/Verify

Category Device Group = /VPN

Also, each login attempt must have a target user name value:

Target User Name Is NOT NULL

Here is how the Field conditions on this query should look in the display once you have set them:



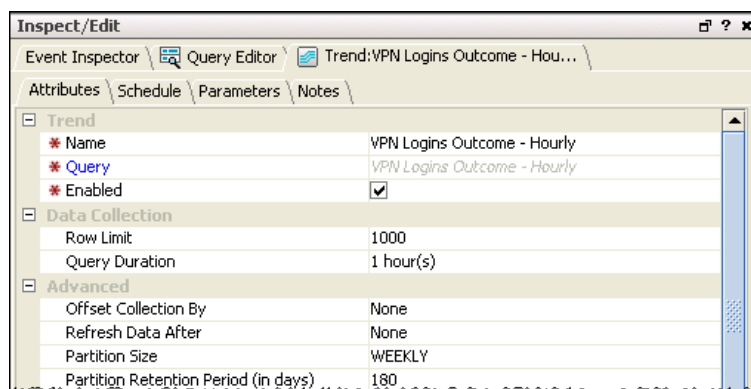
Click **Apply** or **OK** in the Query Editor to save the new query.

2. Build the VPN Logins Outcome Hourly Trend

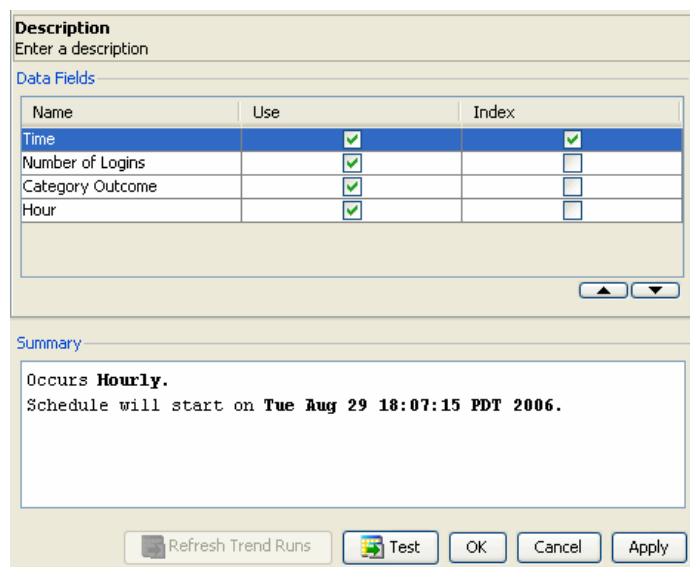
Next, create a new trend, name it, and set general attributes for it on the Trend **Attributes** tab as shown. This trend will use the data results from the VPN Logins Outcome Query you just created. Keep the defaults for Trend Interval (1 hour to collect

data on an hourly basis) and row limit at 1,000 (it will stop collecting data when the table is filled at that limit).

Trend Attributes	Value
Name	VPN Logins Outcome - Hourly
Query	VPN Logins Outcome - Hourly
Enabled	On
Trend Interval	1 hour(s)
Row Limit	1000



Under Data Fields, you can see the fields the trend is getting from the query initially reflected with the original field names: TimeStamp, COUNT(CategoryOutcome), CategoryOutcome, Hour. For readability, change these to the aliases Time, Number of Logins, Category Outcome, and Hour as shown below.



From here, you can test the trend to ensure you are getting correct data. To do this, click the **Test** button on the Trend **Attributes** tab. The Test Trend dialog returns an example

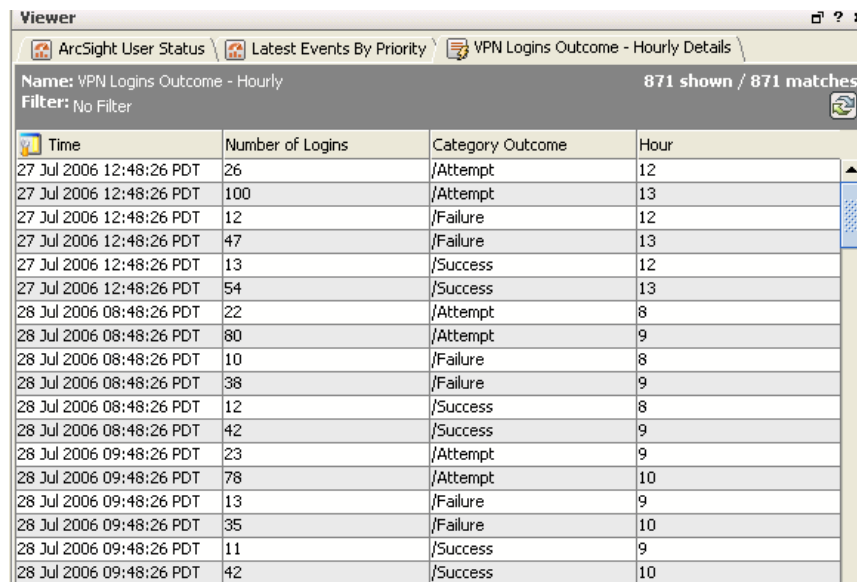
result set. For each row, the Trend should return Timestamp, count of login attempts, Category Outcome (Attempt or Failure), Hour (from the Hour variable).

Trends also have schedules. On the Trend **Schedule** tab, define a schedule that specifies how often you want to run the trend. For the example, define this one to run every hour on the hour (Hourly, every 1 hour at "0 minutes after").

A Trend's range defines when to start and terminate the data collection.

The Trend will start as you specified and keep going until it is manually terminated.

Here is the data collected from a trend that ran hourly for a few days. You can view result data from your trend in the grid view by selecting the Trend in the Navigator and clicking on the Data Viewer for it in the right-click menu.



Time	Number of Logins	Category Outcome	Hour
27 Jul 2006 12:48:26 PDT	26	/Attempt	12
27 Jul 2006 12:48:26 PDT	100	/Attempt	13
27 Jul 2006 12:48:26 PDT	12	/Failure	12
27 Jul 2006 12:48:26 PDT	47	/Failure	13
27 Jul 2006 12:48:26 PDT	13	/Success	12
27 Jul 2006 12:48:26 PDT	54	/Success	13
28 Jul 2006 08:48:26 PDT	22	/Attempt	8
28 Jul 2006 08:48:26 PDT	80	/Attempt	9
28 Jul 2006 08:48:26 PDT	10	/Failure	8
28 Jul 2006 08:48:26 PDT	38	/Failure	9
28 Jul 2006 08:48:26 PDT	12	/Success	8
28 Jul 2006 08:48:26 PDT	42	/Success	9
28 Jul 2006 09:48:26 PDT	23	/Attempt	9
28 Jul 2006 09:48:26 PDT	78	/Attempt	10
28 Jul 2006 09:48:26 PDT	13	/Failure	9
28 Jul 2006 09:48:26 PDT	35	/Failure	10
28 Jul 2006 09:48:26 PDT	11	/Success	9
28 Jul 2006 09:48:26 PDT	42	/Success	10

When you are satisfied that the Trend is set up correctly, click **Apply** or **OK** in the Trend Editor to save the trend.

3. Filter the Trend Data (Login Attempts, Successes, Failures)

You can further refine the VPN login query data by creating separate queries based on the trend, each of which capture information a particular aspect of VPN login events.

Developing several trend-based queries like this (to show different data slices of common scenarios), gives you a rich set of data views from which to run reports later.

Create three more queries all of which use the original trend as their data source, and then further filter the data to show only attempts, failures, or successes, respectively. Use each of these queries, **Attempt**, **Failure**, and **Success**, to further filter the login data captured in the trend:

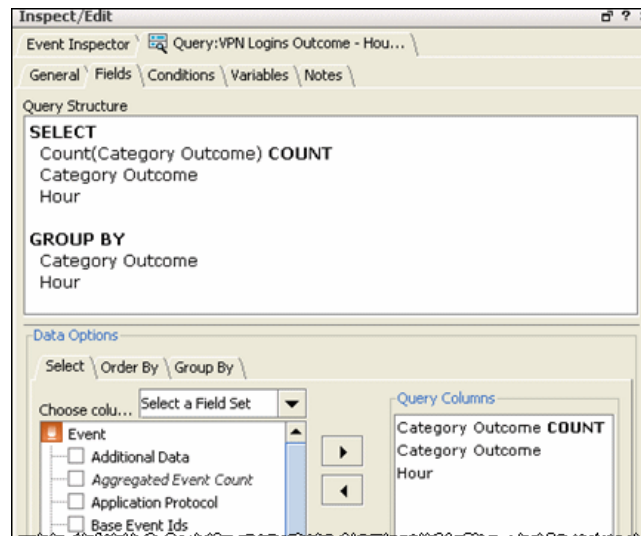
- **Login Outcome Trend Query - Attempt**
- **Login Outcome Trend Query - Failure**
- **Login Outcome Trend Query - Success**

As an example of how this is done, here are the details for creating one of these; the **Failure** Query definition.

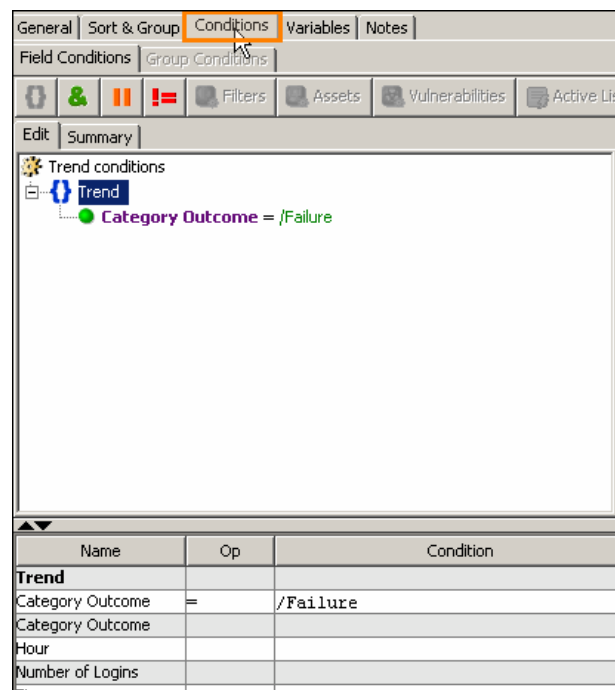
Create a new query and name it **Login Outcome Trend Query - Failure**.

As the query's data source type, choose **Trend** and select the “VPN Logins Outcome - Hourly” trend.

In the Query **Fields** tab, choose the same fields as in the original query to populate columns.



On the **Conditions** tab, specify **Category Outcome = /Failure**. The query will only return the login attempts that failed.



Save your changes. You have now built a query that reports on failed VPN login trends.

Create the other two queries (Login Outcome Trend Query - Attempt and Login Outcome Trend Query - Success) the same way specifying the appropriate Category Outcome condition for each.

Now you are ready to report on the Trend data.

4. Create the VPN Logins Outcome Report on Trend Data

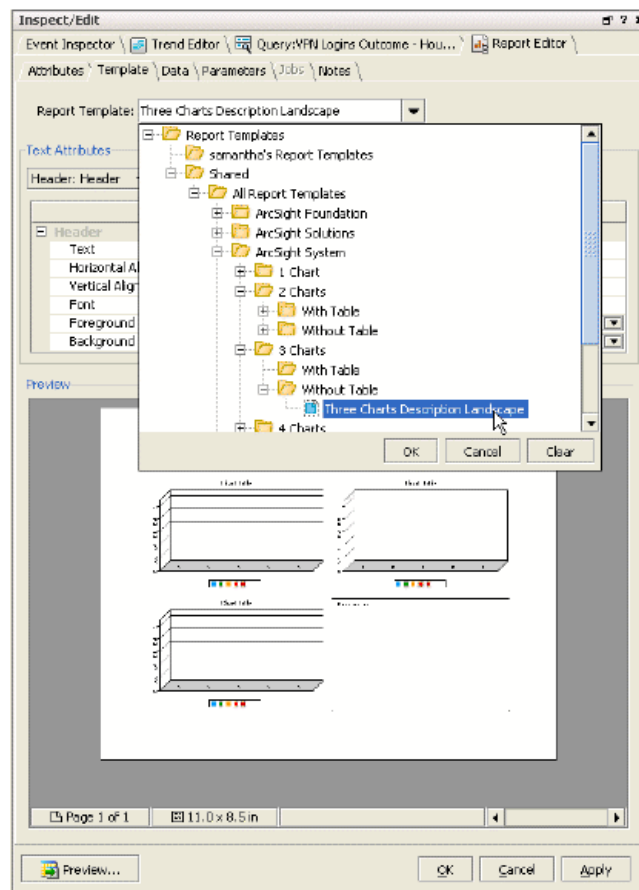
You can leverage multiple data sources in your report. For this example, you can use all three of the VPN Login trend-based queries you just built to create a report.

On the **Reports** tab, create a new report in your user folder and name it **VPN Login Outcome Trend**.

Choose a Template and Bind it to Result Data

A Template defines the visual constructs of a report such as layout, portrait or landscape, number of tables, number and types of charts, placeholders for text areas, and so on. You can find the ArcSight provided templates under **Report Templates/Shared/All Report Templates/ArcSight System/**.

In the Editor (Inspect/Edit panel) for your new report, click the **Template** tab and select the **Three Charts Description Landscape** to use as the Report Template. (Look in the drop-down tree under 3 charts/Without Table/ to find this template). In the preview panel you can see what the report template looks like. Double-click the template preview to open it in the viewer. Here you can see what the report will look like before adding the data.



On the Reports **Data** tab, you can bind each of the three charts in the template to each of the VPN login "trend" queries. (The data source type for each of these charts will be a query, but remember that each of the queries uses a trend as its data source, which, in turn, was built on our original query.)

Chart	Description
Chart 1	<p>On the Report Data Chart 1 tab, select Login Outcome Trend Query - Attempt as the Data Source for the first chart. This query returns the number of login attempts over the last hour.</p> <p>On the X-Axis (horizontal) tab, add the Hour value to the Selected Columns. We'll show the Hour value on the X axis of the chart.</p> <p>On the Y-Axis (vertical) tab, place the Number of Logins (Category Outcome with "Count" applied to it) in Selected Columns. This will show on the Y axis of the chart.</p> <p>For Chart Type select a line chart.</p>
Chart 2	<p>On the Report Data Chart 2 tab, select Login Outcome Trend Query - Failure as the data source for the second chart. This query returns the number of failed logins per hour.</p> <p>Configure this chart also to show the Hour value on the X (horizontal) axis, and the number of failed logins on the Y (vertical) axis</p>
Chart 3	<p>On the Report Data Chart 3 tab, select Login Outcome Trend Query - Success as the data source for the third chart. This Query returns the number of successful logins per hour.</p> <p>Specify the same assignments as the other charts for X and Y axis.</p>



At this point since you have selected some data for the report, you can click **Apply** to create the new Report and then continue working. It is a good idea to save frequently.

Using Custom Parameters

On the Report **Parameters** tab, you can view all the common parameters for the report (in Report parameters area), and all the parameters required for each chart (in Query Parameters area).

You can also provide Custom parameters. You can use Custom parameters to tie together similar parameters from multiple queries for one consistent value. For example, we could do this with Start Time and End Time.

Use Custom Parameters to tie together similar parameters (like Start Time and End Time) from multiple queries for one consistent value.

Query Parameters		
Name	Value	Use Default
Chart3		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart2		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart1		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>

Create a new Custom parameter called "start_time".

Click the **Add** button on the **Parameters** tab, and create a new parameter called start_time to prompt for Start Time field values. Map it to "Start Time" for all three charts (Chart 1, Chart 2, and Chart 3).

Add Custom Parameter

Name: start_time

Map to Parameters

- ☐ Chart1
 - ☐ Row Limit <Integer>
 - ☐ Time Zone <ReportTimeZoneEnumeration>
 - ☐ Filter by <ResourceReference[Filter]>
 - ☒ Start Time <DateTime>
 - ☐ End Time <DateTime>
- ☐ Chart2
 - ☐ Row Limit <Integer>
 - ☐ Time Zone <ReportTimeZoneEnumeration>
 - ☐ Filter by <ResourceReference[Filter]>
 - ☒ Start Time <DateTime>
 - ☐ End Time <DateTime>
- ☐ Chart3
 - ☐ Row Limit <Integer>
 - ☐ Time Zone <ReportTimeZoneEnumeration>
 - ☐ Filter by <ResourceReference[Filter]>
 - ☒ Start Time <DateTime>
 - ☐ End Time <DateTime>

OK Cancel

The custom parameter is added to the list of report parameters under Custom Parameters.

Similarly, add an End Time by adding a new parameter called "end_time" and map it to End Time for all three charts.

On the Parameters tab under Custom Parameters, use the drop down menus to choose the following values for your new parameters:

- Set **start_time** to \$Now-1d
- Set **end_time** to \$Now

Inspect/Edit

Event Inspector | Report:VPN Login Outcome Trend

Attributes | Template | Data | **Parameters** | Jobs | Notes

Report Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input type="checkbox"/>
Run as User	Select a User	<input type="checkbox"/>
Email to		<input type="checkbox"/>
Email Format	Send URL	<input type="checkbox"/>
Custom Parameters		
start_time	\$Now - 1d	<input type="checkbox"/>
end_time	\$Now	<input type="checkbox"/>

+ Add... | Edit... | Remove

Query Parameters

Name	Value	Use Default
Chart3		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart2		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart1		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>

Preview... | OK | Cancel | Apply | Help

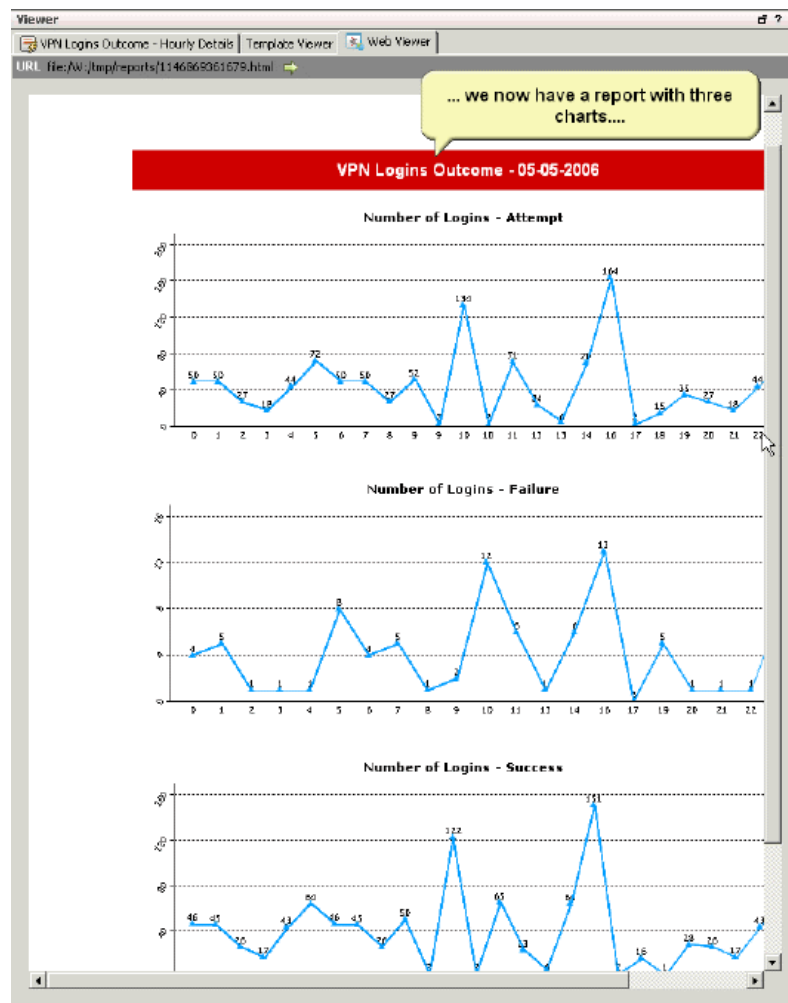
Click **Apply** or **OK** in the Report Editor to save the new report.

5. Run the Report

To run the report, select the VPN Login Outcome Trend report in the Navigator panel and choose **Run > Report with defaults** from the right-click menu to run and view the report.

In the Web Viewer we now have a report with three charts each showing a different slice of the data:

- Number of login attempts
- Number of failed logins
- Number of successful logins



Chapter 12

Running and Managing Reports

This chapter describes how you use ArcSight to monitor enterprise security.

[“Running Reports” on page 287](#)

[“Managing Reports” on page 291](#)

[“Archiving Reports” on page 294](#)

Running Reports

Defined reports are usually run on a schedule and their output archived automatically. But there are also many occasions when you need to run the basic report types directly.

See also [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools, including how to develop new reports, queries, or trends using a provided or custom template.



Tips:

- No more than 5 reports can be run at the same time. The number of reports allowed to run simultaneously is a configurable parameter on the Manager in `ARCSIGHT_HOME/config/server.properties`.
- If you are having problems running a large or complex report, refer to the topic [“Setting Special Parameters for Running Large or Complex Reports” on page 270](#).
- If you are having problems running PDF reports with Asian fonts, see the topic [“Setup and Parameters to Generate PDF Reports with Asian Fonts” on page 271](#).

Running a New or Archived Report

When you run reports, you most often use an existing report definition, or a copy of a report already defined, run, and archived for later use. Defining new reports is a separate topic described in [Creating a Report](#). Please see also [“Archiving a Report” on page 294](#) and [“Scheduling Report Tasks” on page 297](#).



If you are having problems running a large or complex report, refer to the topic [Setting Special Parameters for Running Large or Complex Reports](#).

If you are having problems running PDF reports with Asian fonts, see the topic [“Setup and Parameters to Generate PDF Reports with Asian Fonts” on page 271](#).

Running a Defined Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 Click the **Reports** tab.
- 3 Navigate the Reports tree, and select the report you want to run.
- 4 Right-click the selected report to bring up the Context menu, and select **Run** with one of the report-type options described in Run-Report Options below.

Name	Value
Common Parameters	
Report Format	pdf
Page Size	Letter [8.5x11 in]
Email to	
Email Format	Send URL
Email Subject	\$ReportName
Row Limit	25

Name	Value
Output Parameters	
Archive Report Folder	Select a Archived Report Group
Archive Report Name	\${Today}/\${ReportName}_\${Now}
Archive Report Expiration Time	\$Now+6M

☒ Save Output

OK Cancel Help

- 5 Select **Save Output** if you want to save a copy of the report to disk.

If this option is selected, additional archive parameters are displayed. You can override any of these defaults also. You can select a group in which to archive the report, provide a report name, and specify an expiration time at which to discard the report from the archive. By default, the report is saved in the archive for 6 months from the time it was run.



You can use Velocity template references for fields that accept text, such as Archive Report Name and Archive Report Expiration Time. See [“Velocity References for Reports” on page 796](#) for details.

- 6 In the Report Parameters dialog box, enter new parameters if available and appropriate.
- 7 Click **OK**.
- 8 In the options dialog box click **Open** to open the report, **Save** to choose a location and format for the output file, or **Cancel** to quit. The Save option applies to all but HTML files.

Run-Report Options

To run a report, right-click on a report in the Navigation panel, select **Run** from the Context menu, and choose one of these report-type options.

Report Type	Description
Report	Run the report, but with the opportunity to edit its current parameters (if present). If you choose this option, the Report Parameters dialog is displayed before the report is run. You can override the default report parameters for just this run of the report.
Report with defaults	Run the report directly, using its defined parameters, if present. For focused reports, this is the only option.
Report with selected event	Run the report using as parameters the fields of an event selected in a Viewer panel grid view.
Delta report	For reports based on bar charts, run the report after selecting another report as the comparison for the delta.

Report Parameters

You can override the following default report parameters at the time you run a report. Other parameters are set when the report was created (as described in Report Parameters in [“Creating Reports” on page 251](#)).

Parameter	Use
Report format	<p>The format in which to generate the report. Note that HTML output now appears in the Web Viewer tabs of the Viewer panel rather than in a browser client. Further, RTF appears by default in Word documents, XLS in Excel worksheets, CSV in Excel worksheets, and PDF in browser windows. Please note that the CSV-Plain format intentionally has fewer report header lines.</p> <p>Note: Reports generated in CSV format are not the full equivalent of exports to other formats like PDF or HTML. CSV format is useful for loading report data into a spreadsheet for further manipulation. Since CSV is meant to contain tabular data, only the table data of a report is normally useful. Therefore, ArcSight ESM exports only the table data portion of a report to CSV format, ignoring any other report information such as charts or text, including report titles.</p>
Page size	Choose one of the available standard page sizes for the report.
Run as User	Optionally choose an existing ArcSight user's identity as a report constraint. The user identity can serve as a type of filter on the report's output, or it may be desirable to run a report on behalf of a user, as in a provider/customer (MSSP) circumstance. This capability is sometimes called "impersonation."
E-mail to	One or more e-mail addresses to send notifications to when the report runs. Separate multiple addresses with commas.
Email Format	<p>Specify whether to e-mail a link (URL) to the report or send it directly as an e-mail attachment.</p> <ul style="list-style-type: none"> If the report is large and is saved (archived) to a network-accessible location, you may want to select Send URL to point users to the report. If you want to send the report directly to the user's email box, select Attach Report.

Displaying an Archived Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 On the **Archives** tab, right-click a report and choose **Show Archive Report**.

Running a Delta Report

Delta reports show the difference between two sets of parameters, within a single comparative report. Defining new reports is a separate topic described in [Creating a Report](#). In order to run a delta report, you must have an existing report first. You can also set up a delta report to run and archive on a schedule. Please see also ["Archiving Reports" on page 294](#) and ["Scheduling Report Tasks" on page 297](#) for more information.

- 1 From the Navigator panel drop-down menu, select the **Reports** resource.
- 2 On the **Reports** tab, right-click a report and choose **Run**, then **Delta Report**.



The **Run Delta Reports** option is available only for reports with a bar, 3D bar, or inverted bar chart. The report must contain one chart only (no tables). The X and Y axis must have at least one column each, and no Z-axis. The chart must not have any summary function or top N filter applied. For more information about creating reports with these characteristics, see the ["Report Data" on page 257](#) section (under ["Creating Reports" on page 251](#)).

- 3 Select the parameters for the first report, select a report format from the drop-down menu, and click **OK**.
- 4 Select the parameters for the second report and click **OK**.
- 5 Select **Save Output** if you want to save a copy of the report to disk.

If this option is selected, additional archive parameters are displayed. You can override any of these defaults also. You can select a group in which to archive the report, provide a report name, and specify an expiration time at which to discard the report from the archive. By default, the report is saved in the archive for 6 months from the time it was run.



You can use Velocity template references for fields that accept text, such as Archive Report Name and Archive Report Expiration Time. See ["Velocity References for Reports" on page 796](#) for details.

The Report Viewer appears and displays the delta report. The report shows the difference between two sets of parameters used on a single report. The report also shows the data for each of the parameters.

When a delta report is run or archived, an internal event is sent to the ArcSight Manager. This event contains the following data fields and values:

Delta Report Event-data Field	Description
Event Name	Delta Report Generated (Report: <ReportName>), where <ReportName> is the name of the report.


Rules can be created using the delta report data fields.

Running Reports from a Grid View

You can define reports on-the-fly based on specific events in grid views in the Viewer panel.

Running a Rule-Context Report from a Grid View

- 1 In a grid view, select a correlation event.
- 2 Right-click it and choose **Report > Rule Context Report**.
- 3 In the **Report Parameters** dialog box, enter the time, in minutes, before and after this event's occurrence and click OK.
- 4 You can choose to Open or Save the report file.

In the grid view, a correlation event is marked with a **Flash** icon (). A report showing the correlation event and the events that triggered the rule appear.

Running an Event-Context Report from a Grid View

- 1 In a grid view, select an event.
- 2 Right-click and choose **Report > Event Context Report**.
- 3 In the **Report Parameters** dialog box, enter the time, in minutes, before and after this event's occurrence and click OK.
- 4 You can choose to Open or Save the report file.

The report shows the events that occurred, within the specified time before and after this event appears.

Running a Channel Report from a Grid View

- 1 In a grid view, select an event.
- 2 Right-click and choose **Report > Channel Report**.
- 3 The Report Parameters dialog is displayed, and its fields are automatically populated with the event data fields. You can enter new parameters to limit or extend the report.
- 4 Choose a Report File Format from the drop-down menu.
- 5 Click **OK**.
- 6 You can choose to Open or Save the report file.



The channel report exports all of the events in the channel into a report. A channel report refers to the whole channel, not the selected event. However, you do need to select an event in the grid view in order to "select" the channel and get the Report > Channel Report menu option.

Managing Reports

Managing reports includes editing existing reports, importing/exporting, and organizing reports into groups.

Editing a Report

Over time, reports often need to be adjusted to keep them appropriate and useful. For more information, see ["Creating Reports" on page 251](#).

- 1 Navigate to **Reports** in the Navigator panel, select the **Report** sub-tab, and select the report you want to modify.
- 2 Double-click the report, or right-click and select **Edit Report** from the context menu. This launches the Report Editor in the Inspect/Edit panel, and shows the definition for the selected report.
- 3 Edit the report definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)

Creating Focused Reports

In addition to using the reports already available in the Navigator panel's Reports resource tree, you can easily make and save refinements to these definitions. These more narrowly defined or focused reports are also stored in the resource tree, so other people can also use them.

Focused reports are identical to other reports. They differ only in being useful variations on already defined reports. You create focused reports when you want to make a special variation available to other ArcSight users through the Reports resource tree.

Creating a Focused Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 On the **Reports** tab, right-click a report and choose **New Focused Report**.
- 3 In the Focused Report Editor, select the **Attributes** tab and name the report. Name focused reports in a fashion that properly distinguishes them from their originals.
- 4 Click the **Parameters** tab and change any of the values as appropriate. These values are the same ones you set when Running a New or Archived Report.



You can use Velocity template references for parameter fields that accept text, as described in [“Velocity References for Reports” on page 796](#).

- 5 Click **Apply** to make changes and keep the editor open. Click **OK** to store the definition in the resource tree in the same folder as the original report and close the editor.



A focused report will reflect changes made to the report on which it is based.

Importing and Exporting Reports



To import and export reports, use the packages feature. Since the new reporting capabilities in ArcSight ESM version 4.0 involve using queries, trends, and templates as a part of building reports, the import/export tool must track and manage dependencies across resources. Packages gives you this capability. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. Please see the information on packages in [“Managing Packages” on page 491](#).

You can import or export reports by following these procedures.

Importing Reports

- 1 In the **Reports** resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report group where you want the imported report to be placed and select **Import Report**.
- 3 In the window, select a file to import to the report group.
- 4 Click **Open**.

Exporting Reports

- 1 In the Reports resource tree, select the **Report** tab.
- 2 On the Reports tab, right-click a report and select **Export Report**.
- 3 In the window, select the directory to save the report.
- 4 Click **Save**.

Moving or Copying a Report

You may need to move or duplicate report definitions to better organize your work, to publish your definitions, or to make editable copies of enterprise reports.

- 1 In the Reports resource tree, navigate to a report and drag and drop it into another group.
- 2 Select **Move** to move the report, **Copy** to make a separate copy of the report, or **Link** to create a copy of the report that is linked to the original report.

If you select **Copy**, you create a separate copy of the report that will not be affected when the original report is edited. If you select **Link**, you create a copy of the report that is linked to the original report. Therefore, if you edit a linked report, whether it be the original or the copy, all links are edited as well. When deleting linked reports, you can either delete the selected report or all linked report copies.

Managing Report Groups

Report groups store similar reports, and control access to reports, using access control lists (ACLs). When editing access control permissions, permissions given to a report group are also given to all groups and reports within that group.

Groups and reports can be managed with drag and drop functionality. You can move or copy groups and reports into other groups from the Reports resource tree. If a group is deleted, the reports within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Report Group

- 1 On the **Navigator Panel** drop-down menu, select **Reports**.
- 2 In the Reports resource tree, right-click a group and select **New Group**.
- 3 Enter a report group name in the "name" text field.
- 4 Press **Enter**.

Renaming a Report Group

- 1 In the Reports resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing a Report Group

- 1 In the Reports resource tree, right-click a group and select **Edit Group**.
- 2 In the Report Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying a Report Group

- 1 In the Reports resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Report Group

- 1 In the Reports resource tree, right-click a group and select **Delete Group**.
- 2 Click **Yes** in the dialog box.

Archiving Reports

You can schedule reports to archive automatically with the scheduler. The scheduler accepts multiple schedules by year, month, week, day, or hour. For example, a report can be archived automatically on the first of January at both 5 AM and 6 PM. The scheduler also sends e-mail notifications informing users when a scheduled report has been archived. Report Archiving is a component of ArcSight Reporting resource tools. Be sure to see [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools.

Archiving a Report

To archive a report, do the following:

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report and select **Schedule for Archiving > Report**. (This opens the report definition in the Editor with the **Jobs** tab showing.)

- 3 Click **Add** on the Jobs tab, and choose either **Schedule Report** or **Schedule Delta Report**.



The option to **Schedule a Delta Report** job is available only for certain types of event-based reports, and only when a previously-run report is available in the archives. Otherwise, clicking Add on the **Jobs** tab takes you directly to the job scheduler to schedule a standard report. For more information about Delta reports, see [“Running a Delta Report” on page 290](#).

- 4 Enter a name and description for the job.
- 5 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency** to get the Job Frequency dialog, and configure the schedule.

In the Job Parameters section, select or enter values for the parameter fields as necessary. For date parameters, enter values in the text fields, click the drop-down arrows or click the time buttons to select a time range. For time data, you can enter a specific value, such as 8:54:00 AM or you can use special timestamp variables.

Click **OK** to save changes to the Job schedule.

To view all scheduled jobs, click the **Open scheduled jobs list** tool button (🕒). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

For more information on setting up and viewing scheduled jobs, see [“Scheduling Jobs” on page 756](#) in the [Reference Guide](#).

- 6 Back in the report editor Jobs tab, under the **Job Parameters** section, enter values for the report parameters by clicking off the “Use Default” checkmarks, or change nothing here to keep the defaults. You can set the report format, email options, output

parameters, start and end times, and so on. These are the same parameters described in “Report Parameters” on page 289.

Inspect/Edit

Report: Top 10 Events

Attributes Template Data Parameters **Jobs** Notes

+ Add - Remove ↺ Frequency

Jobs	Description
Top 10 Events	Top 10 Events archive report

Next Run Time **8 Dec 2008 15:00:00 PST**

Job Parameters

Name	Value	Use Default
Common Parameters		
Report Format	html	<input checked="" type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input checked="" type="checkbox"/>
Run as User	Select a User	<input checked="" type="checkbox"/>
Email to		<input checked="" type="checkbox"/>
Email Format	Send URL	<input checked="" type="checkbox"/>
Email Subject	ReportName	<input checked="" type="checkbox"/>
Output Parameters		
Archive Report Folder	Select a Archived Report G...	<input checked="" type="checkbox"/>
Archive Report Name	{Today}/{ReportName}...	<input checked="" type="checkbox"/>
Archive Report Expir...	Now+6M	<input checked="" type="checkbox"/>
Custom Parameters		
StartTime	Now - 1d	<input checked="" type="checkbox"/>
EndTime	Now	<input checked="" type="checkbox"/>
Subtitle		
Text		<input checked="" type="checkbox"/>
Chart		
Time Zone	Manager Time Zone	<input checked="" type="checkbox"/>
Filter by	Select a Filter	<input checked="" type="checkbox"/>
Row Limit	10	<input checked="" type="checkbox"/>
Start Time	Now - 1d	<input checked="" type="checkbox"/>
End Time	Now	<input checked="" type="checkbox"/>
Title		
Text	Top 10 Events	<input checked="" type="checkbox"/>
ChartTitle		
Text		<input checked="" type="checkbox"/>

Summary

Occurs **Hourly**.

Schedule will start on **8 Dec 2008 14:05:24 PST**.

Preview... OK Cancel Apply Help

- 7 Click **Apply** or **OK** on the report Editor to save your changes for this report.

Parameterized Report Entries

The top portion of the dialog may or may not exist, depending on whether you chose any parameterized conditions while creating the report. A typical example of a parameterized condition is: detect time between `$CurrentDate-1d` and `$CurrentDate`. If such parameters exist, they will be used for both immediate as well as scheduled generation of reports. While scheduling reports for archiving, these parameters are displayed in the Edit Parameters dialog. It is possible to independently modify the dates specified in the parameter text fields. In addition to relative dates, absolute dates can be specified as parameter values. Examples of valid absolute dates are: `01/01/2001` and `01/01/2000 11:00:00 AM`.

Viewing an Archived Report

To view an archived report, select the **Reports** resource in the Navigator (if it is not already selected) and click the **Archives** tab. Navigate the Archived Reports tree to find the archived report you want, then right-click the report and choose **Show Archive Report**. The report is displayed in the Viewer.

If you do not find the report you are looking for, you might want to check to see if it has

run yet. To view all scheduled jobs, click the **Open scheduled jobs list** tool button (🕒). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

Scheduling Report Tasks

You can schedule some tasks to occur automatically. Specifically, this feature is available for archiving reports individually or by group, for taking pattern discovery snapshots, and for scheduling rules. This topic discusses the scheduler as it relates to scheduling reports (For more information on job scheduler in general, see also ["Scheduling Jobs" on page 756.](#))

Scheduling Individual-Report Archiving

- 1 Choose the Reports resource tree in the Navigator panel, select the **Reports** tab, and right-click the report you want to schedule.
- 2 Choose **Schedule for archiving**, then **Report** or **Delta Report** for delta reports. (This opens the report with the Jobs tab showing.)
- 3 Click **Add** the Jobs tab.

Inspect/Edit

Event Inspector \ Report:VPN Login Outcome Trend \

Attributes \ Template \ Data \ Parameters \ **Jobs** \ Notes \

+ Add ✕ Remove ↺ Frequency

Jobs	Description
Please Enter a Name	Please Enter a Description

Next Run Time --

Job Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input checked="" type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input checked="" type="checkbox"/>
Run as User	Select a User	<input checked="" type="checkbox"/>
Email to		<input checked="" type="checkbox"/>
Email Format	Send URL	<input checked="" type="checkbox"/>
Output Parameters		
Archive Report Fol...	Select a Archived Report ...	<input checked="" type="checkbox"/>
Archive Report Name	\${Today}/\${ReportName...}	<input checked="" type="checkbox"/>

Summary

[Click here to set up schedule frequency](#)

Preview... OK Cancel Apply Help

- 4 Enter a name and description for the job.
- 5 In the Job Parameters section, select or enter values for the parameter fields as necessary.
- 6 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency**.
- 7 Click the schedule-building buttons in sequence from left to right, as appropriate according to the definitions below, providing specific timing information.
- 8 Repeat Step 3 to add another schedule for the same group.
- 9 Click **OK**.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and appear differently. In addition, Excel format is more memory-intensive than PDF.

- 10 Select the **e-mail scheduled reports** to check box and a user from the drop-down menu to automatically send an e-mail notification when the report is archived.

The user receives an e-mail notification stating that the report has been successfully archived. The e-mail also contains a URL to the report so that the user can view the report from the URL. The e-mail notification is sent to the e-mail address listed in the user's profile. The user must have an e-mail address in their user profile.
- 11 For the **Archive Folder** text field, click the archive report group button to select where to list the archived report.
- 12 In the Archive Report Selector, select a report archive group and click **OK**.
- 13 In the Report Parameters window, click **Update**.
- 14 For delta reports, in the Schedule Summary, right-click **Default** under the **Param Set 2** column and select **Edit Parameters** to change the second parameter set, if any. Click **Update**.
- 15 In the Schedule Summary, click **Close**.



You can use Velocity template references for fields that accept text, such as Archive Folder and Archive Report Selector. See [“Velocity References for Reports” on page 796](#) for details.

Scheduling Report Archiving by Resource Group

- 1 In the Reports resource tree, navigate to a particular group.
- 2 Right-click the group and choose **Schedule for archiving>Report group**. (This opens the report with the **Jobs** tab showing.)
- 3 Click **Add** on the **Jobs** tab.
- 4 Enter a name and description for the job.
- 5 In the Job Parameters section, select or enter values for the parameter fields as necessary.
- 6 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency**.
- 7 Click the schedule-building buttons in sequence from left to right, as appropriate according to the definitions below, providing specific timing information.

- 8 Click **OK**.
- 9 Repeat Step 3 to add another schedule for the same group.

Table 12-1 Group Scheduling Buttons

Button	Usage
Type	Choose a timing scope for the archiving schedule. The typical choices are self-explanatory: hourly, daily, weekly, monthly, and yearly.
Month	For schedules that are yearly in scope, choose a month.
Date	For schedules that are yearly or monthly in scope, choose a date.
Day	For schedules that are weekly in scope, choose a day of the week.
Hour	For schedules that are daily or larger in scope, choose an hour of the day.
Min	For schedules that specify hours, optionally set the minute as well.
AM	Toggle between AM and PM for hourly schedules.

Editing a Report Archiving Schedule

You can change the archiving schedule for report definitions in your Reports resource folders.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report and select **Schedule for archiving**, then **Report** or **Delta Report** for delta reports.
- 3 In the Schedule Summary, right-click in the braces { } column and select the **Parameters** option to change report parameters set for the specific scheduled report. To delete a current scheduled archive report, right-click in the braces { } column of an existing schedule and click **Delete**.
- 4 To change the interval scheduling of a report, click the report interval button and **Yearly**, **Monthly**, **Weekly**, **Daily**, or **Hourly**, click the date and time buttons.
- 5 If editing within the same time frame, click the **Month**, **Date**, **Day**, **Hour**, **Min**, **AM/PM** buttons to specify changes to the report schedule.
- 6 When you've finished editing the schedule, click **OK**.

Editing Report Archiving Parameters

You can change the archiving parameters of the report definitions in your Reports resource folders.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Report Definitions tab, right-click a report and select **Schedule for archiving**, then **Report** or **Delta Report**.
- 3 Right-click in the braces { } column for a scheduled report and select the **Parameters** option.
- 4 In the Report Parameters window, type in the report parameter text fields, if any.

For date and time data fields, such as Detect Time, you can type an actual date value, such as `10/12/2002 8:54:00 AM`, or you can use special timestamp variables.

- 5 Select the **E-mail scheduled reports to** check box, and a user from the drop-down menu, to automatically send an e-mail notification when the report is generated.

The user receives an e-mail notification stating that the report has been successfully archived. The e-mail also contains a URL to the report so that the user can view the report from the URL.

The e-mail notification is sent to the e-mail address listed in the user's profile. The recipient must have an e-mail address in their user profile.

- 6 For the Archive Folder text field, click the archive report group button to select where to list the archived report.
- 7 In the Archive Report Selector, select a report archive group and click **OK**.
- 8 In the Report Parameters window, click **Update**.
- 9 For delta reports, in the Schedule Summary, right-click **Default** under the **Param Set 2** column and select **Edit Parameters** to change the second parameter set, if any. Click **Update**.
- 10 In the Schedule Summary, click **Close**.

Deleting a Report Archiving Schedule

You can remove individual archiving schedules for reports in the Scheduled Tasks list.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Report Definitions tab, right-click a scheduled report (showing a calendar icon) and choose **Schedule for archiving**, then **Report or Delta Report**.
- 3 On the line for the schedule to remove, right-click in the braces **{ }** column and choose **Delete**.
- 4 In the confirmation dialog box, click **Delete** to remove it or **Cancel** to let it remain.

Chapter 13

Rules Authoring

This section explains how to use rules to correlate events in your environment.

[“Choosing How Rules Work” on page 301](#)
[“Managing Rules” on page 302](#)
[“Managing Rule Groups” on page 303](#)
[“Specifying Rule Conditions” on page 304](#)
[“Specifying Rule Thresholds and Aggregation” on page 308](#)
[“Creating Rule Actions” on page 310](#)
[“Applying Rule Actions” on page 315](#)
[“Enabling and Disabling Rules” on page 317](#)
[“Importing and Exporting Rules” on page 319](#)
[“Scheduling Rules” on page 319](#)
[“Verifying Rule\(s\) with Events” on page 326](#)
[“Deploying Real-time Rules” on page 329](#)
[“Loading Rules” on page 330](#)

Choosing How Rules Work

When creating rules, you must define the rule events and conditions, thresholds, and actions you want the rule to contain. Conditions define which events trigger the rule, thresholds set when a correlation event is generated, and actions state what responses are taken when a correlation event is generated. To define rule events and conditions, thresholds, and actions, you might begin by determining:

- Which event occurrences do I want to be aware of? This determines the rule's **events** and **conditions**.
- How many times do I want the event or events to occur and within what time frame? This determines the rule's **threshold**.
- What actions should automatically occur when an event is generated? When should those actions occur? This determines the rule's **actions**.

Before you create rules, determine which events you want to monitor. Be specific and as clear as possible. For example, monitoring all events from a Cisco Router would not be as useful as monitoring all denied events from that Cisco Router. In addition, the more conditions you add to a rule, the more specific the rule becomes. Use the ArcSight data fields to guide you in selecting and specifying conditions. For more information, see [“Data Fields” on page 633](#).

Managing Rules

Like other resources, the rule-management tasks include creating, changing, deleting, and placing them.

Creating Rules

Before creating rules, determine which events you want to monitor. Be as specific and as clear as possible. For example, monitoring all events from a Cisco Router would not be as useful as monitoring all **denied** events from that Cisco Router. In addition, the more conditions you add to a rule, the more specific the rule becomes.

Use the ArcSight data fields to guide you in selecting and specifying conditions.

To create a rule:

- 1 From the Navigator Panel drop-down menu, select **Rules**.
- 2 Right-click a group and select **New Rule**.
- 3 On the General tab, type a name in the **Rule Name** text field.

The Rule Name should be as descriptive as possible. It is stored in the Event Name data field and if the rule has a Send to Console action, the Rule Name appears in the Event Name column of the grid view. The Rule Name text field is required and restricted to 25 characters.

- 4 Type a description in the **Description** text field.

The description should be meaningful and detailed. For example, This rule monitors all denied events from Cisco Routers. To define conditions, add correlating events, specify thresholds and time windows to qualify events and aggregate incoming event data based on matching fields, you can specify entries on the Conditions and Aggregation tabs. See [“Common Conditions Editor” on page 616](#), [“Specifying Rule Conditions” on page 304](#) and [“Specifying Rule Thresholds and Aggregation” on page 308](#) for more information.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

- 5 After defining the conditions and other elements of the rule, click **OK** to save and close the rule. You can also click **Apply** to save changes but keep the rule open.

Editing Rules

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **General** tab to edit the rule name and description.
- 3 Select the **Conditions** tab to edit events, logical operators, and condition statements as described in Common Condition Editor.
- 4 After editing the conditions and other elements of the rule, click **OK** to save and close the rule. You can also click **Apply** to save changes but keep the rule open.

Moving or Copying Rules

- 1 In the **Rules** view, navigate to a rule and drag and drop it into another group.
- 2 Select **Move** to move the rule, **Copy** to make a separate copy of the rule, or **Link** to create a copy of the rule that is linked to the original rule.

If you select **Copy**, you create a separate copy of the rule that will not be affected when the original rule is edited. If you select **Link**, you create a copy of the rule that is linked to the original rule. Therefore, if you edit a linked rule, whether it be the original or the copy, all links are edited as well. When deleting linked rules, you can either delete the selected rule or all linked rule copies.

Deleting Rules

- 1 In the **Rules** resource tree of the Navigator panel, right-click a rule and choose **Delete Rule**.
- 2 Click **Yes** in the confirmation dialog box.

Managing Rule Groups

Rule groups are created to store similar groups or rules in a single location. Groups can be created within groups to meet enterprise needs.

Groups and rules can be managed with drag and drop functionality. You can move or copy groups and rules into other groups from the Navigator panel's Rules resource tree. If a group is deleted, the rules within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating Rule Groups

- 1 In the Navigator panel's drop-down menu, choose **Rules**.
- 2 In the Rules resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 Type a name in the "name" text field.
- 4 Press **Enter**.

Renaming Rule Groups

- 1 In the Rules resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing Rule Groups

- 1 In the Rules resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.

- 3 Optionally, you can designate owners of a rule, and specify user groups that will be notified of rules changes.
- 4 Click **OK**.

Moving or Copying Rule Groups

- 1 In the **Rules** resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting Rule Groups

- 1 In the **Rules** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Specifying Rule Conditions

After creating a new rule, or opening an existing rule for editing, you can specify conditions on which a rule will trigger, based on specific event, filter, asset, or vulnerability criteria. Like other ArcSight analysis components, rules editing uses the [Common Conditions Editor](#).

Creating New Rule Conditions

- 1 In the Rules Editor, select the **Conditions** tab.
- 2 To edit the event name (its alias), right-click **event1** and select **Edit** or select **event1** and press **Enter**. Type a new name in the text field and click **OK**.

Since rules can have numerous events, event names should be unique and descriptive. For example, if monitoring Cisco Router denied events, **Cisco Router denied** could be the event name. The event name appears as a branch under the **Correlate** tree.

- 3 In the rule's property table, scroll to an attribute to create a condition statement. To learn more about these attributes, see ["Data Fields" on page 633](#). See ["Common Conditions Editor" on page 616](#) for all the usage rules and features of this editor.
- 4 On the Conditions tab, click **Apply**.

A single-event, single-condition rule with the default threshold and action is created and listed in the Rules resource tree.

To add more events, select **Correlate** and click the **Event Definition** button, or right-click **Correlate** and choose **New Event Definition**. Type an event name in the **Alias** text field and click **OK**. When adding events, a **Matching Event** branch appears. For more information on joining two events, see ["Creating Matching or Join Conditions" on page 306](#). Other important references are Logical Operators and Conditional Expressions.

See the **Aggregation Time Criteria** in ["Specifying Rule Thresholds and Aggregation" on page 308](#) for aggregation time-frame options.

Adding Filter Conditions to Rules

You add filters to rules as new conditions. It is usually more desirable to use an existing filter resource, if possible.

If there are other conditions in the rule, you choose whether to tie them to the filter condition with AND, OR, or NOT logical operators. For more information on filters, see [“Managing Filters” on page 480](#).

To add a filter condition to a rule:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Click the **And**, **Or**, or **Not** button or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.
- 4 Right-click the logical operator and select **New matchesFilter**.
- 5 In the Filter Selector, select a filter and click **OK**.
- 6 On the Conditions tab, click **OK**.

The Common Condition Editor's buttons and commands are discussed further in [“Creating Filters” on page 147](#).

Adding Asset Conditions to Rules

Asset conditions state whether your enterprise assets are targets or sources of events. An asset condition states “if an event occurs and the selected asset is the source or target, generate a correlation event”. For more information on assets, see [“Modeling Your Network and Managing Assets” on page 456](#).

To add an asset condition to a rule:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Click the **And**, **Or**, or **Not** button, or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.

If there are existing conditions, you can tie them to the asset condition with either the AND, OR, or NOT logic operator. If AND is used, all the existing conditions and the asset condition must occur in the event. If OR is used, either the existing conditions or the asset condition must occur. If NOT is used, all but the asset condition must occur.

- 4 Select the logical operator and click the Assets button or right-click the logical operator and select **New Assets Condition**.
- 5 In the Assets panel below, select **Source Asset ID** to monitor if an asset is the source of an event or **Target Asset ID** to monitor if an asset is the target.
- 6 Select an asset or group and click **Apply**.

The asset condition appears in the Correlate section and is tied to any existing condition statements with the logic operator selected.

- 7 On the Conditions tab, click **OK**.

Adding Vulnerability Conditions to Rules

You can use an existing enterprise vulnerability to create a rule condition. A vulnerability condition states "if an event occurs with the vulnerability selected, generate a correlation event". For more information on vulnerabilities, see ["Modeling Your Network and Managing Assets" on page 456](#).

To add a vulnerability condition to a rule:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Click the **And**, **Or**, or **Not** button or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.

If there are existing conditions, you can tie them to the vulnerability condition with either the AND, OR, or NOT logic operator. If AND is used, all the existing conditions and the vulnerability condition must occur in the event. If OR is used, either the existing conditions or the vulnerability condition must occur. If NOT is used, all but the vulnerability condition must occur.
- 4 Choose the logical operator and click the **Has Vulnerability** button or right-click the logical operator and choose **New Has Vulnerability**.
- 5 In the **Vulnerability Selector**, select a vulnerability and click **OK**.

The vulnerability appears on the Conditions tab and is tied to any existing condition statements with the logic operator selected.
- 6 On the Conditions tab, click **OK**.

Negating Event Conditions

Rather than specifying event conditions to monitor, you can specify which event conditions **not** to monitor by negating them. When event conditions are negated, all but the selected event conditions are monitored. Prior to using the following procedures, event conditions must exist for you to negate. To create event conditions, see ["Creating Rules" on page 302](#).

To negate event conditions:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Right-click an event and select **Negated**.
- 4 The existing event conditions are negated and all but those event conditions will be monitored.

For example, if existing event conditions state `((ConditionOne or ConditionTwo) and in FilterOne)` and it is negated, all events but `ConditionOne` in `FilterOne` or `ConditionTwo` in `FilterOne` will be monitored. A checkmark appears next to the right-click option when the event conditions are negated.

Creating Matching or Join Conditions

A matching or join condition is a condition statement that joins two data fields with the Matching or Join condition logic operator on the Conditions tab. Creating matching or join conditions using data fields provides the flexibility of creating conditions without knowing the specific data field's values. The following join data field conditions can be created:

- Same data field for two events: `EventOne <data field A> <logic operator> EventTwo <data field A>`. For example, `EventOne Source Address = EventTwo Source Address`. In this example, both event data field must have the same value. This rule is useful when monitoring activity from an unknown Source Address that is generating numerous events.
- Different data fields for two events: `EventOne <data field A> <logic operator> EventTwo <data field B>`. For example, `EventOne Source Address = EventTwo Target Address`. In this example, the Source Address of the first event must equal the Target Address of the second event.
- Different data fields for the same event: `EventOne <data field A> <logic operator> EventOne <data field B>`. For example, `EventOne Source Address = EventOne Target Address`. In this example, the Source Address must equal the Target Address of the same event.



There is a relatively high memory cost for join rules with low-selectivity join conditions (such as same source IP or same target IP). Just like queries in SQL, the more selective the conditions (the conditions on the individual events as well as the join conditions), the less expensive it is to execute, because fewer conditions will match.

When authoring a rule you should order conditions on the events to be correlated (or joined) by placing the most restrictive conditions first; for example, adding join conditions like `event1's Source Address = event2's Source Address` or `event2's Detect Time = event1's Detect Time`. This will dramatically reduce the memory consumption by the Correlation Engine, as much as 50% in some cases.

The following procedure can only be used with rules that involve two or more events.

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Select the **Matching Event** branch and select **New Logical Operator**, then **And**, **Or**, or **Not**.

When adding join conditions, you need to decide how the new condition ties to the existing events in the rule. If AND is used, the new join condition must occur, in addition to the existing events, to trigger the rule. If OR is used, the new join condition or the existing events must occur. If NOT is used, all but the new join condition must occur. The logical operator appears as a branch under Joins.

- 4 Click the **Join Condition** button or right-click the logical operator and select **New Join Condition**.

A condition statement appears displaying event, data field, and logic operator text fields. These fields are combined to create `<event> <data field> <logic operator> <event> <data field>` condition statements. For example, if monitoring for the same Source Address data field in EventOne and EventTwo, the condition statement would be `EventOne Source Address = EventTwo Source Address`.

- 5 Select one of the following join data field conditions to use in the following steps:
 - ◆ When monitoring for the same data fields for two events use `EventOne <data field A> <logic operator> EventTwo <data field A>`.
 - ◆ When monitoring for different data fields for two events use `EventOne <data field A> <logic operator> EventTwo <data field B>`.
 - ◆ When monitoring for different data fields for the same event use `EventOne <data field A> <logic operator> EventOne <data field B>`.

- 6 In the text fields, choose an event and data field from the drop-down menus.
Select data fields that you want to monitor but for which you don't have values. For more information, see ["Data Fields" on page 633](#).
- 7 Choose a logic operator from the drop-down menu.
- 8 Choose an event and data field from the drop-down menus.
- 9 Click **OK**.
The join data field condition appears as a branch under the Matching Event logical operator.
- 10 On the Conditions tab, click **OK**.

Editing or Deleting Join Data Field Conditions

- 1 In the Rules resource tree, right-click a rule and select **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab and do the following:
 - ◆ To edit the logical operator, right-click the logical operator and select **Edit** or select the logical operator and press **Enter**. In the text field, select a logical operator and click **OK**.
 - ◆ To edit the condition statement, right-click the condition statement and select **Edit** or select the condition statement and press **Enter**. In the text field, make edits and click **OK**. For more information, see ["Creating Rules" on page 302](#).
 - ◆ To delete the Matching Event event, right-click **Matching Event** and select **Delete**. In the dialog box, click **Yes**. The event, its logical operators, and condition statements are deleted.
 - ◆ To delete the logical operator, right-click the logical operator and select **Delete**. In the dialog box, click **Yes**. The logical operator and all its condition statements are deleted.
 - ◆ To delete the condition statement, right-click the condition statement and select **Delete**. In the dialog box, click **Yes**.
- 3 Click **OK**.

Specifying Rule Thresholds and Aggregation

Thresholds are defined as an aggregate number of occurrences within a time span. When a threshold is met, the rule triggers.

Setting or Changing Rule Thresholds

- 1 In the Rules Editor, select the **Aggregation** tab.
- 2 In the Aggregation tab, enter a number (greater than 1) in the **Number of Matches** field.
- 3 In the **Time Frame** field, enter an appropriate value and choose a time unit.

- 4 If you want to aggregate on the basis of certain fields' content being distinct, check **Aggregate only if these fields are unique** and click **Add** to select the fields to use.



Fields are *unique* only when the combined value of all fields is unique. For example, suppose you wanted to aggregate on three fields: Event Name, Event Message, and Category Outcome, with a threshold of two matches. If you got two events both with values of **Failed Login**, **Attempt**, and **Failure** for these fields, respectively, these events would be aggregated.

However, if you got only one event like this, and another with values of **Failed Login**, **Attempt**, and **Success**, these two events would not be aggregated because the combined value is not the same for the given threshold number of events.

- 5 If you want to aggregate on the basis of certain fields' content being identical, check **Aggregate only if these fields are identical** and click **Add** to select the fields to use.
- 6 Click **OK**.

The choices you make are expressed as a conditional statement in the **Summary** panel below.

Aggregation Time Criteria

In all, there are actually four time-evaluation criteria that can affect event-occurrence aggregation and rule-triggering. You apply these to rules through the Aggregation tab and the statement panel of the Conditions tab.

Criteria	Application
Time Frame	Set on the Aggregation tab, Time Frame establishes the time span for occurrence aggregation. Event-occurrence aggregation is always controlled by Time Frame. Secondly, Time Frame becomes the default for global and alias expiration time, if these are not set separately.
Global Expiration	Set on the Conditions tab, a global expiration applies to an entire rule. This is the amount of time that qualifying events for all aliases will be retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. To set Global Expiration, right-click the rule's root node (Correlate) in the Conditions tab and choose Set Global Expiration Time .
Alias Expiration	Set on the Conditions tab, an alias expiration applies to a single alias within a rule. This is the amount of time that a qualifying event for this alias (only) will be retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. To set Alias Expiration, right-click an alias in the Conditions tab and choose Set Alias Expiration Time .
Matching Time	Set on the Conditions tab, a matching time creates a time-proximity comparison for multiple-alias rules, based on events' actual creation times. When two or more rule-condition aliases are present, a Matching Event node appears. You can right-click this node and choose Set Matching Time to require events' original timestamps (specifically, the event's original end-time) to fall within a range. Note that this time-proximity test is independent of and different than the memory-retention parameter set by global or alias expiration.

Deleting Aggregation from a Rule

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Aggregation** tab.
- 3 In the **Aggregate only if these fields are unique** or **Aggregate only if these fields are identical** lists select the fields to delete and click **Remove**.
- 4 Click **OK**.

Creating Rule Actions

The Actions tab of the Rules Editor offers a consistent interface for defining actions to take based on the thresholds of the events that trigger them.

In the Actions tab, you click the buttons in the top row to Add, Edit, or Remove event-action sets for rules. Click **Hide Empty Triggers** to hide or show triggers not currently used.



Rules, rule triggers, and rule actions can be enabled or disabled at various levels. The rule itself can be enabled or disabled, the trigger on a particular rule can be activated or deactivated, and a rule action associated with a particular trigger can be enabled or disabled. Details on rule triggers and rule actions are described in this topic. For more information and a summary, see also [“Enabling and Disabling Rules” on page 317](#).

In the **Rules “Actions”** tab, you can define actions to take based on thresholds of the events that triggered them. In this example, “On First Event” is a trigger which is currently activated. The user has configured an action associated with this trigger to add events to the specified active list.

The Add list is expanded here to show all the actions you can configure for each trigger.

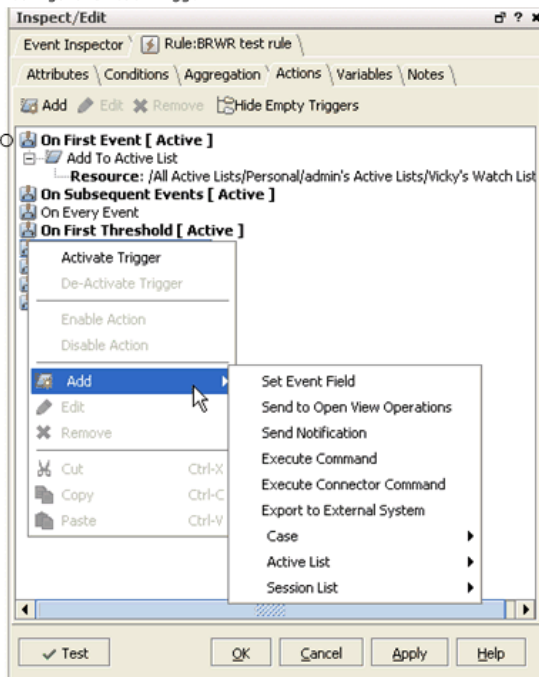


Figure 13-1 Creating Rule Actions

Adding a Rule Action

You add rule actions by choosing an event threshold trigger, clicking **Add**, choosing an action, then setting the action's parameters.

To add a rule action:

- 1 Choose **File>New>Rule** from the Console menu bar.
- 2 In the Rules Editor, click the **Actions** tab.
- 3 Select an applicable threshold trigger.
- 4 Click **Add**, then choose an action from the menu.
- 5 In the **Add Action** dialog box, set the action's parameters, if present.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See ["Velocity Templates" on page 793.](#))

- 6 Right-click the trigger and choose **Activate Trigger** to generate a descriptive event each time this rule action occurs. A rule must have at least one active trigger.
- 7 Click **OK** to add the new action to the rule's threshold trigger.



Always add actions in the order in which you want them to be executed. For example, to set a static value in an active list with values, first add the action to Set Event Field, then add the action to Add to Active List.

Please note that in the current release, the Editor display does not always match the internal representation of the specified order of rule actions. However, if you add rule actions in the proper order, that order is maintained internally.

Actions added to a rule show up the first time in the order you add them. You can continue to modify these and they will show up in this order. After you click Apply the display reorders the actions so that "Add to Active List" shows up first even though the internal representation has not been modified. Even so, rule actions will continue to work as expected unless you change the order. For example, if you delete the Set Event Field action then add it back in after Add to Active List action is already configured, the rule actions will be mis-ordered and will not be triggered as expected.

Editing a Rule Action

You edit rule actions by choosing an event threshold trigger, clicking **Edit**, then changing the action's parameters.

To edit a rule action:

- 1 In the Navigator panel, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, click the **Action** tab.
- 3 Select an action below a threshold trigger.
- 4 Click **Edit** to open that action's Add Action dialog box.

- 5 Change the action's parameters as appropriate.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See [“Velocity Templates” on page 793.](#))

- 6 Optionally, right-click the trigger and choose **De-activate Trigger** to stop generating a descriptive event each time this rule action occurs.
- 7 Click **OK** to record the changes.

Remove a Rule Action

To remove a rule action, select an action below a trigger in the **Actions** tab and click **Remove**.

Activating or De-activating a Rule Trigger

When a trigger is activated, all enabled rule actions it contains will be triggered when conditions are met.

- To activate a rule trigger, select the trigger in the **Actions** tab and click **Activate Trigger**.
- To de-activate a rule trigger, select the trigger in the **Actions** tab and click **De-Activate Trigger**.

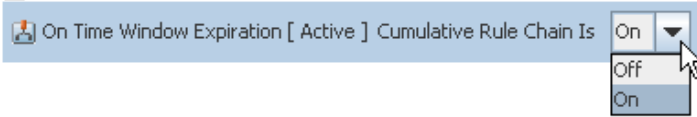
Enabling or Disabling a Rule Action

For finer-grained control over which rules are triggered when, you can enable or disable a rule action associated with any of the triggers.

- To disable an action, select an action below a trigger in the **Actions** tab and click **Disable**.
- To enable an action, select an action below a trigger in the **Actions** tab and click **Enable**.

Threshold Triggering Options

Trigger	Threshold
On First Event	The first time rule conditions are met, overriding aggregation threshold settings.
On Subsequent Events	The second and subsequent times rule conditions are met (not the first), overriding aggregation threshold settings.
On Every Event	Every time rule conditions are met, overriding aggregation threshold settings.

Trigger	Threshold
On Time Unit	<p>Defines an action to take if the given threshold is met in the specified number of minutes specified. (When: On Time Unit: Every <NumberOfMinutes>).</p> <p>This setting can be configured to work in conjunction with aggregation to limit the number of times a rule is triggered. For example, if aggregation is set to 2 matches in 1 minute and you get 50 matches in 1 minute (depending on how you set the rule actions). If you then specify the rule to trigger "On Time Unit" of, for example, 1 minute, then even if there were 50 matches in 1 minute, the rule would only trigger once per minute when the aggregation threshold is met.</p> <p>Note: Activating this trigger does not imply that a rule will be triggered on first event, on subsequent events, or on every event that meets conditions. This specifically sets the rule to trigger per the given time unit <i>if</i> aggregation thresholds are met.</p>
On Time Window Expiration	<p>When the threshold settings have expired.</p> <p>Note: When the On Time Window Expiration (TWE) trigger is activated, it includes an option to display a cumulative rule chain (a summary of triggered rules) at the end of the triggered rules list.</p> <p>To toggle the cumulative rule chain option on or off:</p> <ol style="list-style-type: none"> 1 Click the Rule Editor Actions tab for a selected rule 2 Right click an <i>active</i> On Time Window Expiration trigger and select On or Off as needed.  <p>(To activate or de-activate a trigger, right-click the trigger and select options to activate or de-activate it.)</p> <p>When a the TWE trigger activates a rule, a Correlation Event is generated. If the cumulative rule chain option is <i>on</i>, the correlation event will contain all the base events from the first threshold to the TWE.</p> <p>If the cumulative rule chain option is <i>off</i>, the generated correlation event will contain events from the last threshold to the TWE.</p>

The following options appear if more than 1 Matching Events are specified in the threshold settings:

Trigger	Threshold
On First Threshold	The first time rule conditions and threshold settings are met.
On Subsequent Thresholds	The second and subsequent times rule conditions and threshold setting are met, not the first.
On Every Threshold	Every time rule conditions and threshold settings are met.



Triggering actions on every or subsequent occurrence can quickly use up resources. Use these options conservatively.

Rule Actions

Action	Parameters
Set Event Field	Fills in a data field value for correlation events generated by the rule. You specify the data field and the value to place in the field. If the correlation event already has a value for the selected data field, that value will be overridden with this rule action.
Send to Open View Operations	Communicates the triggered rule's associated events to a specialized ArcSight SmartConnector that resides with the Manager, which in turn forwards the information to an H-P Open View Operations installation for management purposes. This applies only in those environments where Open View has specifically been integrated with ArcSight. Request the ArcSight Tech Note concerning H-P Open View Ops for more information.
Send Notification	Sends e-mail, pager, or cell phone messages to ArcSight users when rules are triggered. This rule action can send an informative message or can begin an escalation chain that requires an acknowledgment from a user. For more information, see "Managing Notifications" on page 482 . Deselect the Ack Required check box to make this notification informative, rather than use the default which begins an escalation chain. Informative notifications go to all destinations in a notification group. They don't need acknowledgement. When Ack Required is selected, notifications require acknowledgement.
Execute Command	Execute a command line function when the rule is triggered. The command line function and its parameters can be executed immediately or sent to the ArcSight Console prior to execution. At the ArcSight Console, you can decide whether to execute or clear the rule action during real-time monitoring. For example, type /bin/ping in the Command text field and type an IP address in the Parameters text field. For the Action Type, Automatically Run on Manager executes the command at the ArcSight Manager without further intervention; Run on Manager with Console Confirmation requires an operator at a Console to approve the command before it executes; Run on Connectors directs the command at applicable SmartConnectors.
Execute Connector Command	Execute a SmartConnector command that is applicable to the device it monitors. This is also known as the CounterACT feature. Notes: Only certain SmartConnectors can process commands beyond the basic set that all SmartConnectors support (e.g., start , stop , pause , continue , and terminate). These SmartConnectors tend to be those for hardware devices that are more complex and configurable. Consult your ArcSight administrator or representative for more information. This feature is comparable to the capabilities described in "Sending Control Commands to SmartConnectors" on page 517 .
Export to External System	Sends the rule and the triggering events to an external system that is integrated with ArcSight. The export is in the form of XML on the ArcSight Manager's archive/exports directory.

Action	Parameters
Create New Case	Create a new case that includes the events that triggered the rule. The maximum number of rule-associated events a case can hold is 100. If this limit is reached, the Console sends a warning message and disables the action until the number of cases drops below the maximum.
Add to Existing Case	Add the associated events to an already defined case. The maximum number of rule-associated events a case can hold is 100. If this limit is reached, the Console sends a warning message and disables the action until the number of cases drops below the maximum.
Add to Active List	Add the associated events to an existing active list that you select. Also select two tracking fields, a source and a destination.
Remove from Active List	Remove the associated events from an existing active list that you select. Also select two tracking fields, a source and a destination.
Active List	The Actions tab in the ArcSight Discovery Profile Editor includes the option to add an event to, or remove an event from, an active list when the trigger occurs.
Add to Session List	Add the associated events to an existing session list that you select.
Terminate Session List	Add the associated events to the selected session list and end the session list.

Applying Rule Actions

Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met. You can choose to be notified of a triggered rule at the ArcSight Console or through the Notifier, have information about the events that triggered the rule sent to a case or an active list, or automatically execute a command-line function. You can also assign more than one rule action to any rule.

More Rule Actions

Some additional actions you can specify for a rule include the following.

- **Add To Active List** - When triggered, adds the qualifying item to the active list.
- **Remove From Active List** - When triggered, clears the qualifying item from the active list.
- [Defining a New Rule Action](#)

Add To Active List and **Remove From Active List** either take no arguments (if acting on an event-bound active list) or a list of event fields (if **not** dealing with an event-bound active list). The values from the specified fields (those specified either by an event-bound active list or by the argument list) form an item that is added to, or removed from, the active list. Removing an item that is not present does not cause an exception. Adding an item that is already present simply increments that item's counter. You can see this counter in the Active Lists Editor. (See ["Active Lists" on page 574](#) and ["Managing Active Lists" on page 385](#) for more information.)

- **Add to Existing Case:** Adds to a case all the events that have triggered the rule. When the rule is triggered, all events associated with the rule are sent to a case for further investigation. The maximum number of rule-associated events a case can hold is 100.

When this limit is reached, a warning message goes to the ArcSight Console. The Add to Case action deactivates and further events are not sent to the case. When the number of events in the case reduces, the Add to Case action re-activates, and it resumes sending events to the case.

- **Create New Case:** Creates a new case and adds all events that have triggered the rule to the case. When the rule triggers, all events associated with the rule are sent to a case for further investigation. The maximum number of rule-associated events a case can hold is 100.

Once this limit is reached, a warning message is sent to the ArcSight Console and the Create New Case action deactivates and further events are not sent to the case. When the number of events in the case reduces, the Create New Case action reactivates, and it resumes sending events to the case.

- **Execute Command:** Executes a command-line function when the rule triggers. The command-line function can be executed immediately or sent to the ArcSight Console prior to execution. For example, you could specify an action to perform the bin/ping command on a specific IP address.

In the ArcSight Console, you can decide whether to execute or clear the rule action during real-time monitoring.

- **Export to External System:** Sends the rule and the triggering events to an external system that is integrated with ArcSight. The export is in the form of XML, in the ArcSight Manager's archive/exports directory.
- **Send to Console:** Sends a correlation event to the ArcSight Console when the rule triggers. A correlation event is generated by a rule when its conditions and threshold settings are met. The Send to Console rule action should always be used. Setting this action displays the "flash" triggered-rule event on the Console.
- **Send to Notifier:** Sends e-mail, pager, or cell phone messages to ArcSight users when rules are triggered. The Send to Notifier rule action can send an informative message or can begin an escalation chain that requires an acknowledgment from a user. Informative notifications are sent to all destinations in a notification group to relay a message. They do not need to be acknowledged. If the **Ack Required** check box is selected, the notification must be acknowledged. For more information, see ["Managing Notifications" on page 482](#).

Defining a New Rule Action

To define a new rule action, select the **Actions** tab of the rule you're creating or editing. Then right-click in the Actions tab display and choose **New**. The Console now displays a list of options for each of the action types you may want to add, for example, **Set Event Field** or **Severity**, **Send to Notifier**, **Execute Command**, **Add to Active List**, **Create New Case**, etc.

To generate a correlation event the rule is triggered. You can specify a Set Event Field rule action. This rule action fills in a data field value for correlation events generated by the rule. You specify the data field and the value to place in that field. If the correlation event already has a value for the data field selected, that value will be overridden with this rule action.

See ["Creating Rule Actions" on page 310](#) for more information on defining rule actions and associated triggers.


Enabling and Disabling Rules

You can enable (set to on) or disable (set to off) rules. Rules can also be automatically disabled by ArcSight ESM.




Keep in mind that only rules deployed in Real-time Rules show up in a live channel when they are triggered. Therefore, once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules as described in Deploying Real-time Rules.


Enabling Rules

In the **Navigator** panel's **Rules** resource tree, right-click the rule and choose **Enable Rule**. The rule will be displayed as enabled or on () in the Navigator.


Disabling Rules


In the **Rules** resource tree, right-click a rule and choose **Disable Rule**. The rule will be displayed as disabled or off () in the Navigator.

Automatically and Manually Disabled Rules

If a rule is **disabled** or off () , the rule is grayed out on the **Navigator** panel in the Rules resource tree.

A rule can be manually disabled by an administrator or automatically disabled by the ArcSight ESM system. A rule will be disabled by the ArcSight ESM system for either of the following reasons. When a rule is automatically disabled, ESM generates an audit event indicating that this happened so that administrators can follow up as needed.

Cause for Automatically Disabled Rule	Description
Rule is invalid	<p>An invalid rule will be automatically disabled and displayed as broken () in the Navigator.</p> <p>If an administrator configures a rule or related resource in a way that "breaks" the rule and leaves it in an invalid state, the system will automatically disable the rule.</p> <p>If a rule is disabled automatically due to an invalid configuration, an "Invalid Reason" is displayed in the Rule Editor on the Inspect/Edit panel. When the rule is reconfigured to a valid state and enabled, the "Invalid Reason" field is no longer displayed.</p> <p>The "Invalid Reason" field is not displayed for rules that are manually disabled.</p>

Cause for Automatically Disabled Rule	Description
Rule is recursive	<p>Starting with ESM v.4.5, rules that trigger themselves in a recursive loop will be automatically disabled <i>temporarily</i>. A rule that is automatically disabled due to recursion will be re-activated after a time frame that matches the aggregation time frame for the rule. (The default aggregation time frame is 2 minutes.)</p> <p>A rule can be inherently recursive due to a flaw in its design, or temporarily recursive because of some particular events involved. In the first case, temporarily disabling the rule often clears out the problem, and allows the rule to run normally when it is re-activated.</p> <p>If the rule is inherently recursive, ESM will continue to re-enable and then auto-disable it. The solution in this case is to redefine the rule logic and redeploy it, since it is effectively a “broken” rule.</p>
Number of rule triggers exceeds configured limits	<p>Number of rule triggers exceeds configured limits A rule that exceeds configured limits will show as disabled () in the Navigator, and offer a right-click option for the user to manually disable it permanently.</p> <p>The ESM system will disable a rule if the rule exceeds the configured limits on number of rules triggered per minute or ratio of base events to triggered rules, as defined in ARCSIGHT_HOME/config/server.defaults.properties file on the Manager.</p> <p>A rule in this state will continue to attempt to run until the user disables it permanently by right-clicking on it in the Navigator and choosing Disable.</p>

For rules that are disabled automatically by ArcSight ESM, a right-click on the disabled rule in the **Navigator** will provide a manual **Disable** option so that users can permanently disable the rule until it is fixed. (If these rules are not manually disabled, they will make continued attempts to run and get intermittently enabled/disabled by the system. This can impact system performance.)

Disabling Rule Components

You can also disable certain components of a rule, such as particular rule triggers or a rule actions associated with particular triggers. For information on this, see [“Activating or Deactivating a Rule Trigger” on page 312](#) and [“Enabling or Disabling a Rule Action” on page 312](#) (in [“Creating Rule Actions” on page 310](#)).

Importing and Exporting Rules

Rules are created in a readable XML format. You can export a rule or rule group to an external file to modify it. After modification, you can import it back into the ArcSight Manager.



To import and export rules, use the packages feature. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. Please see the information on packages in [“Managing Packages” on page 491](#).

Scheduling Rules

You can schedule rules to run at a specified time interval (such as hourly, daily, or monthly).

Scheduled Rules are a useful alternative to real-time rules in situations where you want to deploy rules that take into account historical data along with live data, or when you simply want to control when the rules are run. The scheduled rules engine can process historical data, take real actions, and generate correlated events which are the same as those generated by the real-time rules engine.

Scenarios for Using Scheduled Rules

- **Batched Events.** In many environments, certain types of events are not immediately available to the ArcSight ESM Manager, but instead are sent in batches infrequently; sometimes once a day, or once a week. Such events will have different Manager receipt times and end times. Manager receipt times will be current (when the batches are submitted), but the event end times will be in the past, since the events actually happened in past. Common examples of events that are sent in batches are those involving physical security devices and represent individuals gaining entry to buildings or offices by means of badge readers and card keys. Since these events (like an employee entering an office) arrive late to the ArcSight ESM Manager, they cannot be effectively correlated with other events (like a user login) by typically deployed rules that use the real-time rules engine. When the real-time rules engine receives login events, it waits for 1 minute (or whatever the time window for this rule is) and then throws out the login event, since the other event did not arrive within rule's time window. Suppose you have a rule that looks for a badge swipe event and a login event within 1 minute of each other (aggregates on 1 minute). The login events are received by the Manager real time as they occur. But the badge swipe events are collected and submitted only once a day at 10pm. A real time rule would not correlate the two events because it would throw out the login event before it ever gets the batched event. But if you scheduled your rule to run at midnight with the scheduled rules engine, it could correlate the actual end times of batched events and login events that occur within 1 minute of each other. Scheduled rules can correlate these types of events because (a) rules can be scheduled to run when both the login and batched events are available within the ArcSight ESM database and (b) although manager receipt times for these events would be different, their end times are close together within the aggregation window. Correlations are based on end times of events.
- **Historical Data.** You may want to capture and correlate other kinds of historical data (other than batched events). For example, if you have observed a pattern of events over the last several weeks, decide to write rules to take actions on some of those events, and correlate not only future occurrences of them but also the past events. This is possible to do by scheduling rules to run on events with end times in the past.

- **Optimized Rule Schedules.** Another scenario in which you might want to use scheduled rules is for rules that are more appropriate to run after business hours (for example, in the middle of the night). The job scheduler on rule groups lets you specify the appropriate schedule, and the rules are deployed as correlated events but are executed on off-hours.

In all such cases, scheduled rules will generate correlation events and take real actions when triggered, just like deployed real-time rules.



Although scheduled rules that correlate batched events work in part with historical data, these are deployed rules (not tests) that take actions as appropriate and do affect the live system.

Scheduling a Rule Group

- 1 Click the **Rules** resources on the Navigator.
- 2 Identify the rule(s) you want to schedule. (For information on how to create new rules, see ["Managing Rules" on page 302.](#))
- 3 If these rules are not already in a rule group, create a new rule group and link or move rules into it. (For information on how to create and work with rule groups, see ["Managing Rule Groups" on page 303.](#))
- 4 Select a rule group, right-click, and choose **Edit Rule Group** from the context menu.
- 5 Click **Jobs** in the Rule Group editor.
- 6 Add a job, name and describe it, and specify a schedule on which to run the rule group.

- 7 Specify a filter for these rules. (By default the filter is set to All Events. Click on **Filter Results by** to refine the filter to display only events relevant to the rule. Narrowing the filter will optimize performance when the rule is run.)

Double-click to modify the default job name and description, or click **Add** to add a new scheduled job.

Click the **Hourly** link in the Summary to bring up the Job Frequency dialog where you define the schedule frequency and range of the job (start/end dates). The rule schedule can have an end date or be defined to run indefinitely.

Inspect/Edit

Event Inspector Group: Scheduled Badge Entry an...

Attributes Jobs Notes

+ Add ✕ Remove ↻ Frequency

Jobs	Description
Badge Entry and Logins	Look for matching event card swipe an...

Next Run Time **7 Nov 2006 11:35:00 PST**

Job Parameters

Name	Value
Batched Rule Engine Parameter	
* Filter results by	All Events

Summary

Occurs **Hourly**.

Schedule will start on **6 Nov 2006 16:35:20 PST**.

OK Cancel Apply Help

Job Frequency

Schedule Frequency

☒ Hourly Every hour(s) at minutes after

☐ Daily

Daily Frequency

☒ Occurs once at

Schedule Range

Start:

End: ☒ No End date ☐ End on

OK Cancel Help

- 8 Click **Apply** or **OK** to deploy.

The rule(s) will be deployed according to the schedule specified in the Rule Group editor on the Jobs tab, and will be triggered if the rule conditions are met.



You cannot schedule a single rule outside of a group, but you can schedule it as a "group of one" contained in a folder. To schedule one or more rules, place them in a folder. Multiple rules in the same folder will run together per the schedule as part of the rule group.

Example of a Scheduled Rule (Badge Swipes and Logins)

As an example, here are the **conditions statements** for a rule that correlates Badge swipe events, which are sent to the Manager in a batch file once per day, with login events which are sent to the Manager frequently in real-time. The example rule looks for an event with "swipe" in the name and an event with "login" in the name.

Rule has condition that matches badge swipe entry with login event. (Shown here on both Conditions Edit and Summary display tabs.)

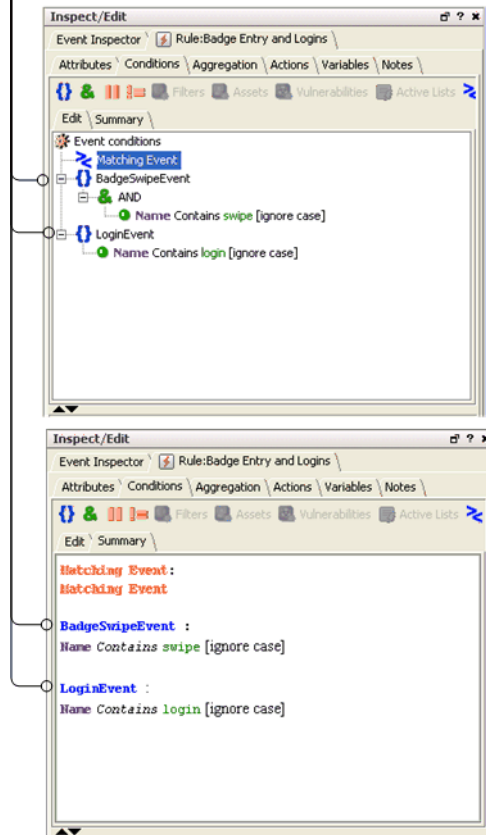


Figure 13-2 Example Scheduled Rule: Condition Statements

This rule sets an **aggregation time window** to correlate these events at 2 minutes. This means that a login event (end time) must occur within 2 minutes of a badge swipe event (end time) in order for the rule to be triggered.

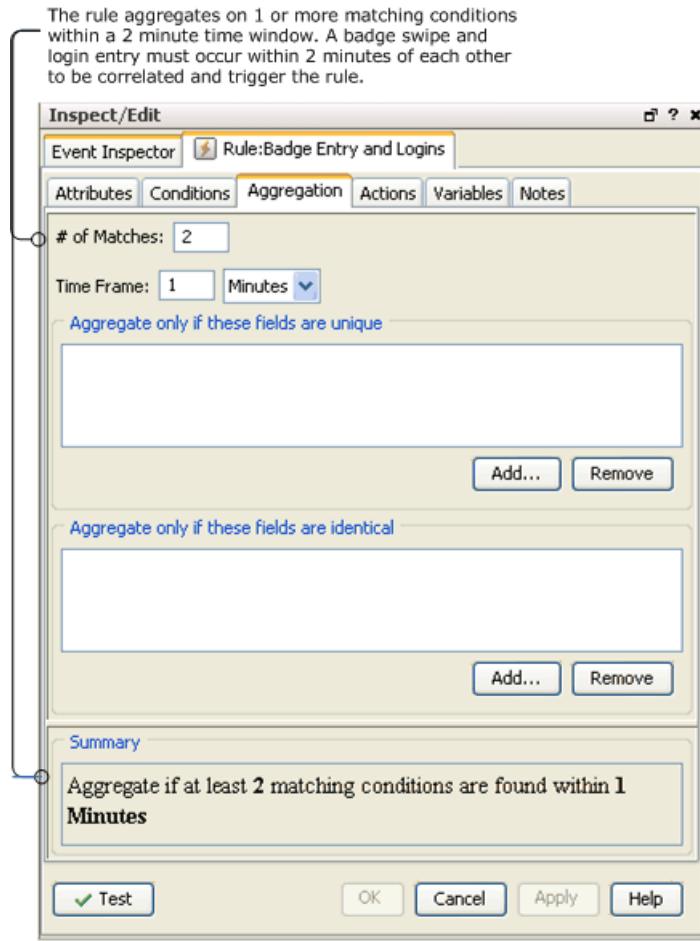


Figure 13-3 Example Scheduled Rule: Aggregation

Note that if you deploy this rule in real-time rules, the rule will not be triggered to capture the events you want to correlate. Although the badge swipe events are actually occurring within 2 minutes of login events (according to event end times), the ArcSight Manager Receipt Time for badge swipe events is always hours later (whenever they are submitted as batched events). In this kind of scenario, the real-time rules engine would never correlate these events because the badge swipe events (with late Manager Receipt time) would be read in so much later.

If, however, you deploy this as a scheduled rule to run on a nightly basis, the rule will be triggered and capture the correlated events. This is because the scheduled rules engine is designed to correlate historical data with live data.

To configure this as a scheduled rule, you would create a new folder (group) for it under Rules resources in the Navigator, link or move the rule into the folder, then edit the rule group to add a scheduled job (on Jobs tab). The job schedule defines when the rule will run. Once the job schedule is applied to the rule group, the rule is deployed as a scheduled rule.

To create and test the example rule:

- 1 Create a rule called "Badge Entry and Logins".
- 2 On the Conditions tab for this rule, set a condition to look for two events joined by "AND"; an event with "swipe" in the event name and an event with "login" in the event name.
- 3 Save the new rule.
- 4 Create a new rule group folder called "Badge Entry and Logins" and link or move the rule into that folder.
- 5 Edit the "Badge Entry and Logins" rule group to add a scheduled job for rule of the same name.
- 6 Save the new rule group.

Once you save the rule group with the scheduled job, the rule is deployed.

For testing purposes, schedule the job to start in 5 minutes from the current time and then use the ArcSight Test Alert connector to test sending events to the Manager with end times within two minutes of each other and different Manager receipt times. (For example, to model a real-world scenario: set Manager receipt time for badge swipes to several hours later than for logins.)

Make sure that the start time of your scheduled job is earlier than the event end times on your test events (so that the scheduled job is running to capture the events). You should see the scheduled rule triggered on correlated events.

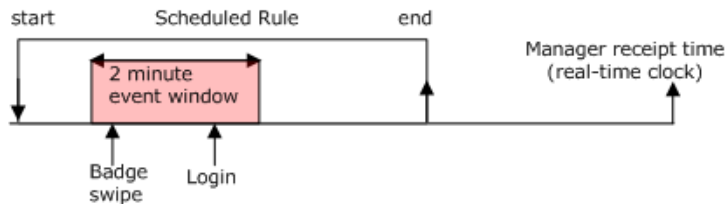


Figure 13-4 Start Time on Example Scheduled Rule is Set Earlier than End Times of Events

As a comparison, deploy the same rule in a real-time rules folder and send the test events again. Note that the same rule will not be triggered by the real-time rules engine because it is not designed to correlate historical data.

In every scheduled run of a rule, only events arriving between that run and the earlier run are considered for input.

Testing Rules

You can test rules against copies of active channels for valid conditions logic, verify that rules are triggered by the events they are supposed to capture, and that they generate correlated events as expected.

The ArcSight Console provides two different ways of getting to tools for testing and verifying rules against events before deploying the rules in real time:

- Test a single rule from within the rule editor by clicking the Test button
- Test rules and rule groups from the navigation tree with the Verify Rules with Events option

These options are somewhat similar. They differ in the navigation paths to select or set up the channels, and more importantly in that from the rule editor you can test only the selected rule but from the navigation tree you can test several selected rules or rule groups. This Help topic explains how to test a single rule from the rule editor. See also [“Verifying Rule\(s\) with Events” on page 326](#).

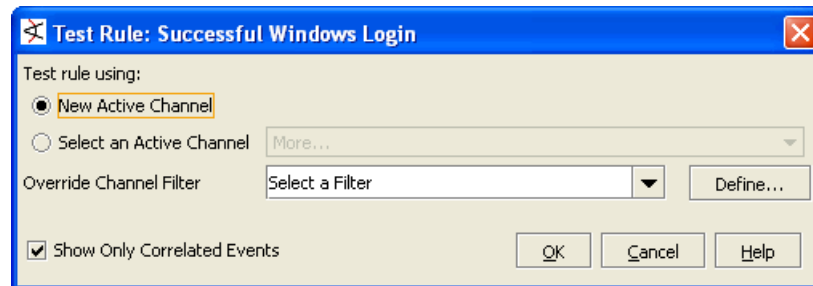


Keep in mind that only rules deployed in Real-time Rules act on live events and show up in a live channel when they are triggered. For more information, see [“Deploying Real-time Rules” on page 329](#).

Testing a Rule from the Rule Editor

- 1 Choose the Rules resource in the Navigator, and select the rule you want to test.
- 2 Right-click and choose **Edit Rule** to bring up the Rule editor for that rule in the Inspect/Edit panel.
- 3 In the editor for the selected rule, click **Test**.

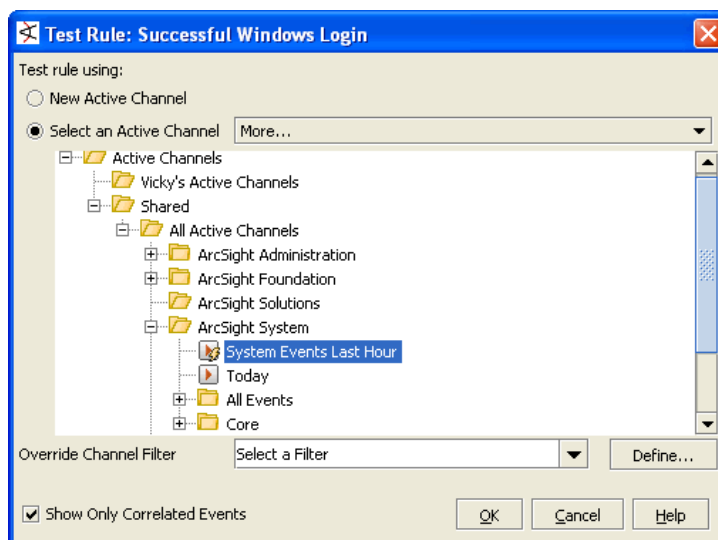
This brings up the Test Rule dialog where you can choose an existing active channel or create a new channel in which to verify the rule.



- 4 Select either **New Active Channel** or **Select an Active Channel** depending on whether you want to test the rule in a new or existing channel.

You can set override channel filters on either a new or existing active channel.

If you choose **Select an Active Channel** (which means you are opting to use an existing channel rather than create a new one), an inline browser is displayed where you can navigate to and choose an existing channel.



- 5 Once you have set up the channel, click **OK**. (If you need more help on setting up channels, see [“Viewing and Using Channels” on page 92](#).)

The channel is displayed in the Viewer panel.

Showing Rule Errors

If rules have errors, the rule icon () changes to indicate it.

In the Rules resource tree, right-click the rule-error icon and choose **Show Error**. The error appears in a dialog box.

Verifying Rule(s) with Events

The ArcSight Console provides two different ways to test or verify rules before deploying them. These options are somewhat similar. They differ in the navigation paths to select or set up the channels, and more importantly in that from the rule editor you can test only the selected rule but from the navigation tree you can test several selected rules or rule groups.

This topic explains how to test multiple rules or rule groups from the navigation tree using “Verify Rule(s) with Events”. See also [“Testing Rules” on page 324](#).

In v4.0, “replay with rules” becomes “verify rules with events”, an enhanced version of the feature. You can test rules by running them against a set of captured events for forensic analysis. Now you can replay events to verify rules in existing active channels or, as before, create new channels for this purpose. Also, you can select a single rule, multiple rules, or a rule group to verify. (In earlier releases, only the last of these options was available.)

To verify rules with events, select an existing active channel or create a new one, and then scan the list of events in the channel to verify that the rule is triggered and that it generated correlated events as expected.

Existing active channels have a sliding time window for events (based on the channel filters).

New active channels created as “replay with rules” channels have a fixed time window for qualifying events, and the events are those that qualify under the rules in the selected group. These active channels incorporate the conditions, aggregation characteristics, and actions defined for the rules in the selected group.



Rules tested against pre-existing active channels are actually executed on copies of active channels the system automatically generates for this purpose. Rules run in verify mode do not generate real rule actions correlated with live or historical system events and, therefore, when they are triggered no real rule actions are impacting the system state. Only real-time rules or scheduled rules (set up to capture batched and other types of historical data) will trigger real rule actions.

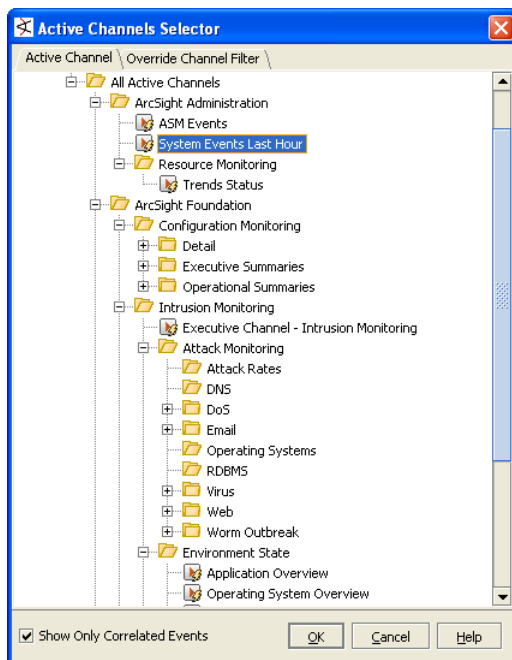
Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. For more information, see [“Deploying Real-time Rules” on page 329](#) and [“Scheduling Rules” on page 319](#).

Verify Rule(s) from the Resource Tree

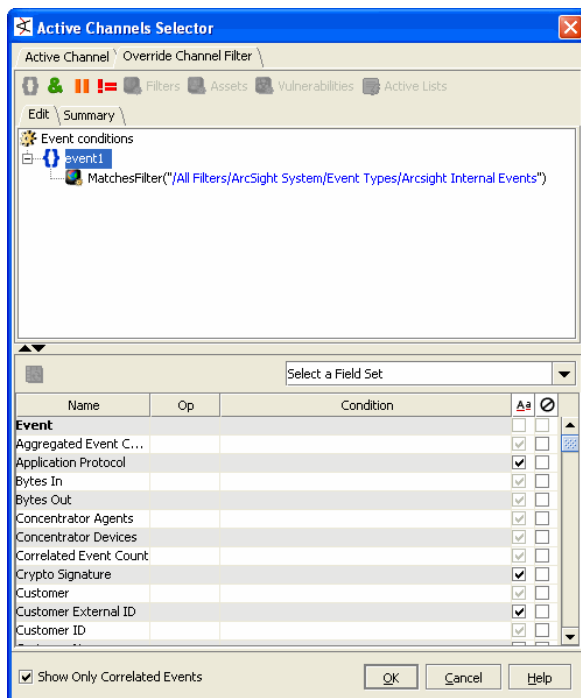
- 1 In the Rules resources tree, right-click an appropriate group and choose **Verify Rule(s) with Events**.

- 2 From the sub-menu, choose **Most Recent Opened Active Channels**, **More**, or **New Active Channel**.

- ◆ **Most Recent Opened Active Channels.** Choose from the list of recently opened channels. The selected channel is displayed in the Viewer panel.
- ◆ **More...** This brings up the Active Channel Selector dialog. Use this dialog to navigate to the channel you want.



If you want to redefine or further narrow the stream of events in the selected channel, click the **Override Channel Filter** tab to add filters to it. The **Override Channel Filter** tab shows the conditions on the currently selected channel. You can add, remove, or modify the filters here.

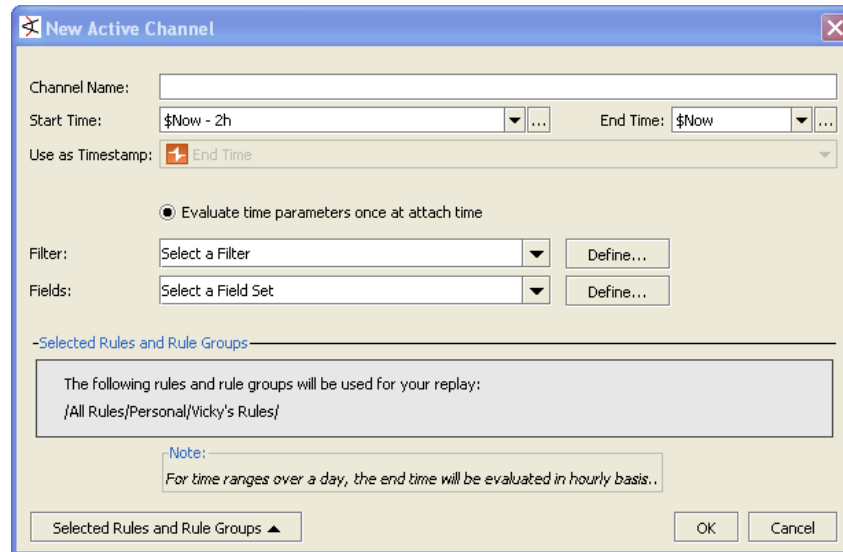


Click **OK** to choose the selected channel with filter modifications (if any).

The selected channel is displayed in the Viewer panel.

◆ New Active Channel...

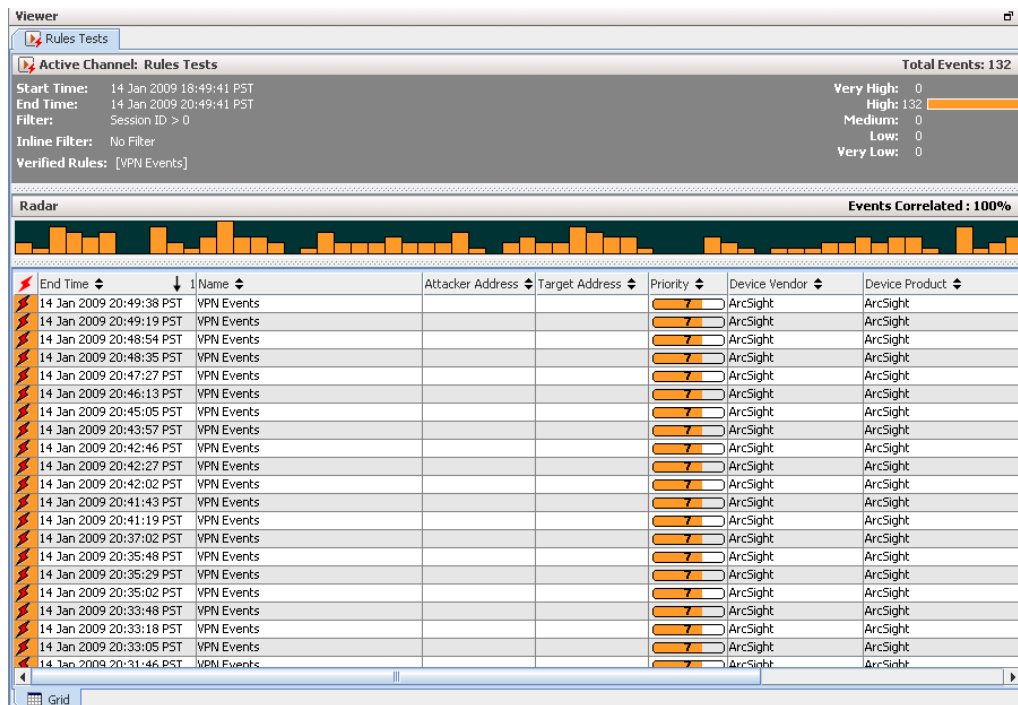
Selecting this option brings up a dialog where you can set up the parameters for the active channel that will display the rules in action. Provide a name for the new channel and set the other channel options as described in [“Viewing and Using Channels”](#) on page 92.



The dialog box titled "New Active Channel" contains the following fields and options:

- Channel Name:** A text input field.
- Start Time:** A dropdown menu showing "\$Now - 2h" with a "... " button.
- End Time:** A dropdown menu showing "\$Now" with a "... " button.
- Use as Timestamp:** A dropdown menu with "End Time" selected.
- Evaluate time parameters once at attach time:** A radio button that is selected.
- Filter:** A dropdown menu showing "Select a Filter" with a "Define..." button.
- Fields:** A dropdown menu showing "Select a Field Set" with a "Define..." button.
- Selected Rules and Rule Groups-** A section containing a text box that says "The following rules and rule groups will be used for your replay: /All Rules/Personal/Vicky's Rules/".
- Note:** A text box that says "For time ranges over a day, the end time will be evaluated in hourly basis..".
- Buttons:** "OK" and "Cancel" at the bottom right.


Click **OK** to create the new channel with your chosen settings. The new channel is displayed in the Viewer panel.



The Viewer panel displays the "Active Channel: Rules Tests" configuration. The start time is 14 Jan 2009 18:49:41 PST and the end time is 14 Jan 2009 20:49:41 PST. The filter is "Session ID > 0". The verified rules are "[VPN Events]". The total events are 132. The events are categorized by priority: Very High (0), High (132), Medium (0), Low (0), and Very Low (0). A radar chart shows the distribution of events over time, with a correlation of 100%.

End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
14 Jan 2009 20:49:38 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:49:19 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:48:54 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:48:35 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:47:27 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:46:13 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:45:05 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:43:57 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:42:46 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:42:27 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:42:02 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:41:43 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:41:19 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:37:02 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:35:48 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:35:29 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:35:02 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:33:48 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:33:18 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:33:05 PST	VPN Events			7	ArcSight	ArcSight
14 Jan 2009 20:31:46 PST	VPN Events			7	ArcSight	ArcSight



About Test Channels: A lightning bolt  on a channel indicates it is a test channel created as a result of choosing **Verify Rules with Events** on a rule. Test channels cannot be re-used, even for the same rule. Remove test channels from the Active Channels folder in the Navigator.

Alternatives to Test Channels: If you would like to re-use a channel to test various rules, create a standard active channel e.g., "My Rules Test Channel" (see ["Creating an Active Channel" on page 93](#)), then send rules test results to that channel. You can re-use a standard channel as many times as you want to test rules (i.e., *verify rules with events*).



Filters shown on rule verification channels are not designed for copying and re-use outside of these special rule testing channels. Rule verification channels will show rule-triggered events and other non-correlation events in the channel, but the complete filtering logic that accomplishes this is not exposed.

Filter conditions on these channels will display the original filter (if one is applied) and "Session ID > 0". The session ID statement is a simplified representation of the back-end filtering taking place in the special rule verification channel to limit this particular channel to show only new rule-triggered events.

Deploying Real-time Rules

Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules.

Rules run in verify or test rule mode do not generate real rule actions correlated with live or historical system events and, therefore, when they are triggered no real rule actions are impacting the system state.

Only real-time rules show up in a live channel, generate correlation events, and trigger real rule actions.



A special category of rules called scheduled rules can capture batched and other types of historical data, generate correlation events, and trigger real rule actions. These act similar to real-time rules, but are deployed differently. They are evaluated according to a schedule, and trigger off of historical/past events. See ["Scheduling Rules" on page 319](#) for more information.



Deploying a Rule

In the **Navigator** panel's **Rules** resource tree, right-click a rule or a rule group (folder) and choose **Deploy Realtime Rule(s)**.

The rule(s) you deploy will be linked into the Real-time Rules folder (Shared/All Rules/Real-time Rules). This means that if you change something in the working copy of a rule (in your user folder), those changes will also take effect in the deployed rule and vice versa.

You can also manually copy, link, or move rules from your working user folder to a user folder in Real-time Rules. To do this, click and drag a rule or rule group to the Real-time Rules folder, then choose an option in the dialog (Copy, Link, or Move). Using this method

of deploying real-time rules is useful if you want to copy or move the rule(s) rather than link them.

If a rule is already enabled () , it will be deployed as enabled. If a rule has been disabled () during testing phase, it will be deployed into real-time rules but remain disabled until you enable it. Rules must be both enabled and deployed in real-time rules to take effect in the live system. (If you enable or disable a deployed, linked rule in the original location it will also be enabled or disabled in real-time rules and vice versa.) For more information, see ["Enabling and Disabling Rules" on page 317](#).

Removing or Un-deploying a Rule

You can remove rules from the Real-time Rules folder, thereby "un-deploying" them from the live system.

To un-deploy a rule (beyond disabling it), select the rule in the Real-time Rules folder, right-click, and choose **Delete Rule** from the context menu.

Depending on whether the rule was linked, moved, or copied into the Real-time Rules folder, you will get different options at this point.

- If the rule has been moved or copied into your working folder, you will get an option to remove it or to cancel the operation.
- If the rule is a link to the original rule in your working folder, you will get options to remove it from this group only, delete it entirely from all locations, or cancel the operation. (A linked file is treated as a single entity, so edit actions taken on the file in any location affect all instances of it.)

Loading Rules

Creating custom rules does have an effect on the load placed upon the ArcSight Manager. This load is a function of how many partial and full matches are generated by those rules. Since partial matches occur when any condition of a rule is met and full matches occur once all conditions of a rule have been met, poorly written rules can generate many partial matches without generating any full matches.

Also, poorly written rules can generate, in a worst case scenario, one additional event for every incoming event. However, well-written rules have conditions that are restrictive enough to limit partial matches to those events that are likely to participate in a full match. Such rules are also likely to generate very meaningful derived events and they also impose a smaller load on the ArcSight Manager. Therefore is it very important that you carefully plan, write, and test all your custom rules.

Automatic Disabling

ArcSight automatically disables improperly written rules that would produce excessive or meaningless events. The conditions that cause rules to be disabled are described below.

The factors that control rule disabling are shown in the table below.

Rule Disabling Factor	Operation
Alias Matches	If an alias is defined in the rule, this is the number of events matching that alias, independent of other defined aliases.
Partial Matches	If more than one alias is defined in the rule, this is the number of events matching the aliases defined before the current one, and for the current one, and for their join condition (if present).
Generated Events Counts	The number of correlation events generated.
Base Event Counts	The number of base events used by the rule to generate correlation events.
Time Unit Counts	The number of time units (minutes) that passed since the current rule activated.

Therefore, the conditions that can result in rule disabling are:

- The number of matching aliases would exceed the default limit of 100000.
- The number of partial matches for any of the aliases would exceed the default limit of 100000.
- The rule generates more than five correlation events for each base event it processes.
- The rule generates more than 100 correlation events in one time unit.

The above values are defaults that may be adjusted differently for your enterprise.

Chapter 14

Use Cases

This topic describes how use cases can help address business requirements/security issues.

[“What are ESM Use Cases?” on page 333](#)

[“Installing Use Cases” on page 335](#)

[“Navigating to Use Cases” on page 336](#)

[“Opening Use Cases” on page 336](#)

[“Configuring Use Cases” on page 338](#)

[“Configuration Panels” on page 344](#)

What are ESM Use Cases?

New in ArcSight ESM v4.5, **use cases** are collections of ArcSight ESM resources used to address:

- security issues
- business requirements

Resources are viewable separately by type in the ArcSight ESM Console. For example, all rules installed on an ArcSight ESM Manager can be viewed from the Resources tab of the panel, as shown in [Figure 14-1](#).

Use cases provide an alternative, integrated view of resources by supporting the grouping of resources by the security issue or business requirement they address, as shown in [Figure 14-2](#). For example, the following resources could be grouped together in a use case: a rule, a query, a report, and an active list.

Figure 14-1 Group Resources by Type

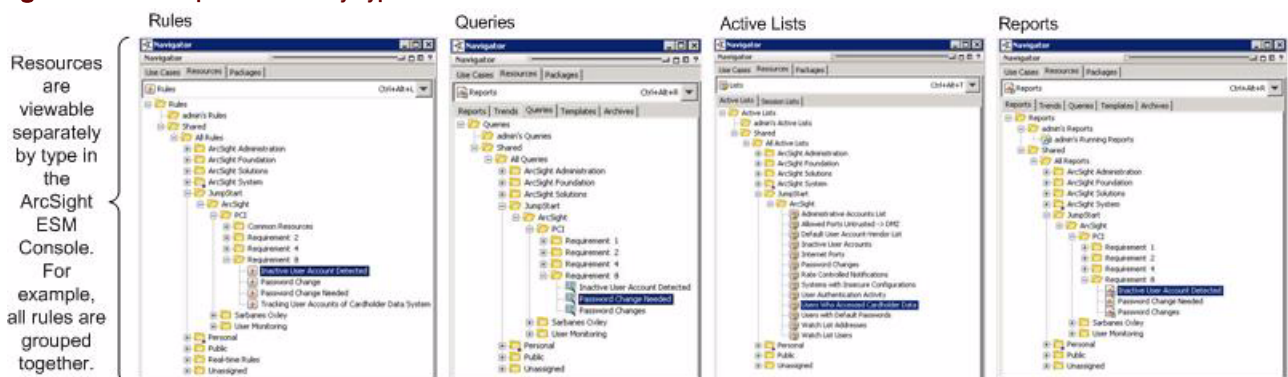
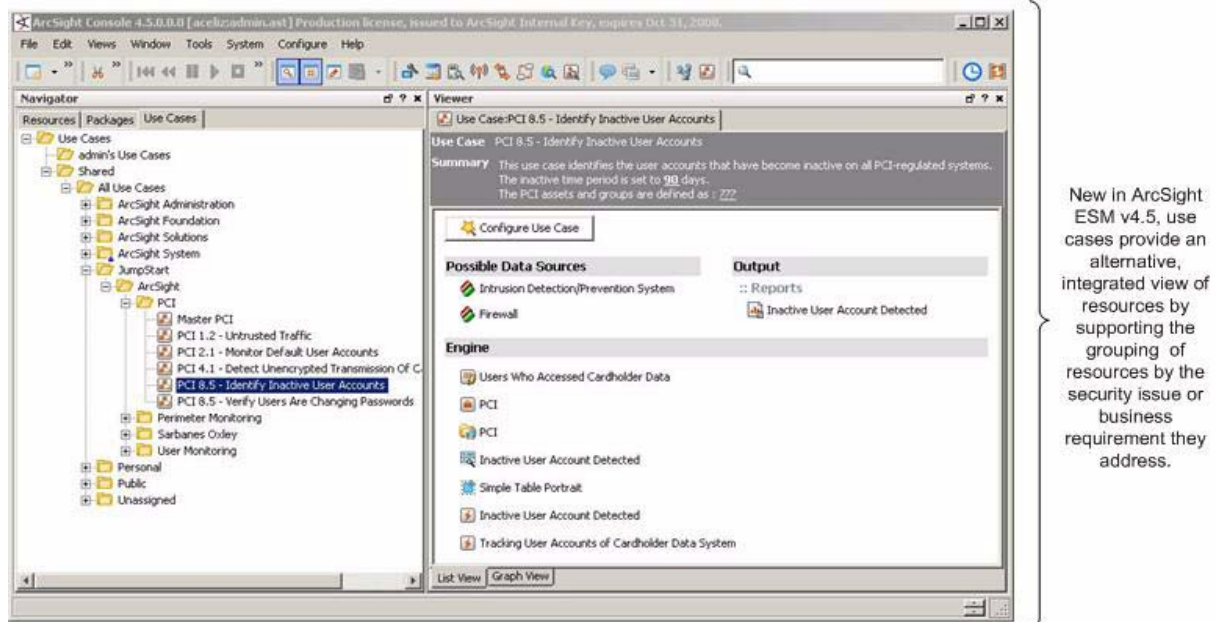


Figure 14-2 Group Resources by Use Case

For example, the *PCI 8.5- Identify Inactive User Accounts* use case contains a set of resources that can help determine when user accounts become inactive on PCI-regulated systems. The Payment Card Industry (PCI) requirement 8.5.5 specifies that inactive user accounts should be removed at least every 90 days. The resources provided with the *PCI 8.5- Identify Inactive User Accounts* use case are available in the Viewer panel as shown in Figure 14-2.

In addition to providing the ability to view all the resources of a use case from the Viewer panel, ArcSight ESM v.4.5 also offers a Use Case wizard that can be used to configure the resources in a use case by asking a set of simple questions as described in [“Configuring Use Cases” on page 338](#).



ArcSight ESM Administrators should run the Use Case wizard. Only Administrators may have the necessary permissions to configure the resources in a use case.

Master Use Cases

Typically, a set of similar use cases are bundled together into an ArcSight Resource Bundle (ARB) file and located in the same group in the Navigator panel. For example, all the use cases from the JumpStart Pack for PCI are located in the [/All Use Cases/JumpStart/ArcSight/PCI](#) group as shown in Figure 14-2.

In addition to the set of regular use cases, a special use case called the Master use case may also be provided. If included, the Master use case does not address a specific security issue or business requirement but instead provides the ability to configure the common resources of the use cases in the same group.

Some common resources can be configured in both the Master use case and in the individual use cases using the Use Case wizard. For example, when configuring the Master PCI use case, you are prompted to select the assets or asset groups that should be categorized as **PCI**. This categorization can be done once for all the PCI use cases by configuring the Master PCI use case. However, when configuring an individual PCI use

case, you are still prompted to select the assets and asset groups that should be categorized as [PCI](#). If you have already done the categorization globally using the Master use case, you can skip this categorization step by clicking **Next** in the Categorize PCI Assets panel of the individual use case.


Some common resources can only be configured in the Master use case. For example, the notification e-mail address and the notification rate can only be set by configuring the Master PCI use case.

When installing an ArcSight Resource Bundle (ARB) file, if a Master use case is associated with use case group in the ARB file, after installing the resources in the ARB file the Use Case wizard launches and starts configuring the Master use case associated with the use case group.

Installing Use Cases

If no use cases are installed on the ArcSight ESM Manager, the Use Case tab on the Navigator panel is not displayed. To activate the Use Case tab on the Navigator panel, import and install an ArcSight Resource Bundle (ARB) file containing a use case. ARB files end with the [.arb](#) extension. Some ARB files containing use cases are supplied with the ArcSight ESM Console installation. For more information, see [Step 4](#) below.

To import and install a use case bundle and package:

- 1 Log into the ArcSight ESM Console as the ArcSight ESM Administrator. Only Administrators may have the necessary permissions to configure the resources in a use case.
- 2 Click the **Packages** tab in the Navigator panel.
- 3 Click **Import** ().
- 4 Browse for an ARB file that contains use cases. Some ARB files containing use cases are available in the [ARCSIGHT_HOME/current/jumpstart](#) directory.
- 5 Choose a use case ARB file to import and click **Open**.

When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.

- 6 Leave the Install check mark selected and click **Next**.

The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.

- 7 In the Installing Packages dialog, click **OK**.
- 8 In the Importing Packages dialog, click **OK**.

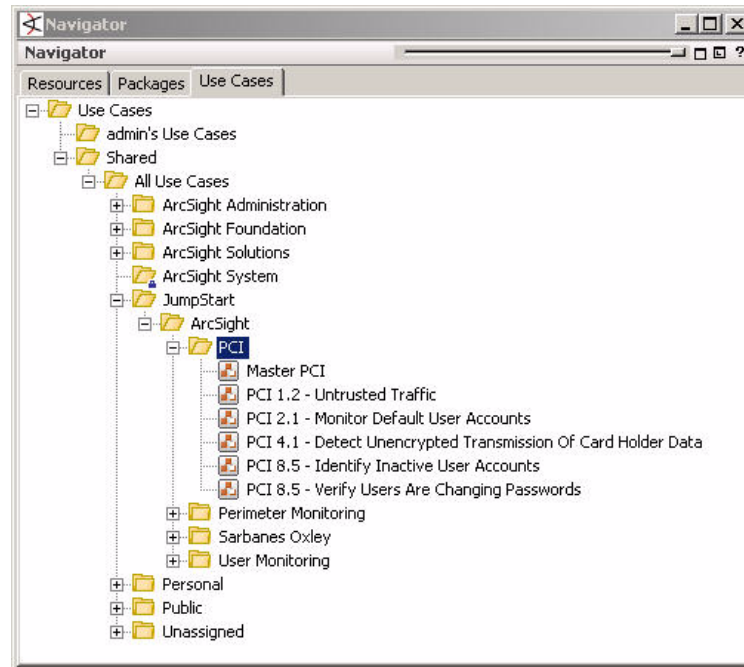
If a Master use case is associated with a use case group in the ARB file, the Use Case wizard launches and starts configuring the Master use case associated with the use case group. The Master use case is provided so you can configure the common resources used by the use cases in the group with a single configuration pass of the wizard. For more information, see ["Master Use Cases" on page 334](#). For instructions on using the Use Case wizard, see ["Configuring Use Cases" on page 338](#).

For more information, see ["Importing Bundles" on page 494](#) and ["Installing Packages" on page 495](#).

Navigating to Use Cases

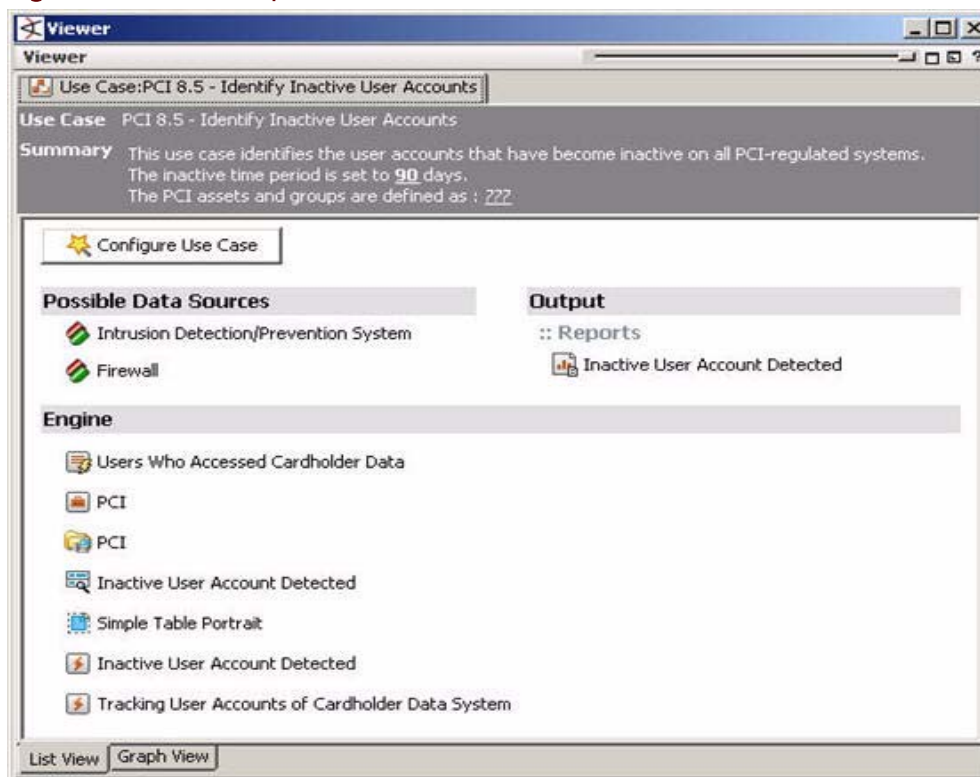
Once a package bundle that contains a use case has been installed from an `.arb` file, the Use Case tab is visible from the Navigator panel and the use cases (📁) are listed in the Use Case tab as shown in [Figure 14-3](#).

Figure 14-3 Use Cases in Navigator Panel



Opening Use Cases

To open a use case in the Viewer panel, right-click a use case and select **Open Use Case**. The use case displays in the Viewer panel as shown in [Figure 14-4](#).

Figure 14-4 Use Case Opened in Viewer Panel

The following information about the use case is displayed in the Viewer panel:

- summary describing the purpose of the use case
- resources that make up the use case:
 - ◆ **under the Output label**—the consumable resources that produce output such as reports, cases and dashboards
 - ◆ **under the Engine label**—the resources that hold data (such as active lists), the resources that process data (such as rules, data monitors, and queries), and groups for categorizing assets
- **under the Possible Data Sources label**—any potential data sources that could provide log data (in the form of ESM events) to the use case using SmartConnectors are listed
- a graphical view of the use case and the associated resources is available from the Graph View tab

In addition to providing the ability to view all the resources of a Use Case from the Viewer panel, ArcSight ESM v.4.5 also provides a Use Case wizard that configures the Use Case by asking a set of simple questions as described in [“Configuring Use Cases” on page 338](#).

Accessing Resources from the Viewer Panel

When a use case is open in the List View tab of the Viewer panel, you can view, edit, navigate, or graph a use case resource, by right-clicking the resource and selecting from one of the following options:

- **View**—Open the resource in the Viewer panel to view the contents of the resource. This option is not available for all resources.

- **Edit**—Open the resource for editing in the Inspect/Edit panel. For more information, see [“Inspecting and Editing” on page 66](#).
- **Find**—Open the resource in the Navigator panel. For more information, see [“Navigating” on page 58](#).
- **Graph View**—View the association between this resource with other resources using a graphical viewer. For more information, see [“Visualizing Resources” on page 537](#).



You can also view a graphical representation of the resources in the use case by selecting the Graph View tab at the bottom of the Viewer panel.

Configuring Use Cases

A Use Case wizard is provided to assist you in configuring the resources in the use case to reflect your environment by asking a series of simple questions.



ArcSight ESM Administrators should run the Use Case wizard. Only Administrators may have the necessary permissions to configure the resources in a use case.



You do not have to use the wizard to configure the resources in a use case. You can manually configure the resources that make up the use case.

To use the Use Case wizard:

- [“Step 1 - Model Your Network” on page 338](#)
- [“Step 2 - Install Use Case Package Bundles” on page 338](#)
- [“Step 3 - Launch the Use Case Wizard” on page 338](#)
- [“Step 4 - Introduction Panel” on page 339](#)
- [“Step 5 - Prerequisites Panel” on page 339](#)
- [“Step 6 - Confirm Event Sources Panel” on page 340](#)
- [“Step 7 - Configuration Panels” on page 341](#)
- [“Step 8 - Summary of Settings to Apply Panel” on page 342](#)

Step 1 - Model Your Network

Model your network first, as a part of the initial configuration of ArcSight ESM. Use case configuration requires having a network model in place. So, model your network before running the Use Case wizard.

To assist in modeling your network, a Network Model wizard is provided on the ArcSight ESM Console (menu option **Tools > Network Model**). For more information, see [“Modeling Your Network and Managing Assets” on page 456](#).

Step 2 - Install Use Case Package Bundles

Import and install the use case package bundle that contains the use case (if it is not already installed). For more information, see [“Installing Use Cases” on page 335](#)

Step 3 - Launch the Use Case Wizard

Launch the Use Case wizard using one of the following methods:

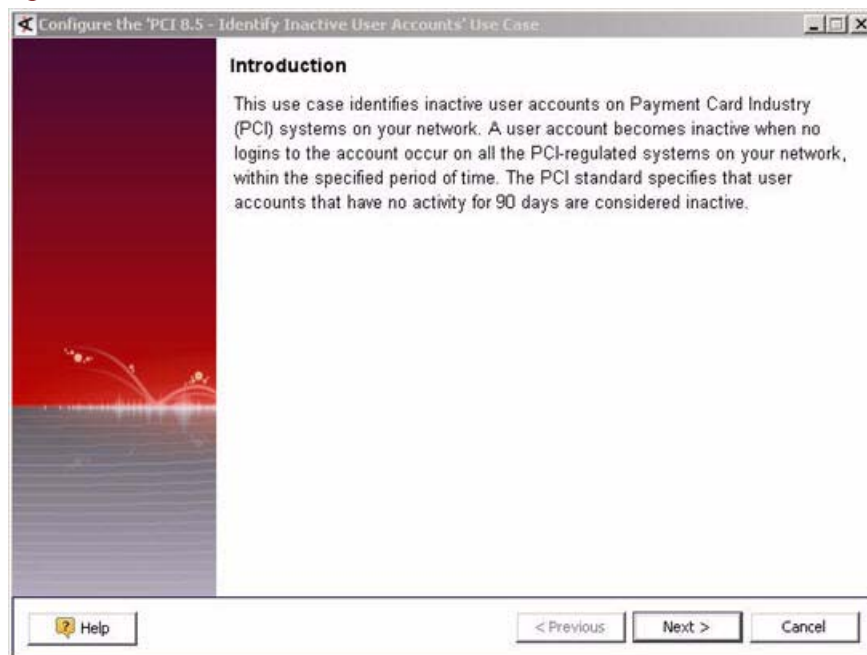
- **Browse from the Navigator panel**—In the Navigator panel, select the Use Cases tab, right-click a use case and select **Configure Use Case**.
- **From the ArcSight ESM Console menus**—Choose **Tools > Use Cases** from the menus. Select a case and click **Next**.
- **From the Viewer panel**—In the Navigator panel, select the Use Cases tab, right-click a use case and select **Open Use Case**. In the Viewer panel, click **Configure Use Case**.

The Introduction panel of the Use Case wizard displays.

Step 4 - Introduction Panel

The Introduction panel (Figure 14-5) describes the purpose of the use case. If you are configuring a Master use case, the introduction specifies if there are essential common resources that can only be configured using the Master use case. For more information, see [“Master Use Cases” on page 334](#).

Figure 14-5 Introduction Panel



Click **Next**.

The Prerequisites panel displays as shown in [Figure 14-6](#).

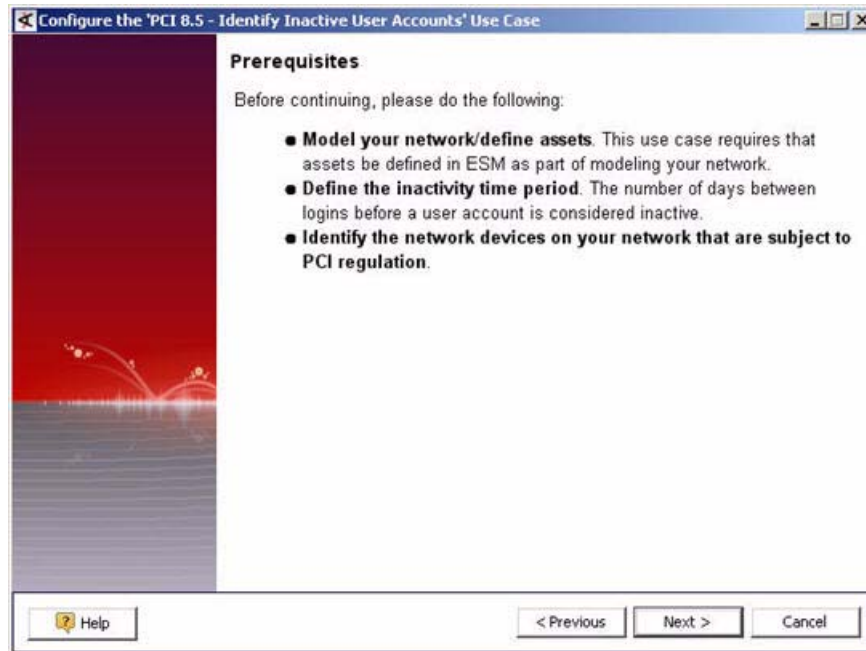
Step 5 - Prerequisites Panel

The Prerequisites panel (Figure 14-6) describes required actions or information needed before continuing with the Use Case wizard:

- **Any actions that should be completed before running the Use Case wizard.** For example, your network should be modeled before using the Use Case wizard to configure the use case. A Network Model wizard is provided from the ArcSight ESM Console (menu option **Tools > Network Model**). For more information, see [“Modeling Your Network and Managing Assets” on page 456](#). Complete these actions before continuing with the Use Case wizard.

- **The information that needs to be provided when running the Use Case wizard to configure the use case.** For example, the number of days before a user is required to change their passwords or the network devices on your network that are subject to the PCI regulation. Gather this information before continuing with the Use Case wizard.

Figure 14-6 Prerequisites Panel



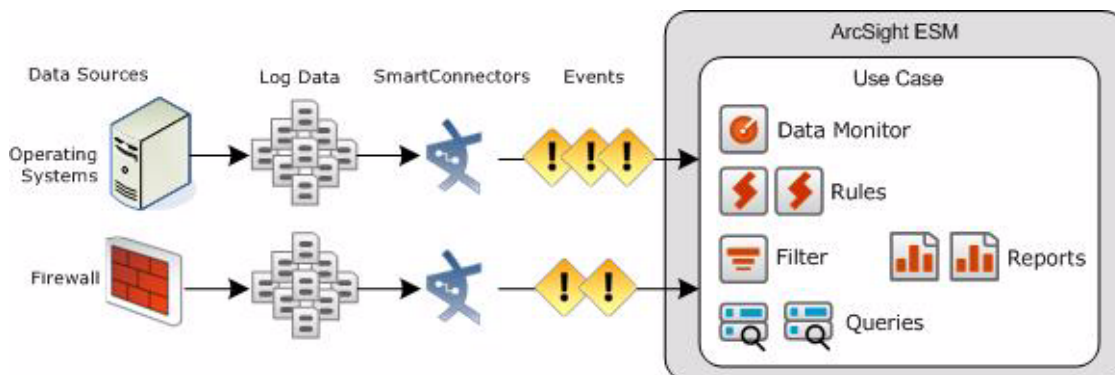
Click **Next**.

The Confirm Event Sources panel displays as shown in [Figure 14-8](#).

Step 6 - Confirm Event Sources Panel

The Confirm Event Sources ([Figure 14-8](#)) panel lists the event sources that send events to ESM via a SmartConnector for the use case. SmartConnectors collect log data from event sources (such as firewalls and operating systems) and generate events that are sent to ArcSight ESM as shown in [Figure 14-7](#).

Figure 14-7 Event Sources



The resources in the use case are driven by these events and without the event sources, the use case does not generate output. For more information, see *Devices and Connectors in a Network* in the *ESM 101 Guide* and [“Managing SmartConnectors” on page 498](#).

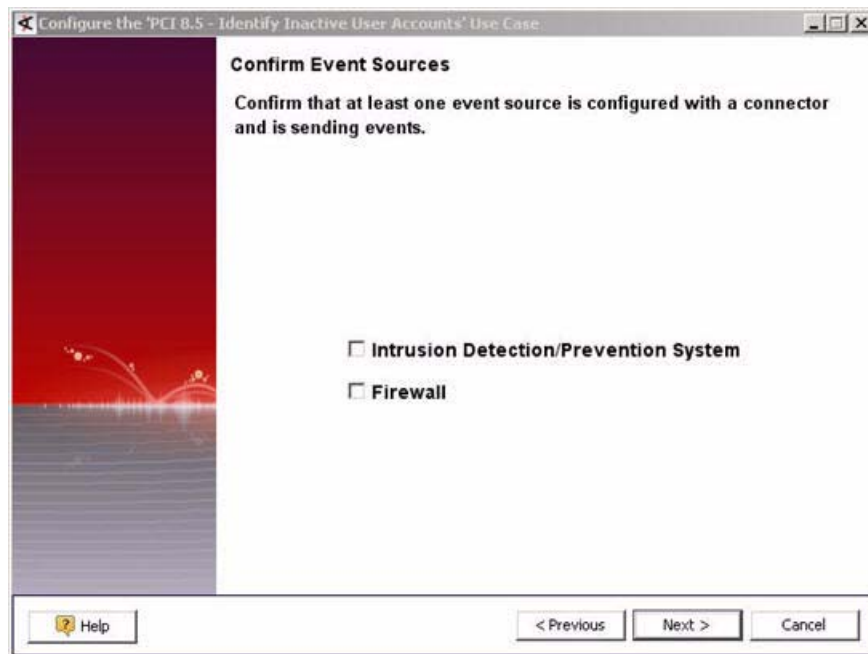
For your environment, confirm the event sources that are configured with a SmartConnector and supplying events to ArcSight ESM for this use case. For most use cases, you are asked to confirm that **at least one of the listed event source** is configured with a SmartConnector and sending events to ArcSight ESM.

Confirm the event sources and click **Next**.



The Confirm Event Sources panel is informational. It simply lists the event sources that can provide data to the use case. The wizard does no configuration based on options you select in this panel.

Figure 14-8 Confirm Event Sources Panel



After the Confirm Event Sources panel, a series of configuration panels display.

Step 7 - Configuration Panels

The series of configuration panels displayed depends on the resources that make up the use case and are different for each use case.

In these configuration panels, you are prompted to supply values that reflect your environment. The values you provide are used to populate the settings in the resources that make up the use case. After the series of configuration panels, the Summary of Settings to Apply panel appears. The settings are not actually saved to the resources until the Next button is clicked in the Summary of Settings to Apply panel. If you click Cancel in any of the configuration panels or in the Summary of Settings to Apply panel, none of the configuration settings specified in any of the configuration panels are saved.

The Use Case wizard displays the following types of configuration panels:

- “Categorize Assets/Zones Panels” on page 344
- “Define Data Sets Panels—Used to Populate Active Lists” on page 346
- “Specify the Notification E-mail Address Panel” on page 348
- “Specify the Expiration Time Period Panel” on page 349
- “Set the Notification Rate Panel” on page 349
- “Schedule Daily Report Panels” on page 350
- “Schedule Weekly Report Panels” on page 351
- “Schedule Monthly Report Panels” on page 353
- “Schedule Yearly Report Panels” on page 355

For each configuration panel, follow the instructions in the appropriate configuration panel and Help topic and click **Next**. Repeat until the Summary of Settings to Apply panel appears as shown in [Figure 14-9](#) and described in “[Step 8 - Summary of Settings to Apply Panel](#)” on page 342.

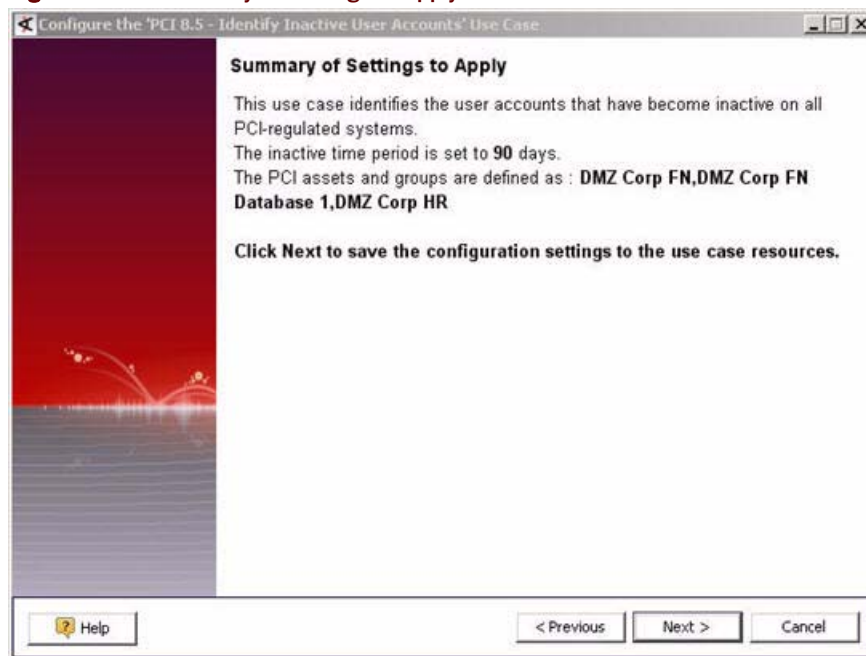
Step 8 - Summary of Settings to Apply Panel

The Summary of Settings to Apply panel ([Figure 14-9](#)) displays a summary of the settings you specified in the previous configuration panels.

Choose one of the following options:

- To apply the settings specified in the previous configuration panels to the use case resources, click **Next**.
- To cancel without applying settings, click **Cancel**.
- To go back to the previous panel, click **Previous**.

Figure 14-9 Summary of Settings to Apply Panel



After clicking Next, the settings are applied to the resources in the use case and the following changes occur:

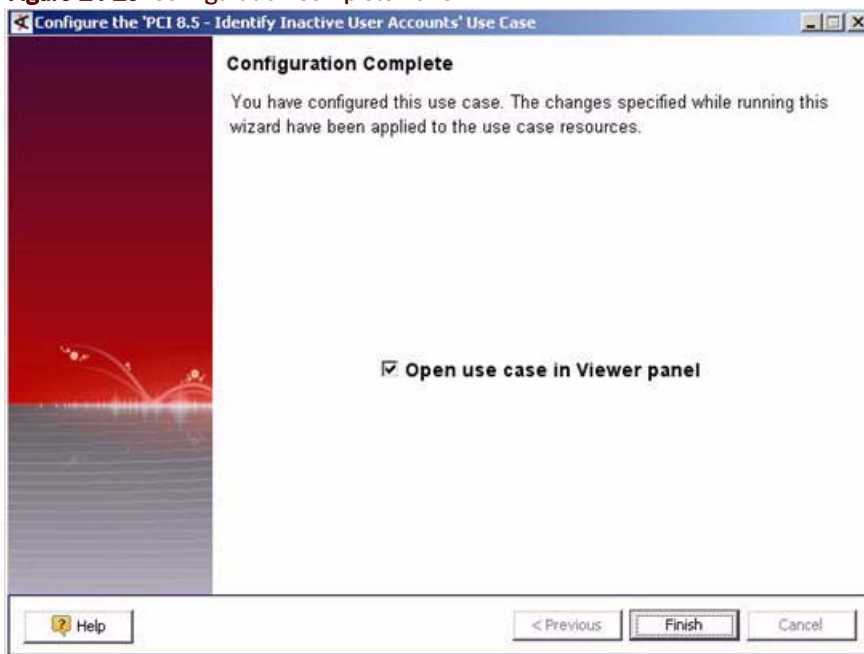
- **data monitors**—If the use case contains data monitors, the data monitors are enabled.
- **rules**—If the use case contains any rules, the rules are deployed into the Real-time Rules group. This deployment means that rules are triggered when events matching the conditions in the rule are satisfied. The rules in use cases are enabled by default. For more information, see [“Deploying Real-time Rules” on page 329](#).

A Commit Changes dialog briefly displays as the settings are applied to the use case resources. After the settings have been applied, a Configuration Complete panel displays as shown in [Figure 14-10](#).

Step 9 - Configuration Complete Panel

The Configuration Complete panel ([Figure 14-10](#)) displays a message indicating that you have completed configuration of the use case.

Figure 14-10 Configuration Complete Panel



Leave the *Open use case in Viewer panel* check box selected and click **Finish**.

The use case displays in the Viewer panel as shown in [Figure 14-4 on page 337](#). The configuration of the use case is complete. If the event sources for this use case are configured with a SmartConnector and are sending events to ArcSight ESM, the following actions occur:

- The engine resources in this use case such as rules, data monitors, and queries start processing events.
- If the conditions in the use case are met, data is provided to the output resources of the use case such as reports, active channels, dashboards, and cases.

In the future, you can reconfigure the use case resources, using either of the following methods:

- Run the Use Case wizard again—For more information, see [“Step 3 - Launch the Use Case Wizard” on page 338](#).

- Edit the resource directly in the Navigator panel—For more information, see [“Navigating” on page 58](#).

Configuration Panels

After the Confirm Event Sources panel, a series of configuration panels display. The set of configuration panels displayed depends on the goal of the use case and is different for each use case.

The Use Case wizard displays the following types of configuration panels:

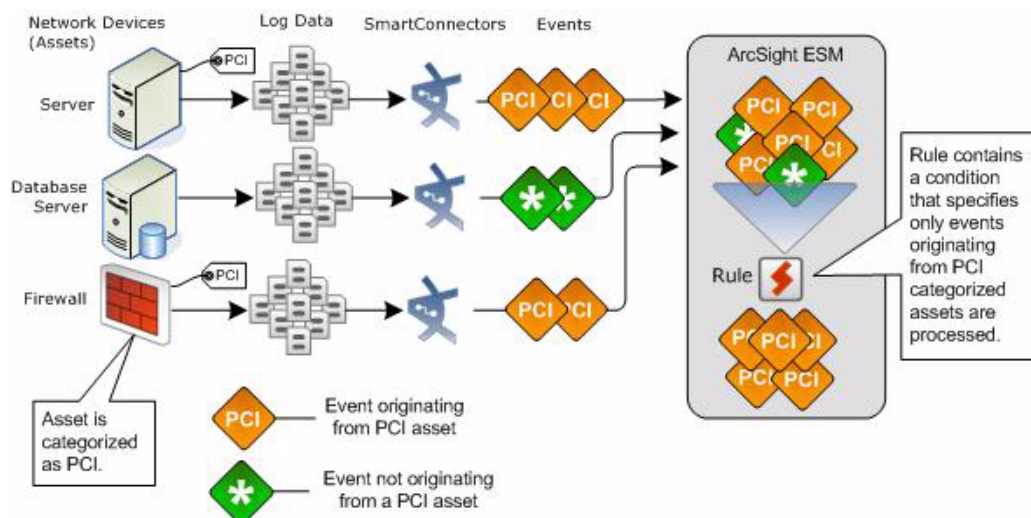
[“Categorize Assets/Zones Panels” on page 344](#)
[“Define Data Sets Panels—Used to Populate Active Lists” on page 346](#)
[“Specify the Notification E-mail Address Panel” on page 348](#)
[“Specify the Expiration Time Period Panel” on page 349](#)
[“Set the Notification Rate Panel” on page 349](#)
[“Schedule Daily Report Panels” on page 350](#)
[“Schedule Weekly Report Panels” on page 351](#)
[“Schedule Monthly Report Panels” on page 353](#)
[“Schedule Yearly Report Panels” on page 355](#)

After preceding through the series of configuration panels, the Summary of Settings to Apply panel ([Figure 14-9](#)) displays. Return to [“Step 8 - Summary of Settings to Apply Panel” on page 342](#).

Categorize Assets/Zones Panels

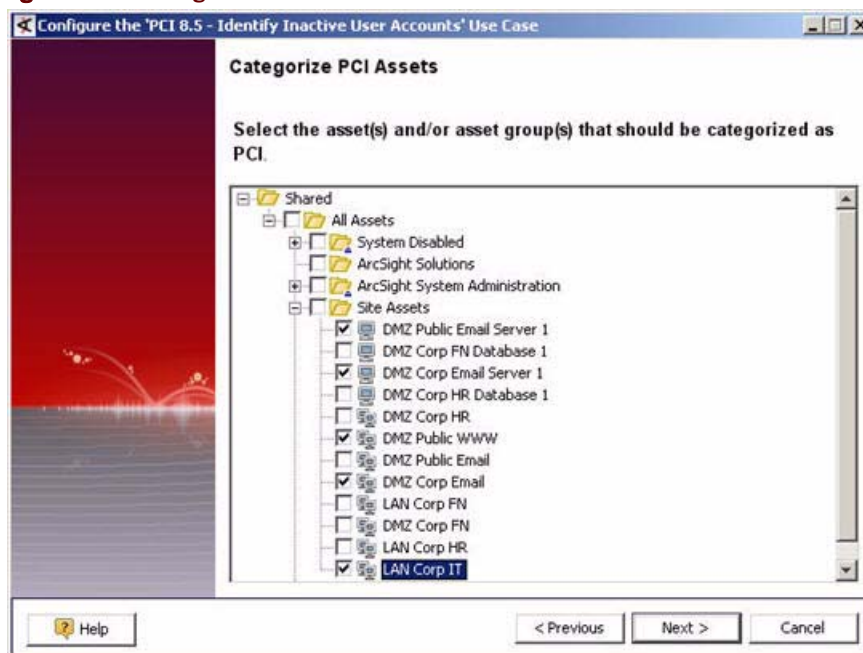
In the Categorize Assets or Zones panels, you are asked to classify assets or zones into an ArcSight ESM category. A logical category (such as [PCI](#) or [SOX](#)) can be applied to assets, asset ranges, asset groups, zones, or zone groups. These categories provide a cross-referencing capability that makes it possible to track and filter network activity based on business relevance. Using these categories, the events processed by the use case resources can be restricted.

For example, classifying assets into the [PCI](#) group can limit the set of events processed by the use case resources to only those events that originate from PCI assets. For example, a rule in a PCI use case may be configured to only process events originating from assets categorized as PCI as shown in [Figure 14-11](#).

Figure 14-11 Rule Processing Only PCI Events

In the Categorized PCI Assets panel, you are prompted to supply the network devices (assets) that should be regulated by the Payment Card Industry (PCI) standard and therefore categorized as a PCI asset, as shown in [Figure 14-12](#). The assets and asset groups you select in this panel are classified as a PCI asset in ArcSight ESM.

For more information, see [“Understanding ESM Asset Resources” on page 457](#), [“Categories” on page 606](#), and “Asset Model” in the *ESM 101 Guide*.

Figure 14-12 Categorize PCI Assets Panel

If any assets/zones have already been categorized, a check mark displays next to the asset/zone name. If your assets/zones are already categorized and no revisions need to be made, click **Next** to skip this step. For example, if you already categorized your assets/zones in the Master use case, you do not need to categorize your assets/zones

again. You can however, revise your asset/zone categorization while configuring the individual use case.

Select the assets that should be categorized and click **Next**.



The new categorization is not applied until **Next** is clicked in the Summary of Settings to Apply panel as described in [“Step 8 - Summary of Settings to Apply Panel” on page 342](#).

The categorization of assets, assets groups, zones, or zone groups is global in ArcSight ESM and not specific to a use case. Any categorization changes made in this panel (while configuring either an individual use case or the Master use case) affect any resources that reference this category in any use case. The last set of categorization changes, applied by clicking Next in the *Summary of Settings to Apply* panel, overrides any previous settings.

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Define Data Sets Panels—Used to Populate Active Lists

In the Define Data Sets panels, you are prompted for sets of data that are used to populate Fields-based active lists. Active lists store data over a period of time. Resources such as rules and data monitors can reference the data stored in active lists. For example, an active list could store the port numbers that are allowed access to the PCI CardHolder Data Environment (CDE). For more information, see *How Active Lists Work* in the *ESM 101 Guide*.

You may be prompted for a single column of data or multi-column sets of data. For example, you might be prompted to supply a set of trusted port numbers (one column of data) or a set of default User Accounts and associated Vendor Names (two columns of data). The data you provide in the panels is added to the data that may already exist in the active list.

To define the input data:

- 1 If you plan on importing the data using a CSV file, create the CSV file to import. The data types of the columns and the number of columns in the CSV file must match the columns in the active list. For example, in the Define Default User Accounts panel, you are prompted to provide a set of default User Accounts and associated Vendor Names. The *Default User Account-Vendor List* active list is a two column active list that expects default User Accounts in the first column and associated Vendor Names in the second column.
- 2 Select a method for populating the active list. In the first Define Data Sets panel ([Figure 14-13](#)), select one of the following options:
 - ◆ **Import CSV file**—Provide the data by importing a Comma-Separated Value (CSV) file
 - ◆ **Manual data entry**—Provide the data by typing the values directly into a table

Figure 14-13 Define Default User Accounts Panel—First Panel

Define Default User Accounts

Supply the default user accounts and vendor names for your network e.g. scott Oracle. If a CSV file is used, it should contain two columns.

User Account	Vendor Name
lpr	Unix

How do you want to import the list of default account names?

☒ Import CSV file

File: ...

☐ Manual data entry

Help < Previous Next > Cancel

- 3 If the **Import CSV file** option is selected, click... and browse for a CSV file to import. Select the file and click **OK**.

- 4 Click **Next**.

The second define data panel displays as shown in [Figure 14-14](#).

Figure 14-14 Define Default User Accounts Panel—Second Panel

Define Default User Accounts

Supply the default user accounts and vendor names for your network e.g. scott Oracle. If a CSV file is used, it should contain two columns.

User Account	Vendor Name

Add Remove

Help < Previous Next > Cancel



If you imported data using a CSV file, the data is displayed in the panel.

- 5 Enter values.
- 6 Add additional rows as needed:
 - a Click **Add**.
 - b Enter the data into the new row.
- 7 Click **Next**.

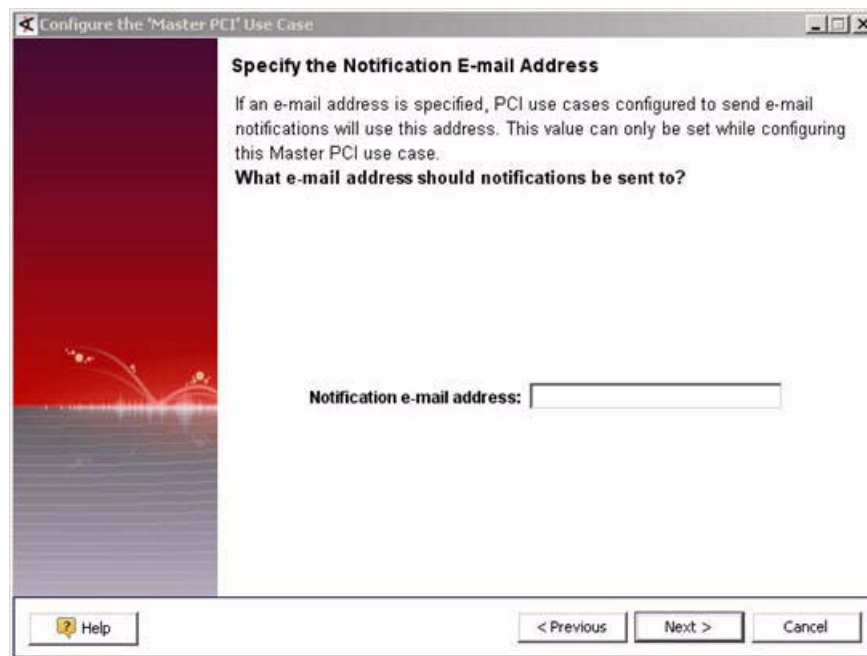
When Next is clicked in the Summary of Settings to Apply panel as described in [“Step 8 - Summary of Settings to Apply Panel” on page 342](#), the new values are added to the existing values already present in the active list. If you specify a value that already exists in the active list, an additional entry is added and the Count for that entry is increased by one.

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Specify the Notification E-mail Address Panel

In the Specify the Notification E-mail Address panel ([Figure 14-15](#)), you are prompted to supply an e-mail address or an e-mail alias (distribution list). If an e-mail address is specified, a notification (alert) is sent to the specified e-mail address when the condition(s) described in the panel are satisfied. For example, the use case could contain a rule that tests when default system accounts are used. Once the rule is triggered, an e-mail notification is sent to the specified email address or distribution list.

Figure 14-15 Notification E-mail Address Panel



The screenshot shows a window titled "Configure the 'Master PCI' Use Case". Inside, there is a panel titled "Specify the Notification E-mail Address". The panel contains the following text: "If an e-mail address is specified, PCI use cases configured to send e-mail notifications will use this address. This value can only be set while configuring this Master PCI use case." Below this is a question: "What e-mail address should notifications be sent to?". At the bottom of the panel is a text input field labeled "Notification e-mail address:". The window has a "Help" button on the bottom left and "< Previous", "Next >", and "Cancel" buttons on the bottom right.



The e-mail address does not have to be an ArcSight ESM user.

In order for notifications to be sent to specified e-mail address, notifications must be configured. For more information, see [“Managing Notifications” on page 482](#) and [“Using Notifications” on page 76](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Specify the Expiration Time Period Panel

In some panels, you are prompted to supply an expiration time period as shown in [Figure 14-16](#). In this example, an account expires if no logins have occurred within the specified time period.

Figure 14-16 Specify Expiration Time Period Panel

The numeric value you specify sets the expiration time period in days. This expiration time period is the Time To Live (TTL) in days for an active list. Entries in the active list expire when the Time To Live (TTL) has been reached. This expiration causes an event to be generated. This event can be used by other ArcSight ESM resources such as filters and rules. For more information, see [“Managing Active Lists” on page 385](#).

For example, in the *PCI 8.5 - Identify Inactive User Accounts* use case, you are prompted to supply the Inactivity Time Period. If you answer 45 days, the Time To Live (TTL) for the *Users Who Accessed Cardholder Data* active list is set to 45 days which means once an account has been on the active list (indicating no activity) for more than 45 days, it expires. This expiration generates an event which triggers the *Inactive User Account Detected* rule.



The value specified in this panel is saved as Time To Live (TTL) in days for the active list. If other resources reference this active list, the change to the TTL value can affect the behavior of other resources listed in different use cases.

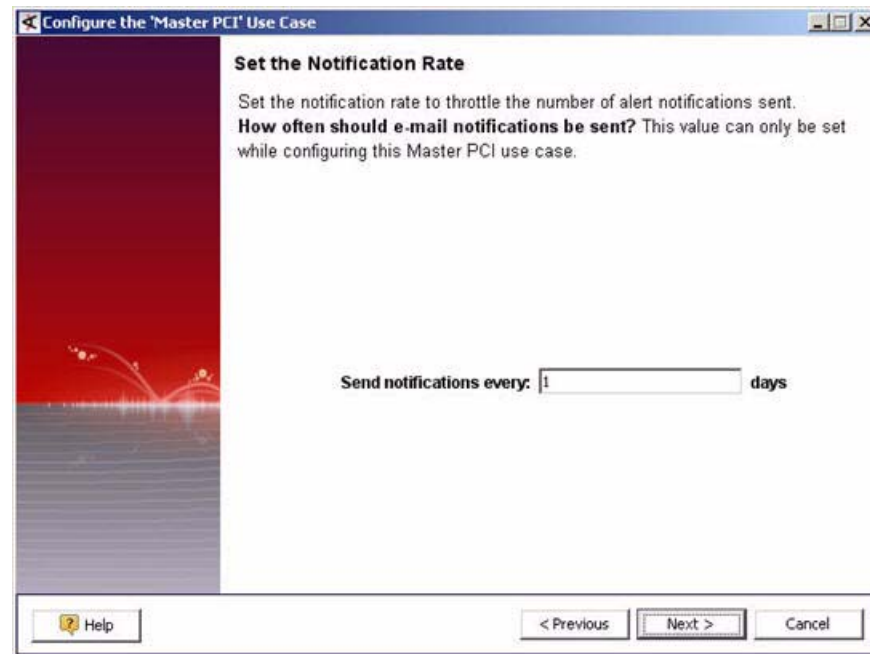
Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Set the Notification Rate Panel

In the *Set the Notification Rate* panel, you are prompted to supply the how often a notification e-mail should be sent—the notification rate. This rate is used to throttle the number of alert notifications sent. The rate specified in this panel sets the Time To Live (TTL) in days for the *Rate Controlled Notifications* active list.

If the notification rate is set to 0, only one e-mail is sent for every issue until the entry is manually removed from the *Rate Controlled Notifications* active list.

Figure 14-17 Set the Notification Rate Panel

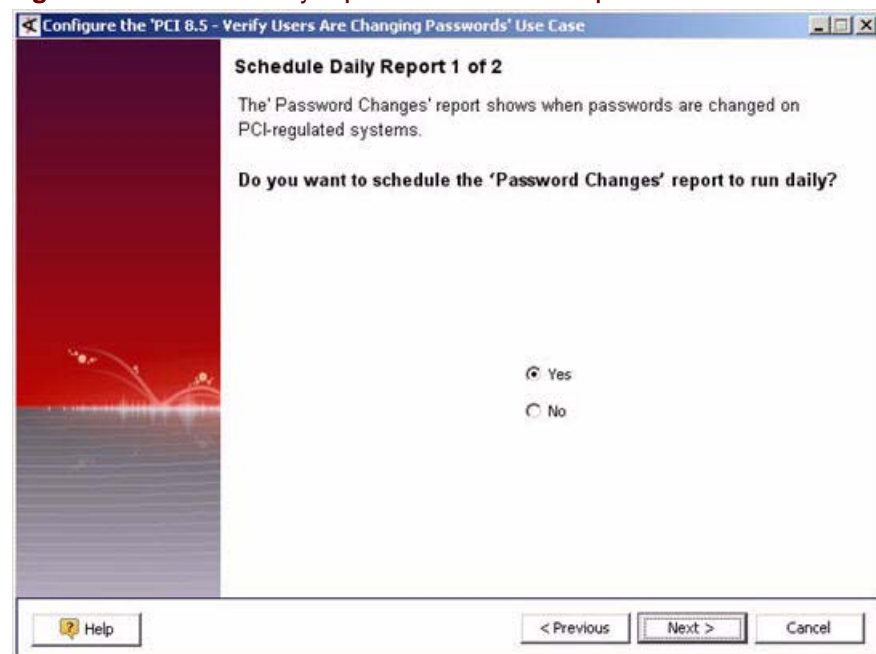


Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 341](#).

Schedule Daily Report Panels

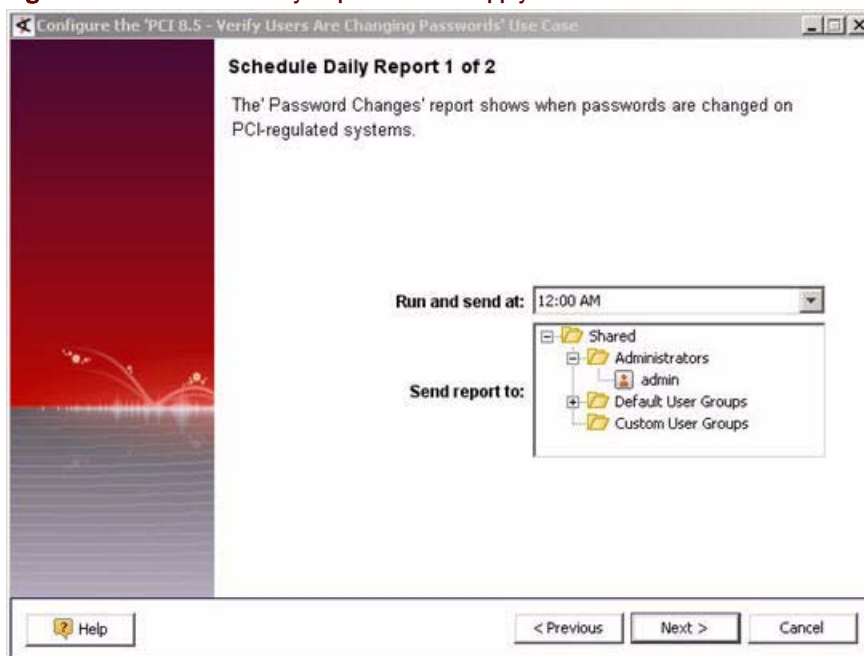
In the **Schedule Daily Report** panel, you are prompted to schedule a daily report, as shown in [Figure 14-18](#).

Figure 14-18 Schedule Daily Report Panel—Schedule Report?



If you answer **Yes**, another panel displays as shown in [Figure 14-19](#).

Figure 14-19 Schedule Daily Report Panel—Supply Values



In the **Run and send at** field, select a time during the day when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see ["Managing Users" on page 438](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

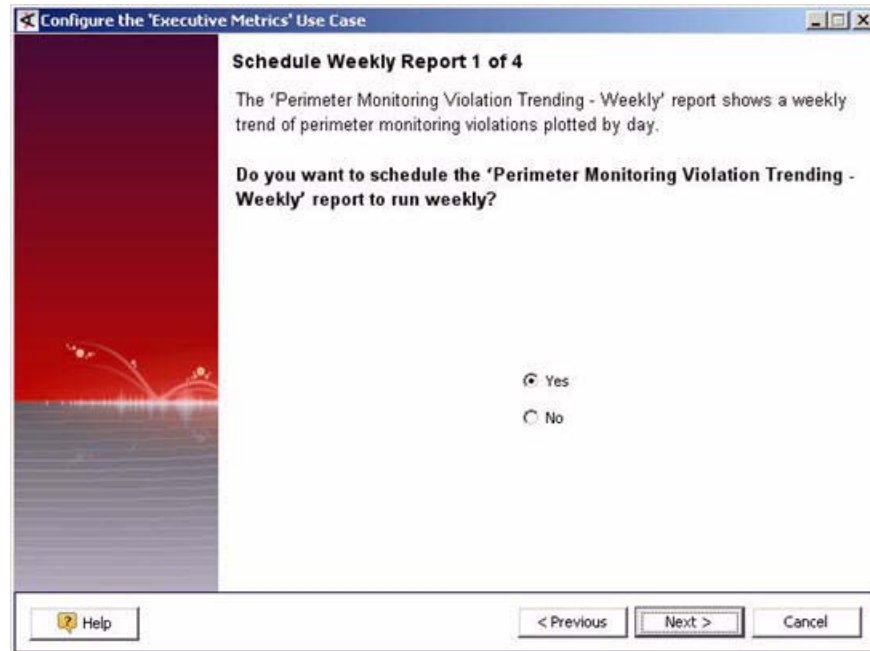
When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run daily. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.

For more information, see [Chapter 12, Running and Managing Reports, on page 287](#).

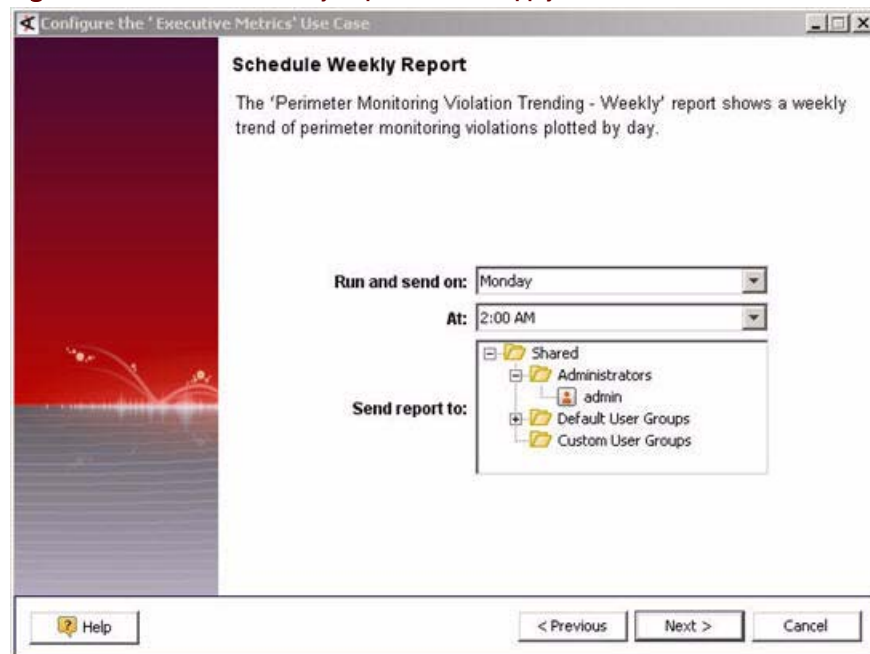
Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 341](#).

Schedule Weekly Report Panels

In the **Schedule Weekly Report** panel, you are prompted to schedule a weekly report, as shown in [Figure 14-20](#).

Figure 14-20 Schedule Weekly Report Panel—Schedule Report?

If you answer **Yes**, another panel displays as shown in [Figure 14-21](#).

Figure 14-21 Schedule Weekly Report Panel—Supply Values

In the **Run and send on** field, select the day of the week when the report should run.

In the **At** field, select a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see [“Managing Users” on page 438](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run weekly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



Weekly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

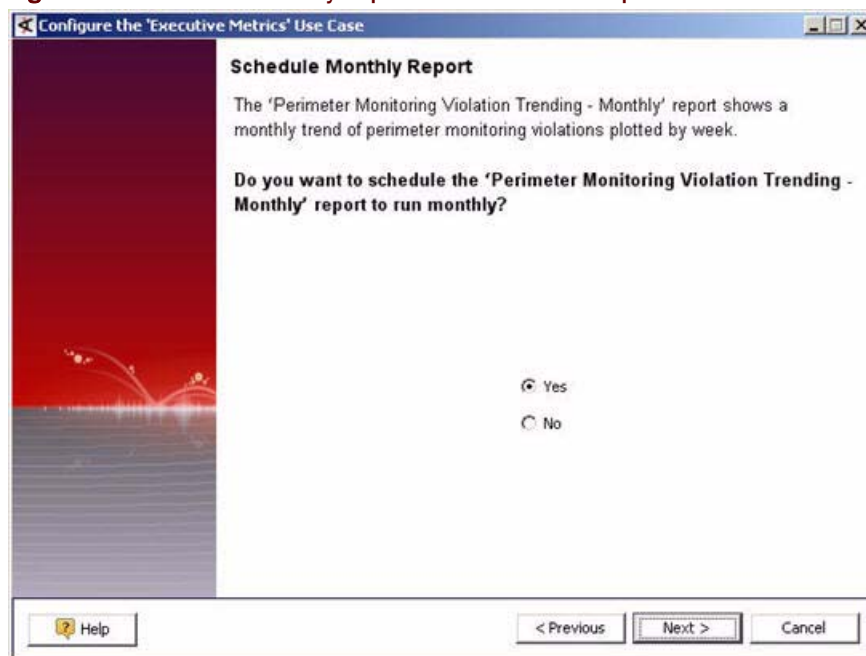
For more information, see [Chapter 12, Running and Managing Reports, on page 287](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Schedule Monthly Report Panels

In the **Schedule Monthly Report** panel, you are prompted to schedule a monthly report, as shown in [Figure 14-22](#).

Figure 14-22 Schedule Monthly Report Panel—Schedule Report?



If you answer **Yes**, another panel displays as shown in [Figure 14-23](#).

Figure 14-23 Schedule Monthly Report Panel—Supply Values

Configure the "Executive Metrics" Use Case

Schedule Monthly Report

The 'Perimeter Monitoring Violation Trending - Monthly' report shows a monthly trend of perimeter monitoring violations plotted by week.

Run and send on: day of each month

At:

Send report to:

- Shared
 - Administrators
 - Default User Groups
 - Custom User Groups

Buttons:

In the **Run and send on** ___ day of each month field, specify the day of the month when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **At** field, specify a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see ["Managing Users" on page 438](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run monthly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



Monthly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

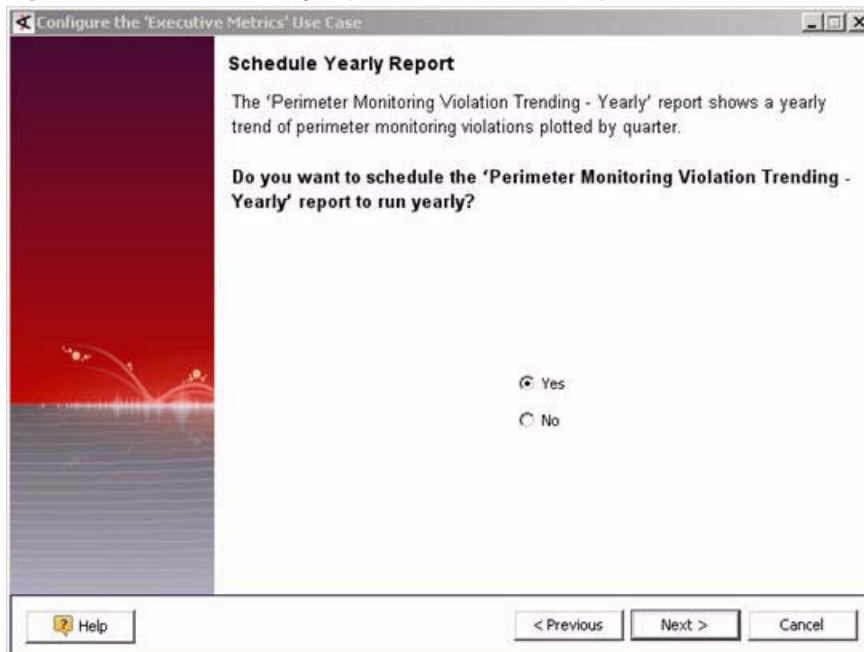
For more information, see [Chapter 12, Running and Managing Reports, on page 287](#).

Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 341](#).

Schedule Yearly Report Panels

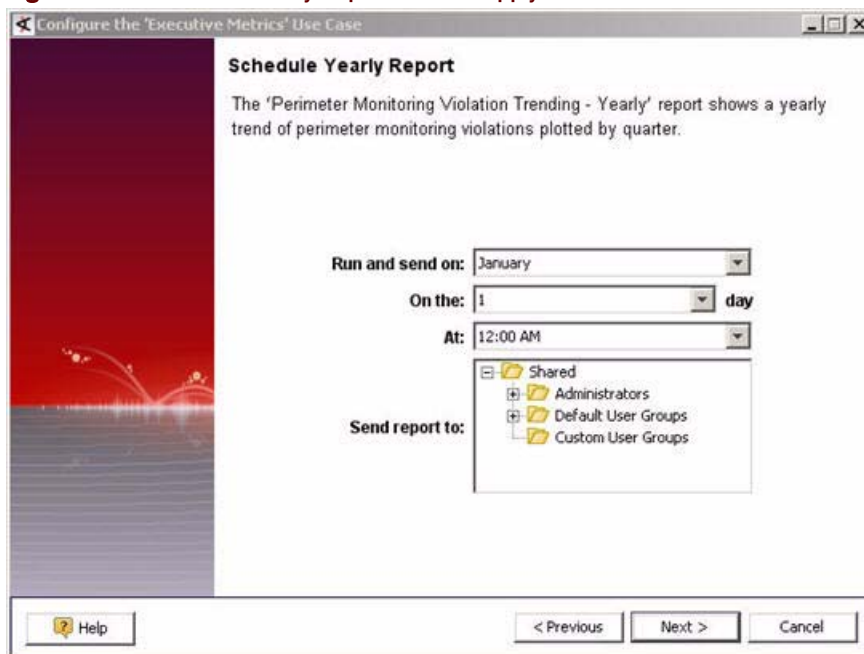
In the **Schedule Yearly Report** panel, you are prompted to schedule a yearly report, as shown in [Figure 14-24](#).

Figure 14-24 Schedule Yearly Report Panel—Schedule Report?



If you answer **Yes**, another panel displays as shown in [Figure 14-25](#).

Figure 14-25 Schedule Yearly Report Panel—Supply Values



In the **Run and send on** field, specify the day of the month when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **On the _ day** field, specify the day of the month when the report should run.

In the **At** field, specify a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see [“Managing Users” on page 438](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run yearly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



Yearly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

For more information, see [Chapter 12, Running and Managing Reports, on page 287](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 341](#).

Chapter 15

Identity Correlation

Identity correlation provides the ability to model users and associate them with events. Identity correlation can be accomplished using **session lists** for some scenarios (*session correlation*) and **active lists** for others (*user or device correlation*).

You can capture and record session-related data in a user-defined *session list* where it can be used for a number of purposes in identifying and tracking users in relation to MAC addresses, IP addresses, machines, network logons, and so forth.

Also, you can use a pre-populated *active list* to find a value and then use the value (as a variable) in a rule. You can use this strategy to identify entities or objects in a variety of scenarios such as correlating various user IDs (logins, email addresses, badge IDs) to unique IDs; mapping unique user IDs to user roles; and even finding the status of a machine by its host name.

The following topics describe scenarios for using both resources, and include step-by-step examples of using sessions lists and active lists with rules and variables for identity correlation.

["Understanding Session Correlation" on page 357](#)

["Managing Session Lists" on page 361](#)

["Using Session Lists to Correlate Session Data on User Logins \(Example\)" on page 365](#)

["Using Active Lists to Correlate Users \(Example\)" on page 375](#)

Understanding Session Correlation

You can leverage ArcSight provided resources (pre-defined [Session Lists](#) and [Rules](#)) or develop customized session lists to use for identity correlation, as described here.

How Session Correlation Works

Session correlation captures and records session-related data in a user-defined list, where it can be used by ArcSight's Correlation Engine to:

- Resolve event endpoints against DHCP sessions to identify which device was located at the reported IP address at the time of the event
- Utilize existing maps that link MAC addresses and/or host names to users, if available
- Attribute actions originating from a specific device to its owner
- Extract and resolve user information from VPN logins, including the VPN user name and session characteristics

- Track who accesses a given network node at a given time to trace events that originate from this device to users that were logged in at the time

Session correlation is a three-step process that involves three or more ArcSight resources.



Figure 15-1 Session Correlation Steps Overview

The user defines a session list, then creates a rule to populate it. The results written to the session list can be used anywhere variables are used, such as to trigger other rules, or to populate active channels, dashboards, and reports.

The high-level steps are:

- 1 Create a session list (as described in [“Creating a Session List” on page 361](#)).
- 2 Create a rule to populate the session list (as described in [“Creating a Session List Rule” on page 358](#)).
- 3 Use the session list output wherever needed (as described in [“Using the Session List Output” on page 360](#)).

See also [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 365](#) for a walkthrough of creating and populating a session list with Windows session information.

Creating a Session List Rule

To create a rule that writes new sessions into your session list or that re-sends session start times to your session list:

- 1 In the Navigator panel's drop-down menu, choose **Rules**.
- 2 In the Rules resource tree, right-click a group and select **New Rule**. The Rules Editor displays in the Inspect/Edit panel.
- 3 At the **General** tab, enter the following values:

In this field...	...enter this
Name	Enter a name in the Rule Name text field. The Rule Name should be as descriptive as possible. It is stored in the Event Name data field and if the rule has a Send to Console action, the Rule Name appears in the Event Name column of the grid view. The Rule Name text field is required and restricted to 25 characters.
Common: External ID, Alias	If this rule will be referenced by an external system, such as Remedy or vulnerability scanner, enter the pertinent external ID information here. If not, leave these fields blank.

In this field...	...enter this
Description	Enter a description in the Description text field. The description should be meaningful and detailed. For example, This rule creates an entry to the DHCP session list when a new DHCP session starts.
Assign: Owner, Notification Groups	If you wish to specify an owner for this resource and to automatically notify other users when this rule is changed, select existing users and notification groups from the drop-down menu. This step is optional.

- 4 At the **Conditions** tab, enter the conditions that indicate a session start and click **Apply**.
- 5 At the **Aggregation** tab, specify the event fields from the session list that you want to have displayed in the event grid when the rule is triggered by the session conditions specified in the Conditions tab. You should probably aggregate all <4> items you specified in your session list so that those values get populated when the event occurs.
- 6 At the **Actions** tab, set the trigger and the action you wish the rule to take when the conditions are met.
 - a Select the trigger you want to apply to this rule. **On First Event** is the default trigger. This determines which occurrence of the session start conditions will trigger the action to write the event to the session list as the session start.

Trigger	Description
On First Event	Triggers the action the first time rule conditions are met.
On Subsequent Events	Triggers the action the second and subsequent times rule conditions are met (not the first).
On Every Event	Triggers the action every time rule conditions are met. This overrides threshold settings.
On Time Unit	Triggers the action based on the time increment specified in the Every... text field in the Add Action dialog box.
On Time Window Expiration	Triggers the action when the threshold settings have expired.
On First Threshold	Triggers the action the first time rule conditions and threshold settings are met.
On Subsequent Thresholds	Triggers the action the second and subsequent times rule conditions and threshold settings are met, not the first.
On Every Threshold	Triggers the action every time rule conditions and threshold settings are met.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See ["Velocity Templates" on page 793.](#))

- b After you have selected a trigger, click **Add** to add an action. **Select Session List | Add to Session List**.

- c In the Add Action dialog box at the Session List drop-down menu, navigate to the session list you created earlier. The parameters you set for the session list are displayed in the Session Field Mapping area.
- d In the Session Field Mapping area at the Start Time field, select which event time stamp you wish to use to record as the official start time.

Start Time	Description
End Time	The time the event ended.
Manager Receipt Time	The time the event arrived at the Manager.

- e For the remaining fields you specified in your session list that have multiple choices, select which value you wish to use for your session list and click **OK**. You can find a description of the data fields, see ["Data Fields" on page 633](#).
- 7 When all parameters are entered, click **OK**. The relevant events matching this rule will now populate the session list.

Using the Session List Output

Once the session list has been populated by events that trigger the session list rule, the session data can be accessed anywhere variables can be used:

- Active channels
- Data monitors
- Dashboards
- Filters
- Reports
- Rules

Creating a Variable

From the editor of one of the resources (active channel, data monitors, dashboards, filters, reports, rules), you can create a variable. This variable will be derived from the session time-stamp data stored in the session list.

To create a variable:

- 1 In the Navigator panel's drop-down menu, choose the resource that you wish to consume the session list data. These steps will use Filters as an example. Right-click a filter group and select New Filter.
- 2 At the Attributes tab, enter a name for the filter, and optionally, external ID and alias information, and/or owner and notification group information.
- 3 At the Variables tab, click **Add**. In the "Add Dependent Variable" dialog, enter the following values and click **OK**:

In this field...	...enter this
Name	Enter a name for the variable. This name appears in the <Lists> menu available from the Common Conditions Editor . Spaces and special characters are OK.
Function	In the Function pull-down menu, select List Functions > GetSessionData .

In this field...	...enter this
Arguments	In the <field name> pull-down menu, select the session list you created previously.
More Options	
Preview	To preview the results, select an asset from the list of assets reporting events to ArcSight and click Calculate .

- 4 Perform any necessary Session Field Mapping.
- 5 In the Filters tab conditions editor, scroll down to the bottom of the Fields list until you see Variables. Here you will see the name of the variable you created in [Step 3](#). In the Operator field, select an operator appropriate for the GetSessionFunction variable you created in [Step 3](#). In the Condition field, enter an appropriate value. Session lists that allow overlapping sessions would take a list of values separated by commas. Session lists that do not allow session overlapping would take a single value. This instructs the filter to derive its values from your session list.
- 6 When you have finished setting all the conditions, click **Apply** to save changes and keep the editor open; click **OK** to save the filter and exit the editor.

Populating a Session List Manually

Session lists are really designed to be populated automatically by rule actions, however, there may be times when you need to populate the list manually. For example, you may wish to enter known values to your session list for testing purposes, or to get session correlation started with known values while you are waiting for the event stream to populate the list with more session-related values.

To manually add data to the session list you just created, see [“Adding a Session List Entry” on page 364](#).

Managing Session Lists

While you can manually update session lists, their real value comes when you author automatic, rule-driven lists with dynamic content.

See also [“Understanding Session Correlation” on page 357](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 365](#).



As described in [“Creating a Session List” on page 361](#), filters improve session list performance by restricting the number of events that must be evaluated. Filters, such as DHCP IP address ranges, are installation-specific. Therefore, consider adding a filter to pre-defined session lists, such as /All Session Lists/ArcSight Foundation/Network Monitoring/DHCP, to improve performance.

Creating a Session List

Note that session lists are usually defined in conjunction with rules specifically tailored to interact with those lists dynamically. Lists not driven by rules will be empty or contain only manually added entries that have not timed out.

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Session Lists** tab.

- 3 Right-click a session list group and choose **New Session List**.
- 4 In the Session List Editor, in the Inspect/Edit panel, define the following values.

In this field...	...enter this
Name	Enter a name for the session list. This name identifies the session list in ArcSight pick lists. Spaces and special characters are OK.
Overlapping Entries	Check this box to alert the system to allow multiple instances of key pairings, which keeps the previous session with the same key field open. For example, you might check this box if the list will be tracking activity for an asset that supports multiple-user logins.
In Memory Capacity (x1000)	This setting indicates the maximum number of session entries the system will keep in memory. 10,000 is the default value. For most cases, 10,000 will be appropriate, however, you may wish to adjust this setting if the devices you are monitoring for this session list contain a lot of data to ensure you have adequate memory cache available.
Entry Expiration Time	Enter an expiration time for session list entries. This indicates the time after which entries are marked as terminated (if no explicit termination event is received previous to this). The default is 0 seconds, which means the entry will never expire. An entry with no expiry date/time can only be terminated explicitly (through user action on Console, rule actions, or archives).

- 5 Set the **Common** and **Assign** fields as appropriate.
- 6 Define columns for session list entries by clicking on the row of the lower panel labeled "<Enter Name>." Columns for Start Time, End Time, and Creation Time are pre-defined.

In this field...	...enter this
Name	Enter a name for each session parameter you wish to track; for example, IP address, zone, or MAC address. The name you enter here will appear as a label in the session list, and in the Variable pick list. Names can contain spaces, such as "User name."
Type	Type indicates the data type of the entry. Data types can be: Address (IP address or MAC address) <ul style="list-style-type: none"> • Date • Double • Integer • Long • Resource Reference (with appropriate subtype) • String

In this field...	...enter this
Subtype	<p>There are only two data types that require subtypes: Address and Resource reference.</p> <ul style="list-style-type: none"> • Address – Choose IP address or MAC address. • Resource reference – A Resource reference can refer to any resource, such as Asset, Knowledge Base Article, or Zone.
Key Field	<p>Select one or more fields that must be unique to indicate a session start. In most cases, you would select at least two fields to make a key-value pair. For example, in the case of a DHCP login event, when a new IP and zone combination are written to the list, this indicates that a new session has started.</p>

Columns can only be defined when the session list is created. Column definitions cannot be added, removed, or changed once the new session list is saved.

- 7 Click the **Filter** tab in the Session List Editor and define a filter that limits the number of events that will be considered for the new session list. Session lists without filters must evaluate every event, which can negatively affect performance. The Filter tab presents the familiar [Common Conditions Editor](#). Although the filter editor is similar, session list filters are not the same as Filter resources. Session list filters use different fields than Filter resources, for one thing.

Session lists are often concerned with logins to specific machines. In this case, you would write a filter that would limit evaluation to IP address ranges of interest. By filtering out all events except those targeting IP addresses in the DHCP server's subnet, for example, you are effectively limiting session list evaluation to inside traffic, reducing the overhead of session list evaluation. Other uses of session lists will suggest other installation-specific knowledge that can be used to create session list filters that restrict the number of events matched against the session list.

Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entry** button in the Session List Editor to manually create more entries for the current session list.

Editing Session Lists

- 1 In the Session Lists resource tree, right-click a session list and choose **Edit Session List**.
- 2 Make appropriate changes to the properties of the session list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Moving or Copying Session Lists

- 1 In the Session Lists resource tree, navigate to a session list and drag and drop it into another group.
- 2 Choose **Move** to move the session list, **Copy** to make a separate copy of the session list, or **Link** to create a copy of the session list that is linked to the original session list.

If you choose **Copy**, you create a separate copy of the session list that will not be affected when the original session list is edited. If you choose **Link**, you create a copy of the session list that is linked to the original session list. Therefore, if you edit a linked session

list, whether the original or the copy, all links are edited as well. When deleting linked session lists, you can either delete the selected session list or all linked session list copies.

Exporting Session Lists

In the session list viewer, you can export selected entries from an session list to a CSV file. This is useful if you want to manage session list data external to the console.

- 1 In the Session Lists resource tree, select a session list, and choose **Show Entries**. The data in the session list is displayed in the Viewer panel as session list details.
- 2 On the session list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting Session Lists

- 1 Right-click a session list and choose Delete Session List.
- 2 In the dialog box, click Delete.

Adding a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click an entry that is similar to the entry you would like to add. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to post the changed entry as a new one.

Adding a Session List Entry Based on an Existing Entry


- 1 Right-click an item in the Session List resource tree and choose **Edit Session List**. The Session List Entry editor appears in the Inspect/Edit window.
- 2 Click the **Add Entry** button.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to save the new entry. The **Reset** button clears all values.

Deleting a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to delete. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click the entry's **Value** to make changes. The column type may limit the kind of data that can be entered.

- 4 Click **Add** to post the changed entry as a new one.

Terminating a Session List Entry

- 1 In the Session Lists resource tree, right-click a session list and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to terminate. Choose **Terminate Session Entry**.
- 3 Enter the date and time for the session end time. Click the  button for a context menu containing relative times such as Now, 1 hour ago, 1 day from now, and so on. Click **OK**.

Using Session Lists to Correlate Session Data on User Logins (Example)

Using session lists for identity correlation is a three-step process that involves three or more ArcSight resources. The high-level workflow for creating and using session lists for identity correlation is:

- 1 Create a session list.
- 2 Create a rule to populate it.
- 3 Use the session list output.

The results written to the session list can be used anywhere variables are used, such as to trigger other rules, or to populate active channels, dashboards, and reports.

This Help topic steps through an example of building and populating a session list to track Windows user login sessions.

(For a full explanation of working with session correlation, see the overview list of topics in [Chapter 15, Identity Correlation, on page 357](#).)

Example Overview

This example shows you, first, how to create a session list (essentially, a container) with a schema appropriate for storing information about Windows logins and logoffs.

Next, we create two rules to populate the session list:

- A rule that is triggered at start of a successful Windows login and populates the session list with the successful login event data
- A rule that is triggered when a user logs off and populates the session list with the session termination event data

Then, we verify the rules using the Verify Rules with Events tool to make sure that the rules are triggered and that your session list is populated appropriately with session logins and start/end times.

Finally, we create a new report using the session list you just created as the data source, and run the report.



You will need a set of canned or live Windows session events (user logins/logoffs) to properly verify the resources you create for this example.

1. Create a Session List to Store Windows Sessions

Start by creating a session list that will serve as a container for Windows login sessions.

Choose the **Lists** resource in the Navigator, and click the **Session List** tab. Right-click a user folder and choose New Session List. (For more detailed help on creating session lists, see ["Creating a Session List" on page 361](#).)

In the Session List editor, name the session list, and add the fields as shown.

Session List Attributes	Value
Name	Windows Login Sessions
Overlapping Entries	Disabled (leave unchecked) This example assumes that the Windows server we are monitoring does not support multiple-user logins, which is why we leave Overlapping Entries unchecked.
In MemoryCapacity(x1000)	10



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 552](#).

Add the following three fields with names and types as shown. Set "Username" as the key-field.

Field Names for Session Lists	Type	Key Fields
Username	String	Enabled
NT Domain	String	
Device	String	

Session List Name

Disable Overlapping Entries if server does not support multi-user logins

Fields: The session list will include these fields. Username, marked as the Key-field, must be unique to indicate a session start.

Name	Type	Sub-type	Key-field
Username	String		<input checked="" type="checkbox"/>
N T Domain	String		<input type="checkbox"/>
Device	String		<input type="checkbox"/>

2. Create Rules to Populate the Session List with Windows Logins

Create two rules with which to populate the session list:

- A rule that triggers on Windows session logins
- A rule that triggers when a Windows session terminates

To create a new rule, choose the Rules resource from the Navigator drop-down menu, right-click a user group, and select New Rule from the context menu. (If you need more help on creating rules, see [“Managing Rules” on page 302](#). For a general introduction to working with rules, see [Chapter 13, Rules Authoring, on page 301](#).)



For this example, first create rules in a user folder under Rules for testing purposes. Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. Only rules deployed in Real-time Rules will filter on live events and show up in a live channel when they are triggered. See [“Deploying Real-time Rules” on page 329](#) for more information.

Rule 1: Triggers on Windows Session Logins

Create a rule to populate the session list. Use the following attributes, conditions, aggregation, and actions as shown below.

Attributes

On the **Attributes** tab, enter the name of the session login rule as follows.

- **Name:** Successful Windows Login

The screenshot shows the 'Inspect/Edit' window for the rule 'Successful Windows Login'. The 'Attributes' tab is selected. The rule details are as follows:

Rule	
Name	Successful Windows Login

Common	
Resource ID	5+DQZ8Q0B8CAEKKAQjivLA==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

Assign	
Owner	
Notification Groups	

Parent Groups	
Vicky's Rules	/All Rules/Personal/Vicky's Rules/

Creation Information	
Created By	Vicky
Creation Time	27 Sep 2006 14:05:35 PDT
Time Since Creation	2 day(s) 3 hour(s) 32 min(s) 35 sec(s)

Last Update Information	
Last Updated By	Vicky
Last Update Time	27 Sep 2006 17:06:13 PDT
Time Since Last Update	2 day(s) 31 min(s) 57 sec(s)

Conditions

Click the **Conditions** tab for the login rule, and enter the following conditions.

- Target User Name Is NOT NULL
- Target Nt Domain Is NOT NULL
- Device Host Name Is NOT NULL

Setting these conditions will cause the rule to be triggered on any event that includes a device host name and a user name where the target is a Windows NT domain. (For more information on using the Common Conditions Editor or "CCE", see ["Common Conditions Editor"](#) on page 616 and ["Conditional Statements"](#) on page 625.)

The screenshot shows the 'Inspect/Edit' window for the 'Rule Editor'. The 'Conditions' tab is selected. The conditions are defined as follows:

```

graph TD
    event1[event1] -- AND --> C1[Device Host Name != NULL]
    event1 -- AND --> C2[Target Nt Domain != NULL]
    event1 -- AND --> C3[Target User Name != NULL]
  
```

The bottom section shows a table for field sets:

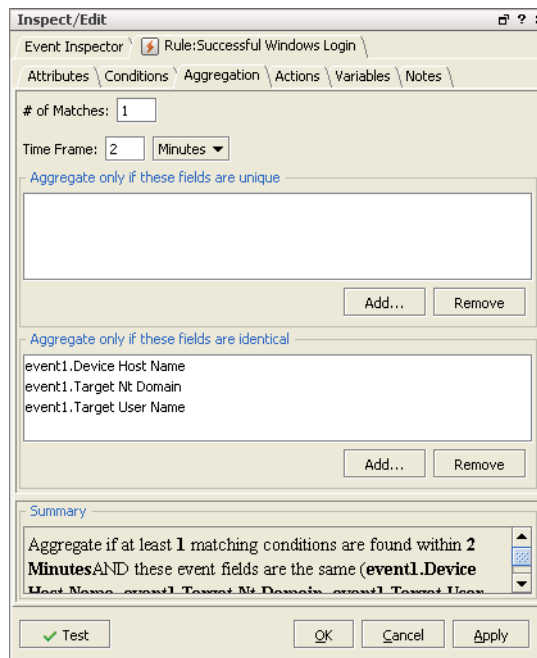
Name	Op	Condition
Device Asset Local ID		
Device Direction		

Aggregation

Click the **Aggregation** tab for the login rule. Under **Aggregate only if these fields are identical**, click **Add...** to bring up the Add Fields dialog. Select the following fields on which to aggregate and click OK to add them to the rule.

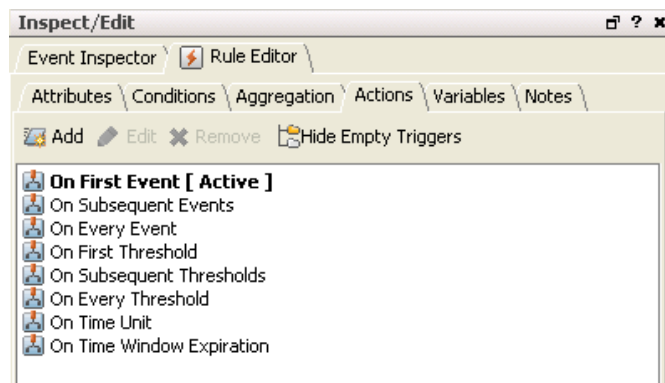
- Target User Name
- Target Nt Domain
- Device Host Name

Aggregation can be used to combine multiple events (as specified in the number of matches) into a single entry for the session list. But in this case (where we are aggregating events with identical fields on only a single match), we are specifying fields in the Aggregation tab for the purpose of making those same fields available in the Actions tab.



Actions

Click the **Actions** tab for the login rule.



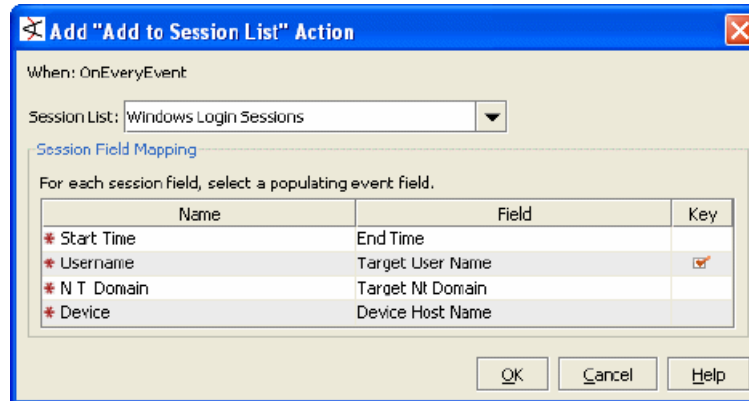
Select **On Every Event**, and click **Add | Session List | Add to Session List**.

In the Session List drop-down menu on the Add dialog, select the Windows Login Sessions session list you created in the first step.

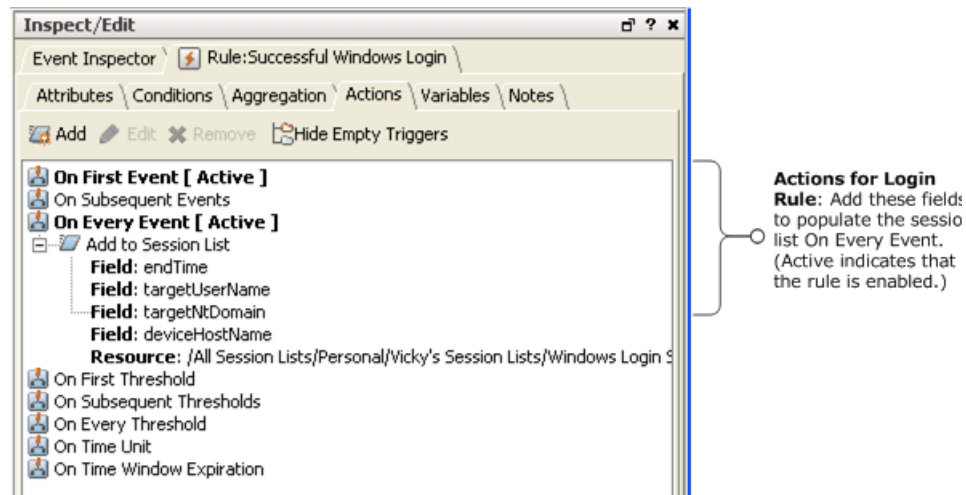
Map the fields as follows.

- Start Time: End Time
- Username: Target User Name
- NT Domain: Target Nt Domain
- Device: Device Host Name

This will prompt the rule to add a login event to the Windows Login Sessions list every time a matching login event occurs.



Click **OK** on the Add to Session List dialog to add the actions to the rule. When the actions are properly configured, they are displayed under the "On Every Event" action as shown. Windows session logins will be added to the session list on every event.



Click **OK** to save the session login rule.

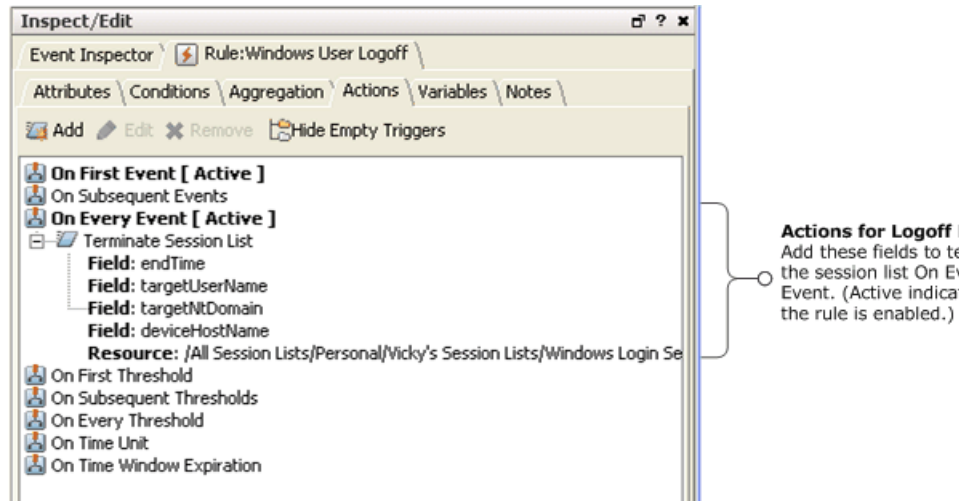
Rule 2: Triggers on Termination of Windows Sessions

Create a rule to populate the session list with Windows session termination information. Define this "terminate session list" rule with the same settings as the "add to session list" rule you just created, with the following differences specific to terminating the session:

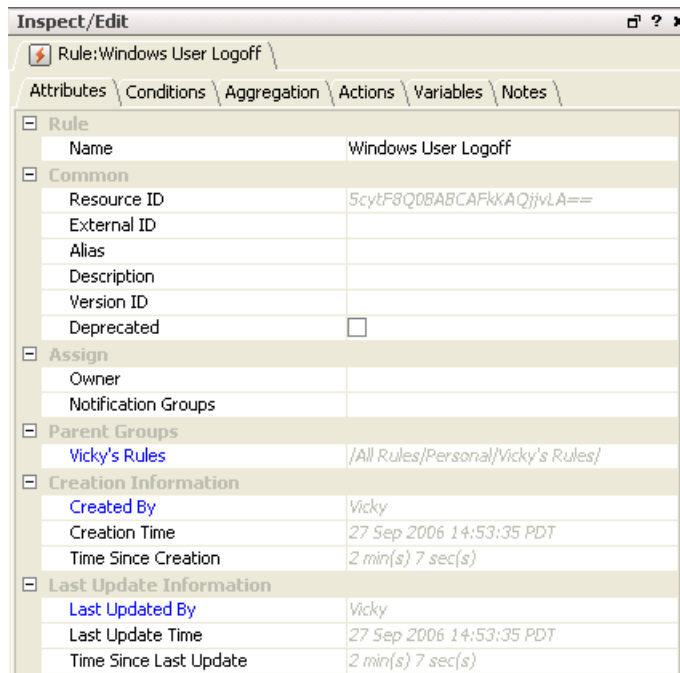
- On the **Attributes** tab, Rule Name is Windows User Logoff (instead of Login)
- On the **Conditions** tab, define the same Conditions as in the previous rule.
- On the **Aggregation** tab, aggregate on the same fields as in the previous rule.

- On the Actions tab, define the same actions as in the previous rule but add the actions to **Terminate Session List** instead of Add to Session List. (The menu path for adding the logoff rule is **Add | Session List | Terminate Session List**.)

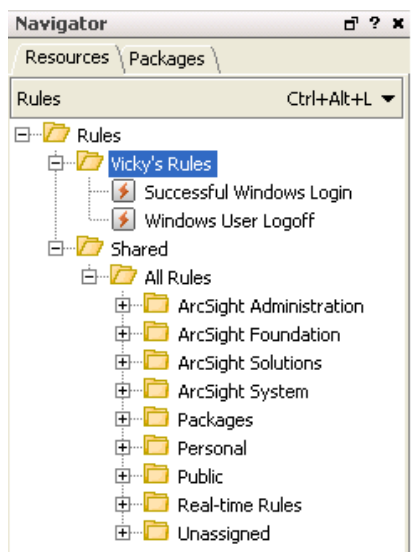
The **Actions** tab for the logoff rule is shown below. Notice that for Windows logoffs, the rule triggers the action to add an entry to the terminate session list on every logoff event.



Here is an example of the **Attributes** tab for the logoff rule when it is completely configured.



3. Verify Rules



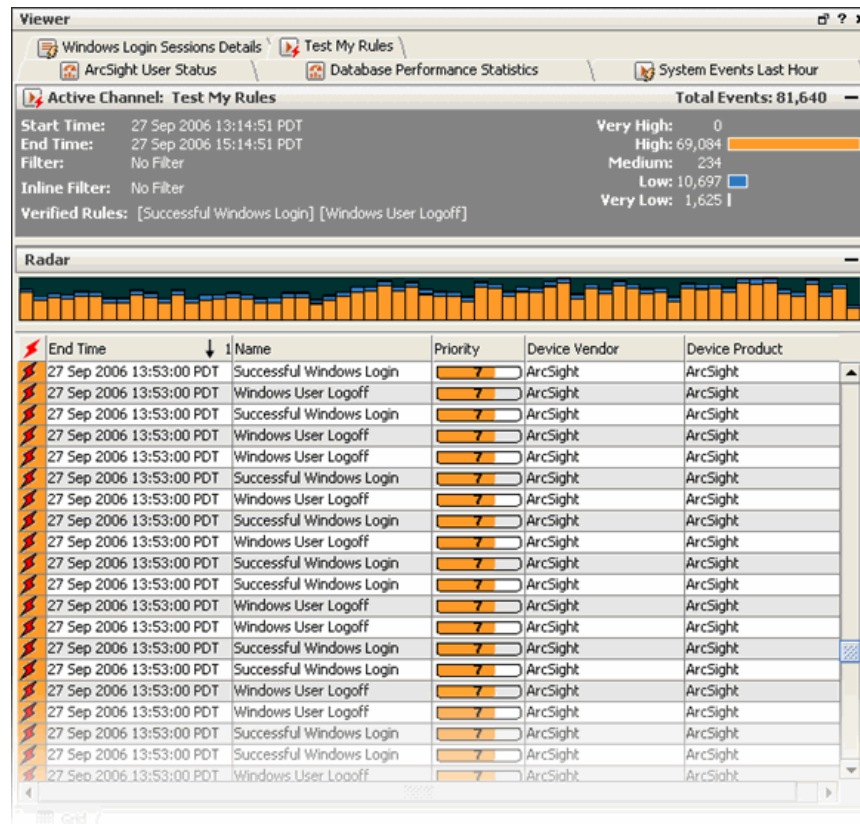
For each rule, we want to answer some key questions to verify the rules are working as expected.

Rule	Verify Questions
Add to Session List	Is the rule triggered when a Windows logon occurs? Are the values inserted into the Session List?
Terminate Session List	Is the rule triggered when a Windows logoff occurs? Is the End Time in the Session List changing according to the rule (that is, is it terminating the session for this user)?

To test the rules before deploying in real time, we can use an active channel created from the Verify Rule(s) with Events option, and also view entries in the Windows Login session list we created in the first step of this example.

- 1 Select the Rules folder that contains them, right-click, and choose **Verify Rule(s) with Events** in the context menu. You can create a New Active Channel to test the rules.

The following example shows the login rule triggered for several events.



- 2 Choose the **Lists** resource in the Navigator, and click the **Session Lists** tab. Select your **Windows Login Sessions** list, right-click, and choose **Show Entries** from the context menu.

Viewer				
Windows Login Sessions Details				
ArcSight User Status Database Performance Statistics Windows Login Sessions Details Test My Rules				
Name: Windows Login Sessions			2,000 shown / 3,100 matches	
Filter: No Filter				
Username	N T Domain	Device	Start Time	End Time
jarrod		orangeblast	27 Sep 2006 13:43:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:44:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:45:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:46:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:47:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:48:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:49:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:50:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:51:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:52:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:53:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:54:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:55:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:56:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:57:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:58:19 PDT	27 Sep 2006
jarrod		orangeblast	27 Sep 2006 13:59:19 PDT	27 Sep 2006
lucy		johnnyquest	27 Sep 2006 14:00:04 PDT	27 Sep 2006
lucy		johnnyquest	27 Sep 2006 14:00:04 PDT	27 Sep 2006
lucy		orangeblast	27 Sep 2006 14:00:04 PDT	27 Sep 2006

For more information on testing rules, see [“Verifying Rule\(s\) with Events” on page 326](#) (formerly Replay-with-Rules).



Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. Only rules deployed in Real-time Rules will filter on live events and show up in a live channel when they are triggered. For more information, see [“Deploying Real-time Rules” on page 329](#).

4. Use the Session List in a Report

You can leverage session lists in a variety of resources including reports, active lists, active channels, data monitors, and as input to other rules. (For example, you could use a rule to correlate multiple failed VPN logins over a short timeframe with a particular user entry in the session list. You might specify that if both conditions are met, add the user to an active list such as /Active Lists/Shared/All Active Lists/ArcSight System/Threat Tracking/Suspicious List.)

For this example, use the session list in a simple report.

Create a new report on the session list for this example. The steps are:

- Create a report
- Choose a report template
- Choose the session list as the data source for the report
- Run the report

Here are step-by-step instructions for creating a report showing the Windows logins

- 1** In the Navigator, choose the **Reports** resource and click the **Templates** tab.
- 2** Expand the folder /Report Templates/Shared/All Report Templates/ ArcSight System/, right-click **Simple Table Portrait** and choose **New Report from Template**.
- 3** Provide a name for the report (for example, Windows Login Sessions).
- 4** Click the **Data** tab and select Session Lists for the Data Source type and the Windows Login Sessions list for the data source.
- 5** Click Apply or OK to save the report.
- 6** Still under the Reports resource in the Navigator, click the **Reports** tab. The report you created is displayed under your user folder.
- 7** Select the new report, right-click and choose **Run Report** or **Run Report with Defaults** from the context menu.

Following is an example of an HTML version of the Windows Login Sessions report.

Report					
Username	N T Domain	Device	Start Time	End Time	Creation Time
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15		Sep 27 2006 16:23:06
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55

For more information on creating and using reports, see [“Creating Reports” on page 251](#) and [“Running Reports” on page 287](#).

Using Active Lists to Correlate Users (Example)

You can use active lists to find a value and then use value (as a variable) in a rule. You can use this strategy to identify entities or objects in a variety of scenarios; for example:

- Given that logins from the same attacker are showing up under multiple IP addresses, find out whether the attacks are coming from the same machine with different IP addresses.
- Correlate user logins (e.g., onto server machines) with physical building or room entry. A user's login ID is not the same as badge ID. You use an active list to map various user identifiers (login, e-mail, badge) to a unique user ID (UUID) for each user.
- Map UUIDs to user roles.
- Find the current status (e.g., up, down) of a given machine host name.

- Find the current status (e.g., up, down) of a given SmartConnector.

(The last two can be handled using data monitors also.)

This example shows how to build a rule that leverages unique user ID information from a pre-populated active list to correlate user logins on critical servers with badge swipe entries to the server room. The rule is triggered when a server user login does not have a matching badge swipe ID.

The example highlights how an active list with values can be leveraged for identity correlation. In this case, the active list collects target user IDs for the same user from different sources (e.g., user login, badge ID, e-mail address, phone number) and maps those different IDs to a unique user ID. The rule then uses the unique user ID to correlate badge swipe IDs with user login IDs.

(For a full explanation of working with identity correlation, see the overview list of topics in [Chapter 15, Identity Correlation, on page 357](#). For more about active lists, see also [“Managing Active Lists” on page 385](#), [“Case-Insensitive Lookup in Active Lists” on page 386](#), and [“Using Rules to Populate an Active List” on page 387](#).)

Example Overview

For this example, consider a scenario where server machines with critical data reside in a secure area. Only users in a specialized group are allowed physical access to the server room (with badge swipe on a card reader) and user login permissions to the servers. This example assumes a policy against remote logins to the server room machines.

We want to use ESM to monitor and correlate user access to the server room (badge swipes) and user logins on the server machines, and take action (e-mail notification) if our access policies are violated. Some examples of policy violations that we want to catch are:

- Cases where someone logged into a server but no badge swipe is registered. This could indicate policy violations such as remote logins or unauthorized server room entry (e.g., server room door was left open)
- There is no matching badge swipe ID for a server console login (e.g., a user stole someone's badge to get into the server room, then logged in to the server with a different user ID)

This example assumes a pre-populated active list with values with a schema appropriate for storing information about user IDs. The active list will key off of user identifiers from various sources (e.g., user login, e-mail address, phone number) and map these variants to the same unique user ID (UUID).

The UUID can then be used as a variable in a rule for correlating user login IDs with badge IDs. We'll show how to create this rule, which leverages the user information collected in the active list.

1. Build and Populate the Active List with User IDs

This example assumes that you have a pre-populated active list that maps user identifiers from various sources (badge ID, user login, e-mail, phone number) to unique user IDs (UUIDs). For the purposes of the example, we are interested in correlating badge IDs and user logins for users who log into critical servers. The active list (populated with our list of users) provides the “User Map” we need to derive each user's unique ID.

The active list definition includes the following two fields with names and types as shown. “User Identifier” is set as the key-field. This information will be available in incoming events

(badge swipes and user logins). Each user identifier is mapped to a UUID. Assume, for this example, that we got this mapping from IT or Human Resources departments. The UUID value is the information we'll want to extract from this list via a variable.

Field Names for Session Lists	Type	Key Fields
User Identifier	String	Enabled
UUID	String	

Active List Name

Fields: The active list includes these fields. User Identifier, marked as the Key-field, is the value returned from various sources (badge, user login, etc.).

The unique user ID (UUID) that the user identifier maps to is provided here through an LDAP system, or some other data source. This is the focus of this active list; to map various user IDs to this UUID. The UUID will be used as a variable in a rule.

Populating an Active List with User Data

There are various ways to populate an active list with this kind of user information:

- Human Resources (HR) or IT database
- Identity management system
- Import from a spreadsheet (in the Navigator, right-click the active list and choose **Import CSV File**. See [“Importing an Active List” on page 390](#))

■ Manually add names to the list



Note that this is a different type of task than populating an active list based on data gleaned from events (e.g., [“Using Rules to Populate an Active List” on page 387](#)).


In this example, we *already have the “map” and the values we need (the unique user IDs) provided in the active list*, and we are going to feed them into a rule as a variable.

In the other example (using rules to populate the active list), we are using a rule to add items to an active list and to discover and use values as items are added to the list.

Here is an example of an active list pre-populated with user information.

User Identifier	UUID	Creation Time	Last Modified Time	Count
badge0123	SamanthaStevens	3 Feb 2009 18:21...	3 Feb 2009 18:21...	1
badgeID4156	StephanieMartinelli	3 Feb 2009 18:17...	3 Feb 2009 18:17...	1
badgeID5245	RobertJackson	28 Jan 2009 16:3...	3 Feb 2009 18:18...	1
rjackson	RobertJackson	28 Jan 2009 16:3...	3 Feb 2009 18:18...	1
rjackson@xyz.com	RobertJackson	4 Feb 2009 15:50...	4 Feb 2009 15:50...	1
samstevens	SamanthaStevens	3 Feb 2009 18:21...	3 Feb 2009 18:21...	1
samstevens@abc.com	SamanthaStevens	4 Feb 2009 15:49...	4 Feb 2009 15:49...	1
stephmartinelli	StephanieMartinelli	3 Feb 2009 18:17...	3 Feb 2009 18:17...	1
stephmartinelli@xyz.com	StephanieMartinelli	4 Feb 2009 15:50...	4 Feb 2009 15:50...	1

If you want to follow along with the example but don't have a database or spreadsheet of user information handy, you can manually add example data:

- 1 Build and save the User Map active list definition as described in [“1. Build and Populate the Active List with User IDs” on page 376](#).
- 2 In the Navigator, right-click the User Map active list and choose **Show Entries**.
The list is shown in the Viewer panel.
- 3 Click the Add Entry button  at the top right of the list to get the Active List Entry Editor.
- 4 Use the Active List Entry Editor to manually add user identifiers and unique user IDs. Click **Add** on the editor to add each line of data. To support the example, add at least two lines for each user. Keep the UUID the same, but the user identifiers different to illustrate the mapping.

User Identifier	UUID
badge0123	SamanthaStevens
samstevens	SamanthaStevens
badgeID5245	RobertJackson
rjackson	RobertJackson

2. Create a Rule that Uses Active List Values to Correlate User IDs

Now that we have an active list that maps various user IDs to unique user IDs (UUIDs), we can create a rule that makes use of the active list to correlate events coming from the same user with different user IDs (such as a badge swipe ID and a server login ID).

The following sections show how to define this example rule.

Attributes

On the **Attributes** tab, provide a name for the rule.

- **Name:** Server Room Console Login Policy

Variable

Next, we'll define a variable we can use to find unique user IDs (UUIDs) in the active list we created in the previous step ("[1. Build and Populate the Active List with User IDs](#)" on [page 376](#)).

Create a variable called `UserMap`. (Click the **Variables** tab for your rule and click **Add** to begin). Provide these values for the variable definition.

Option	Specify this Value
Name	<code>UserMap</code>

Option	Specify this Value
Function	<p>GetActiveListValue</p> <p>Use the drop-down menu to navigate to this function, which is found under "List Functions".</p>
List	<p>UserMap</p> <p>This is the active list we created in the previous step ("1. Build and Populate the Active List with User IDs" on page 376).</p>
User Identifier (Active List Key field mapping)	<p>Target User ID</p> <p>Use the pull-down under "Field" to select Target User ID event field.</p> <p>For matching events, the rule will use the value in the Target User ID field as a lookup key in the active list.</p> <p>For example, if the Target User ID is a login ID of "samstevens", a badge ID of "badge0123", or an e-mail address of "samstevens@abc.com", all of these will resolve to a unique user ID of "SamanthaStevens" in the active list mapping. The variable value passed to the rule to be evaluated in a condition would be SamanthaStevens, the UUID for any of those user identifiers.</p>

The following figure shows the example variable definition on the Add Variable dialog.

Add Variable

Name: UserMap

Function: GetActiveListValue

Retrieve ActiveList value

Arguments

List: User Map

Field Mapping

For each key field, select a matching event field.

Name	Field	Key
User Identifier	Target User ID	<input checked="" type="checkbox"/>

Preview

Set a value for each key field.

Name	Value
Key Fields	
User Identifier	

Calculate

OK Cancel Help

Click **OK** to save the variable.

The new variable is listed on the Variables tab as shown below.

Rule: Server Room Console Login...

Attributes Conditions Aggregation Actions **Variables** Notes

+ Add... Edit Remove

Name	Expression
UserMap	get_activeList_value("/All Active Lists/User Map")

Conditions

We define the rule conditions so that each time a server machine login occurs, the rule conditions are evaluated. (The `ServerRoomConsoleLogin` condition causes this to happen.)



For more information on using the Common Conditions Editor (CCE), see ["Common Conditions Editor" on page 616](#) and ["Conditional Statements" on page 625](#).

A comparison (`Matching Event`) is made between server room logins and badge swipe IDs in a 2-minute time window. The matching event uses our `UserMap` variable (see ["Variable" on page 379](#)) to get the unique ID from the active list we built in the previous step (["1. Build and Populate the Active List with User IDs" on page 376](#)).

The rule is triggered in cases where you do not find a matching badge swipe ID for a user login.

We define the rule conditions as follows.

- ◆ The `ServerRoomConsoleLogin` condition finds server room machine logins via the event name and asset category. The summary of this condition is:

```
ServerRoomConsoleLogin : ( Name = Console Login AND Target
Asset ID InGroup("/All Asset Categories/Server Room
Machines/") )
```

This is the "start" condition that causes the rule conditions to be evaluated because **it is looking for server logins**.

- ◆ We define a `Matching Event` condition that correlates server machine logins (one type of user identifier) with badge IDs used for server room entry (another type of user identifier) based on the unique user ID (UUID) from the Active List. We do this by using the `UserMap.UUID` variable we created for this purpose (see ["Variable" on page 379](#)).

Matching Event: `SeverRoomConsoleLogin.UserMap.UUID = BadgeSwipe.UserMap.UUID`

If we find a badge ID matches for all server logins, the rule will not be triggered. If there is a server login with no matching badge ID within our time window, the rule is triggered.

- ◆ If someone logs in, we want to find a matching badge swipe ID for it. Since we are looking for users who logged in to servers but did not use their own badges to enter the room, we add a condition specifying that no badge swipe event occurred for this user. The summary of this condition is:

```
! BadgeSwipe : Name = Badge Swipe Event
```

The following figures show the rule conditions definition (Edit panel) and summary (Summary panel).

Figure 15-2 Example Rule Conditions Definition (Edit panel)

Matching Event Condition: Correlates server login IDs with badge swipe IDs based on unique IDs (UUIDs) gleaned from the active list. The UserMap variable is used to get UUID values from the active list.

Server Room Console Login Condition: Finds server room machine logins (via event name and asset category). This is the "start" condition that causes the rest of the rule conditions to be evaluated.

Not Badge Swipe Event Condition: We are looking for users who logged in but did not use their own badges to enter the room. Adding this condition completes the scope of the conditions. When there is a server login, the rule correlates IDs (via the Matching Event), but triggers only if there is no matching badge swipe (this condition).

Figure 15-3 Example Rule Conditions Summary

Matching Event:
`ServerRoomConsoleLogin.UserMap.UUID = BadgeSwipe.UserMap.UUID`

ServerRoomConsoleLogin :
`(Name = Console Login AND Target Asset ID InGroup("/All Asset Categories/Server Room Machines/"))`

! BadgeSwipe :
`Name = Badge Swipe Event`

Aggregation

For this example, use default aggregation settings. Aggregate on 1 match in a 2 minute timeframe.

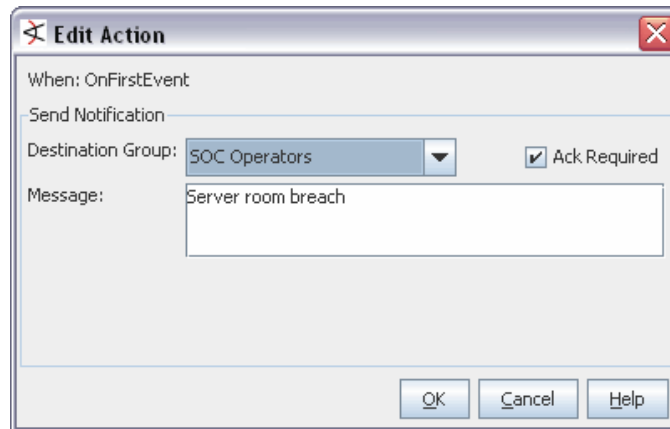
Actions

Click the **Actions** tab for the rule to set up an action to take if the server room is breached.

Select **On First Event** (this trigger is activated by default), right-click and choose **Add > Send Notification** to bring up the Add "Send Notification" Action dialog.

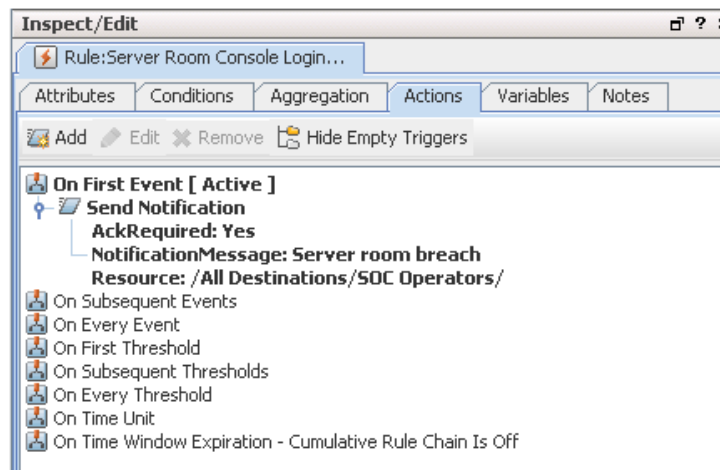
Choose the Destination Group for the e-mail, type in a message, and click **OK** to add this action to the On First Event trigger.

For this example, we chose **SOC Operators** as the Destination Group. Our message is **"Server room breach"**.



Click **OK** to save the notification definition.

When the action is configured, it is displayed under the "On First Event" trigger as shown in the figure. According to this rule, a message will be sent on the first trigger event; the first event in every time window that indicates a server room policy violation.



Click **Apply** or **OK** on the rule editor to save the example rule.

Chapter 16

List Authoring

Active lists and Session Lists are important tools for tracking traffic with IP addresses of interest.

[“Managing Active Lists” on page 385](#)

[“Managing Active List Groups” on page 391](#)

[“Managing Session Lists” on page 392](#)

Managing Active Lists

While you can manually update active lists, their real value comes when you author automatic, rule-driven lists with dynamic content. See [“Creating an Active List” on page 385](#) and then [“Using Rules to Populate an Active List” on page 387](#).

Creating an Active List

Active lists are usually defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules will be empty or contain only manually added entries that have not timed out. (See [“Using Rules to Populate an Active List” on page 387](#) and [“Rules Authoring” on page 301](#) for more information on how to create rules that work with active lists.)

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Active Lists** tab.
- 3 Right-click an active list group and choose **New Active List**.
- 4 In the Active List Editor, enter a name in the **Name** text field.
- 5 If you want to create a hash-based list, click the **Optimize Data Option** to toggle it on. (This option reduces the memory usage of an active list. It is useful for active lists with more than 1,000 entries or for lists that contain a large amount of information per entry. See [“Optimize Data with Hash-Based Active Lists” on page 576](#) (in the reference topic [“Active Lists” on page 574](#)).

- 6 In the **Capacity** field, set the maximum number of results to be stored.



Notes:

- If the maximum number of entries is reached, an existing entry is randomly selected and removed.
- Capacity influences the maximum memory that can be consumed by the active list.
- Note that the memory usage is proportional to the number of entries in the list, which usually are less than the capacity.
- Default capacity is 10,000 entries.
- Capacity affects the memory usage, but has little if any impact on performance.

- 7 In the **TTL** (Time To Live) fields, set the number of **Days**, **Hours**, or **Minutes** an unused result should remain on the active list before it is removed. Use **0** (zero) to cause the field to never expire. The maximum number of days is **99999**.
- 8 Set the **Common** and **Assign** fields as appropriate.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 552](#).

- 9 Choose **Event-based** or **Fields-based** lists in the **Data** panel. The Event-based option is convenient for choosing event attributes as found in existing events. When checking or adding to an Event-based list, you only need to supply an event. The Field-based option offers detailed event and attribute selection controls that involve mapping fields to event attributes.
- 10 Select event attributes or define arbitrary fields for list data collection.
- 11 For Fields-based lists optionally check **Key Fields** to enable a per-field Key option, and then select one or more data fields that must be unique.

For example, the Arcsight provided active list ArcSight Foundation/Configuration Monitoring/Assets with Recent Configuration Modifications uses fields-based data, and keys on unique values for asset address, zone, and name.

Field-based lists that use "Key Fields" are known as **active lists with values**. (For more information, see ["Active Lists with Values" on page 577](#).)

- 12 Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entries** button in the Active List Editor to manually create more entries for the current active list.

Case-Insensitive Lookup in Active Lists

By default, active list lookups are case-sensitive. For example, suppose you create an active list designed to capture user logins, aggregated on user name. (If user "John" logs in 10 times and user "Ringo" logs in 7 times, you want the Active List to display two lines: one line showing John's 10 logins, and another showing Ringo's 7 logins.)

You then need to create a rule to rule populates the list with login information. (See ["Using Rules to Populate an Active List" on page 387](#).) If all login names received from your

devices are formatted in the same “case” (upper case, lower case, or initial caps), the list will provide the desired display. However, if the user names arrive in different formats from active directories and other sources (e.g., John, JOHN, and john for a single user), by default the list and associated rule will not aggregate these different forms of the same user name on a single line, but rather treat them each as a different login names.

If you do not want case-sensitive results (as, in this example), you can use either the **ToUpper** function or the **ToLower** function in a **Variable** as a part of the rule(s) that populate your active list. You can use one of these functions as a variable in a rule, and map it (as a “DeviceCustomString”) to any field in the active list for which you want to normalize upper/lower case format. The following topic provides a walk-through example that shows how to make case-insensitive active lists. See [“Using Rules to Populate an Active List” on page 387](#), especially the sections [“Use Variable to Make Active List Case-Insensitive” on page 388](#), [“Aggregation” on page 389](#), and [“Actions” on page 389](#).



Please keep in mind that more fine-grained conditions logic requires more processing and can have a performance impact. For example, specifying a case-insensitive active list requires more processing than a case-sensitive active list. Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation.

Using Rules to Populate an Active List

Typically, active lists are defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. (See [“Rules Authoring” on page 301](#) for more information on how to create rules.)

Example

For example, to create a active list that captures information about VPN login events, you need to create both (a) the active list that forms the *table* or *shell* to store/display the data and (b) the rule(s) to capture and send matching events to the list. The rules **populate** the list for you.

This example shows how to create a active list and a rule that work together to capture VPN login events. The active list will show number of logins by user name.

Example Active List

To try out this example, first create a Fields-based active list named “VPN Events”, with fields named **User Name** and **Category**, both of type **String**. Set **User Name** as the Key field. Click **OK** to save this active list.

* Data: <input type="radio"/> Event-based <input checked="" type="radio"/> Fields-based <input checked="" type="checkbox"/> Key Fields			
Name	Type	Sub-type	Key-field
User Name	String		<input checked="" type="checkbox"/>
Category	String		<input type="checkbox"/>

Example Rule to Populate Active List

Next, create a rule also named “VPN Events” to populate the active list with user names and category information for matching login events.


What the Rule Does

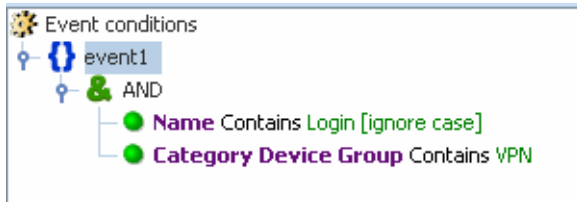
The goal is to define this rule to look for VPN login events, using values found in **Event Name** and **Category Device Group** fields as indicators of such events. A matching event will trigger the rule. When triggered, the rule will interact with our “VPN Events” active list as follows.

Populate this field in the Active List	With the value from this field in incoming events
User Name	Target User Name
Category	Category Device Group

Conditions

Set **Conditions** to capture events when the **Event Name** contains **Login** and **Category Device Group** Contains **VPN**. To capture event names from various sources that might be formatted differently (e.g., in all upper case, all lower case, or initial capitalization),

uncheck the Case-Sensitive  option next to the Event Name field



This will show up in the **Conditions Summary** tab as follows:

```
event1 :
( Name Contains Login [ignore case] AND Category Device Group Contains VPN )
```



Please keep in mind that more fine-grained conditions logic (as used in this example) requires more processing and can have a performance impact. For example:

- Specifying that a field be case-insensitive requires more processing than the default case-sensitive setting.
- Using "<SomeField> Contains <SomeString>" for a field lookup requires more processing than writing a field lookup like "<SomeField> = <SomeString>".
- Combining these types of conditions (as shown in this example) is even *more performance-intensive* (e.g., doing a lookup on <SomeField> Contains <SomeString> and making that case-insensitive).

Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation. Streamlining conditions wherever practical helps to optimize ESM system performance.

Use Variable to Make Active List Case-Insensitive

For this example, we want to make our active list *case-insensitive*. That is, since **User Name** is the active list *key field*, we want to aggregate matching events from the same user regardless of the original capitalization format of the user name in the event. If 3 events come in with user name "Jeff", and 4 more come in with user name "jeff", these should be shown on a single line in the active list showing that Jeff logged in 7 times. As described below, we'll map a **Variable** String Function called **ToUpper** to achieve this. (You can also use **ToLower**).

On the **Variables** tab in the rule, create a variable named **ConvertToUpperCase**, select the String Function **ToUpper**, and select Target User Name as the argument. Click **OK** to save the variable. In subsequent steps, we will use this variable to insert Target User Name

values in the active list. This way, all lookups from the active list will use upper case key field values.



Please keep in mind that more fine-grained conditions logic requires more processing and can have a performance impact. For example, specifying a case-insensitive active list requires more processing than a case-sensitive active list. Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation.

Aggregation

On the **Aggregation** tab in the rule, set Aggregation on [Category Device Group](#), [ConvertToUpperCase](#) (our variable), and [Device Custom String](#).

Aggregate only if these fields are identical —

```
event1.Category Device Group
event1.ConvertToUpperCase
event1.Device Custom String1
```

Actions

Activate the rule **Actions** option **On Every Event** (de-activate others), and select **Add to Active List**.

- **Insert ConvertToUpperCase variable into Active List.** Select **On Every Event**, right-click and choose **Add Set Event Field**. Map [Device Custom String 1](#) to [\\$ConvertToUpperCase](#). (This is calls the velocity template for the function. See ["Using Velocity Expressions in Rule Actions to Retrieve Values from Event Fields or Variables"](#) on page 794.)
- **Add values for User Name and Category to Active List.** Map the fields as follows:

Name	Field
* User Name	Device Custom String1
* Category	Category Device Group

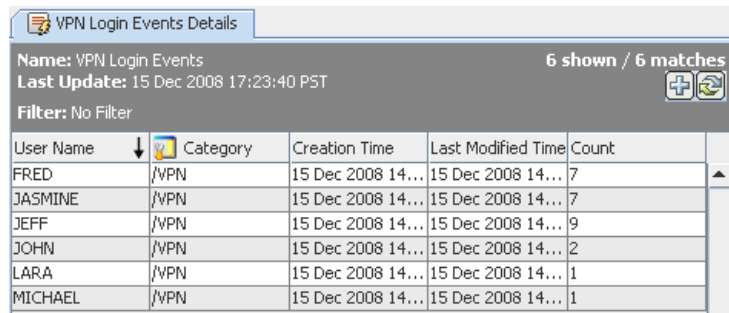
- User Name: Device Custom String1
- Category: Category Device Group

Save and Test

Click **OK** on the Rule Editor to save the rule.

When you are ready to test this; remember to drag-and-drop the rule(s) into the Real-time Rules folder to deploy them. When you do this, you'll get a choice of whether to move, copy, or link them. Linking is often most efficient. (See ["Deploying Real-time Rules"](#) on page 329.)

When the VPN Events rule is triggered, user names are added to the VPN Events active list.



The screenshot shows a window titled "VPN Login Events Details". It displays a table with 6 matches. The table has columns: User Name, Category, Creation Time, Last Modified Time, and Count. The data is as follows:

User Name	Category	Creation Time	Last Modified Time	Count
FRED	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	7
JASMINE	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	7
JEFF	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	9
JOHN	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	2
LARA	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	1
MICHAEL	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	1

A logical next step in this example scenario would be to create another rule that checks to see if certain user names are showing up in the active list, and then takes some action (like sending an e-mail or adding those names to a "suspicious users" list, if appropriate).

Editing Active List Entries

- 1 Right-click an item in the Active List resource tree and choose **Show Entries**.
- 2 In the active list grid view, right-click an entry and choose **Edit**.
- 3 Click the entry's **Source Address** or **Count** to make changes.
- 4 Click **Modify** to change the existing entry or **Add** to post the changed entry as a new one.

Editing an Active List

- 1 In the Active Lists resource tree, right-click an active list and choose **Edit Active List**.
- 2 Make appropriate changes to the properties of the active list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Move or Copy an Active List

- 1 In the Active Lists resource tree, navigate to an active list and drag and drop it into another group.
- 2 Choose **Move** to move the active list, **Copy** to make a separate copy of the active list, or **Link** to create a copy of the active list that is linked to the original active list.

If you choose **Copy**, you create a separate copy of the active list that will not be affected when the original active list is edited. If you choose **Link**, you create a copy of the active list that is linked to the original active list. Therefore, if you edit a linked active list, whether the original or the copy, all links are edited as well. When deleting linked active lists, you can either delete the selected active list or all linked active list copies.

Importing an Active List

You can import a comma-separated-value (CSV) file as data. This is useful if you have data from other systems that you want to import; you can use the import to populate your active lists.

- 1 In the Active Lists resource tree, select an active list, right-click, and choose **Import CSV File**. This brings up a file browser.
- 2 Browse to find the CSV file you want to import, select it, and click **Open**.

The Import Preview displays. If this is the file you want to import, click **OK** to add it to the active list.

- 3 Right-click the active list you just populated with the CSV file and choose **Show Entries**. This displays the newly-added data from the CSV file in the Viewer panel as active list details.



The default view limit is 2000 entries. To view more, specify the number of entries in your filter.

Exporting an Active List

In the active list viewer, you can export selected entries from an active list to a CSV file. This is useful if you want to manage active list data external to the console.

- 1 In the Active Lists resource tree, select an active list, and choose **Show Entries**. The data in the active list is displayed in the Viewer panel as active list details.
- 2 On the active list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting an Active List

- 1 Right-click an active list and choose **Delete Active List**.
- 2 In the dialog box, click **Yes**.

Managing Active List Groups

Active list groups are created to store similar groups or active lists in a single location. Groups can be created within groups to meet enterprise needs.

Groups and active lists can be managed with drag and drop functionality. You can move or copy groups and active lists into other groups in the Active Lists resource tree. If a group is deleted, the active lists within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Navigating to Active Lists

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Active Lists** tab.

Creating an Active List Group

- 1 In the Navigator panel, choose the **Active Lists** resource tree.
- 2 In the Active Lists tree, right-click a group and choose **New Group**.

- 3 A name text field appears under the group you selected.
- 4 In the name text field, type in a name.
- 5 Press **Enter**.

Renaming Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Rename**.
- 2 In the name text field, rename the group.
- 3 Press **Enter**.

Editing Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying Active List Groups

- 1 In the Active Lists resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Delete Group**.
- 1 In the dialog box, click **Yes**.

Managing Session Lists

While you can manually update session lists, their real value comes when you author automatic, rule-driven lists with dynamic content.

See also [“Understanding Session Correlation” on page 357](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 365](#).



As described in Creating a session list, filters improve session list performance by restricting the number of events that must be evaluated. Filters, such as DHCP IP address ranges, are installation-specific. Therefore, consider adding a filter to pre-defined session lists, such as /All Session Lists/ArcSight Foundation/Network Monitoring/DHCP, to improve performance.

Creating a Session List

Note that session lists are usually defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules will be empty or contain only manually added entries that have not timed out. (See [“Understanding Session Correlation” on page 357](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 365](#) for more information.)

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Session Lists** tab.
- 3 Right-click a session list group and choose **New Session List**.
- 4 In the Session List Editor, in the Inspect/Edit panel, define the following values.

In this field...	...enter this
Name	Enter a name for the session list. This name identifies the session list in ArcSight pick lists. Spaces and special characters are OK.
Overlapping Entries	Check this box to alert the system to allow multiple instances of key pairings, which keeps the previous session with the same key field open. For example, you might check this box if the list will be tracking activity for an asset that supports multiple-user logins.
In Memory Capacity (x1000)	This setting indicates the maximum number of session entries the system will keep in memory. 10,000 is the default value. For most cases, 10,000 will be appropriate, however, you may wish to adjust this setting if the devices you are monitoring for this session list contain a lot of data to ensure you have adequate memory cache available.
Entry Expiration Time	Enter an expiration time for session list entries. This indicates the time after which entries are marked as terminated (if no explicit termination event is received previous to this). The default is 0 seconds, which means the entry will never expire. An entry with no expiry date/time can only be terminated explicitly (through user action on Console, rule actions, or archives).

- 5 Set the **Common** and **Assign** fields as appropriate.
- 6 Define columns for session list entries by clicking on the row of the lower panel labeled "<Enter Name>." Columns for Start Time, End Time, and Creation Time are pre-defined.

In this field...	...enter this
Name	Enter a name for each session parameter you wish to track; for example, IP address, zone, or MAC address. The name you enter here will appear as a label in the session list, and in the Variable pick list. Names can contain spaces, such as "User name."

In this field...	...enter this
Type	Type indicates the data type of the entry. Data types can be: <ul style="list-style-type: none"> • Address (IP address or MAC address) • Date • Double • Integer • Long • Resource Reference (with appropriate subtype) • String
Sub-type	There are only two data types that require subtypes: Address and Resource reference. <ul style="list-style-type: none"> • Address – Choose IP address or MAC address. • Resource reference – A Resource reference can refer to any resource, such as Asset, Knowledge Base Article, or Zone.
Key field	Select one or more fields that must be unique to indicate a session start. In most cases, you would select at least two fields to make a key-value pair. For example, in the case of a DHCP login event, when a new IP and zone combination are written to the list, this indicates that a new session has started.

Columns can only be defined when the session list is created. Column definitions cannot be added, removed, or changed once the new session list is saved.

- 7 Click the **Filter** tab in the Session List Editor and define a filter that limits the number of events that will be considered for the new session list. Session lists without filters must evaluate every event, which can negatively affect performance. The Filter tab presents the familiar [Common Conditions Editor](#). Although the filter editor is similar, session list filters are not the same as Filter resources. Session list filters use different fields than Filter resources, for one thing.

Session lists are often concerned with logins to specific machines. In this case, you would write a filter that would limit evaluation to IP address ranges of interest. By filtering out all events except those targeting IP addresses in the DHCP server's subnet, for example, you are effectively limiting session list evaluation to inside traffic, reducing the overhead of session list evaluation. Other uses of session lists will suggest other installation-specific knowledge that can be used to create session list filters that restrict the number of events matched against the session list.

Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entry** button in the Session List Editor to manually create more entries for the current session list.

Using Rules to Populate a Session List

Session lists are usually defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules will be empty or contain only manually added entries that have not timed out. See [“Understanding Session Correlation” on page 357](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 365](#) for more information, including an example walk-through of how to create a session list and rules with which to populate it.

For information about rules, specifically, see [Chapter 13, Rules Authoring, on page 301](#).

Editing a Session List

- 1 In the Session Lists resource tree, right-click a session list and choose **Edit Session List**.
- 2 Make appropriate changes to the properties of the session list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Moving or Copying a Session List

- 1 In the Session Lists resource tree, navigate to a session list and drag and drop it into another group.
- 2 Choose **Move** to move the session list, **Copy** to make a separate copy of the session list, or **Link** to create a copy of the session list that is linked to the original session list.

If you choose **Copy**, you create a separate copy of the session list that will not be affected when the original session list is edited. If you choose **Link**, you create a copy of the session list that is linked to the original session list. Therefore, if you edit a linked session list, whether the original or the copy, all links are edited as well. When deleting linked session lists, you can either delete the selected session list or all linked session list copies.

Exporting a Session List

In the session list viewer, you can export selected entries from an session list to a CSV file. This is useful if you want to manage session list data external to the console.

- 1 In the Session Lists resource tree, select a session list, and choose **Show Entries**. The data in the session list is displayed in the Viewer panel as session list details.
- 2 On the session list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting a Session List

- 1 Right-click a session list and choose **Delete Session List**.
- 2 In the dialog box, click **Delete**.

Adding a Session List Entry Based on an Existing Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click an entry that is similar to the entry you would like to add. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to post the changed entry as a new one.


Adding a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Edit Session List**. The Session List Entry editor appears in the Inspect/Edit window.
- 2 Click the **Add Entry** button.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to save the new entry. The **Reset** button clears all values.

Deleting a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to delete. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click the entry's **Value** to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to post the changed entry as a new one.

Terminating a Session List Entry

- 1 In the Session Lists resource tree, right-click a session list and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to terminate. Choose **Terminate Session Entry**.
- 3 Enter the date and time for the session end time. Click the  button for a context menu containing relative times such as Now, 1 hour ago, 1 day from now, and so on. Click **OK**.

Case Management and Queries

You use ArcSight cases for organized, workflow-style tracking and management of interesting events or situations.

Please also refer to the Case Editor Tab Field Reference when building and using cases.

["Managing Cases" on page 397](#)

["Managing Case Groups" on page 402](#)

["Running Case Queries" on page 403](#)

Managing Cases

This topic describes the basic tasks necessary to create, manage, and delete cases.

It is important to note that, most often, you create and update cases automatically using rule actions.

See also, ["Collaborating on Events" on page 141](#).

Create a New Case

- 1 Choose the **Cases** resource tree in the Navigator panel.
- 2 Right-click a case group and choose **New Case**. You can also choose the **New Case** option on the File menu.
- 3 In the Case Editor, select the **Initial** tab.
- 4 Select the **Attributes** tab.
- 5 Enter text in the required **Name** field.
Display ID numbers are assigned automatically when you save the case.
- 6 Specify **Ticket** info for the case as described below in the Case Properties table.
- 7 In the Assign section, choose a user on the **Owner** drop-down menu, to assign one or more case owners.
- 8 Also in the Assign section, choose groups on the **Notification Groups** drop-down menu, to notify groups of the new case.
- 9 Click **OK**.

For details on defining case attributes, see ["Case Properties" on page 398](#), ["Editing a Case" on page 399](#) and ["Case Editor Tab Fields" on page 600](#) (a complete reference).

Case Properties

Property	Usage
Ticket Type	The drop-down list includes Internal , Client , and Incident types.
Stage	Selections indicate workflow stage of ticket; default selections include Queued , Initial , Follow-Up , Final , and Closed . (See also “Creating New Stages” on page 143 and “Editing Stages” on page 144.)
Frequency	Indicates how often reported issue occurs. Values assigned are 0 (never or once), 1 (less than 10 times), 2 (10 to 15 times), 3 (15 times), 4 (more than 15).
Operational Impact	Impact of reported issue. Values assigned are 0 (no impact), 1 (no immediate impact), 2 (low priority impact), 3 (high priority impact), 4 (immediate impact).
Security Classification	Values assigned are 1 (Unclassified), 2 (Confidential), 3 (Secret), 4 (Top Secret).
Consequence Severity	Values assigned are 0 (None), 1 (Insignificant), 2 (Marginal), 3 (Critical), 4 (Catastrophic).
Reporting Level	Calculated based on Ticket info values entered. You can also use entries in all Case Ticket fields to generate reports so you can categorize cases based on specific case information.
Incident Information	Automatically populated based on events included in the case.

For more information on entries in the remaining Initial tabs, and the **Follow-Up**, **Final**, **Events**, and **Notes** tabs, see [“Editing a Case” on page 399](#) and [“Case Editor Tab Fields” on page 600](#) (a complete reference).

Creating a Case from Displayed Events

You can also create cases directly from the Viewer panel, while monitoring suspicious events.

- 1 In an active channel grid view, select one or more events.
- 2 Right-click and choose **Add to Case**.
The selected event appears in the Case Editor on the Events tab.
- 3 In the Case Editor, select the **Initial** tab.
- 4 Select the **Attributes** tab.
- 5 Enter text in the required **Name** field.
Display ID numbers are assigned automatically when you save the case.
- 6 Specify **Ticket** info for the case as described above in the Case Properties table.
- 7 In the Assign section, choose a user on the **Owner** drop-down menu, to assign one or more case owners.
- 8 Also in the Assign section, choose groups on the **Notification Groups** drop-down menu, to notify groups of the new case.

- 9 Click **OK**.

For more information on entries in the remaining **Initial** tabs, and **Follow-Up**, **Final**, **Events**, and **Notes** tabs, see [“Editing a Case” on page 399](#).

Editing a Case

To be able to edit a case that has already been saved, you first need to lock it by selecting the **Locked by** check box. This prevents other users from modifying the case while you're editing it.

- 1 In the Cases resource tree, right-click a case and choose **Edit Case**.
- 2 In the Case Editor, select the particular workflow tab you want to edit, as described below.
- 3 Select the tab and add or edit its information. When you are finished with this, click **OK** to save your changes.
- 4 When you are finished with the case, clear the **Locked by** check box to release the lock on the case before you click **Close**.

Cases Editor Workflow Tabs

Tab	Usage
Initial	Provides basic case information: case ticket attributes, description and security classification.
Follow-Up	Descriptions of actions taken, planned, or recommended.
Final	Ticket resolution and reporting, including attack mechanism, attack agent, incident information, and vulnerability information.
Events	A list of the events included in the case.
Notes	Miscellaneous case information.

Finding Cases

You can locate a particular ArcSight case by its reference ID if you wish.

- 1 Right-click a group in the Cases resource tree and choose **Edit Case by ID**.
- 2 Enter the ID string in the dialog box and click **OK** to display it in the Case Editor.

When working from cases listed in a Viewer panel channel view, you can locate a particular case's position in the Navigator panel's resource tree.

- 1 Right-click a case in the channel grid view and choose **Find Case in Navigator**.
- 2 Look for the highlighted item in the Navigator panel's Cases resource tree.

Attaching a File to a Case

- 1 Open an existing case and click **Lock** to edit it.

- 2 Click **Attachments** and attach by uploading the file.

Field	Description
File Name	The default is the uploaded filename, which you can change.
Attachment Name	A descriptive name for the file. This name can differ from the actual file name, and can include spaces. If you do not provide an alternative name here, the original file name is used.
Attachment Description	Optional description of the file.
Sharing	Click Share this file in Arcsight if you want to make the file available as a shared resource on the ArcSight Manager.
Mime Type	Read-only field that indicates the Multipurpose Internet Mail Extensions (MIME) type of the attached file.
Encoding	Text encoding; for example, you could select Chinese text for internationalization requirements.

- 3 Click **Attach**.

- 4 The Attachments list displays. Select a file to view its summary. From the summary view, you can attach, edit, or detach a file.

- ◆ Attach: attaches the file to the case.
- ◆ Edit: enables you to edit the name and description. You can also upload a new file to replace the existing file by selecting **Replace file** and click **Update**.
- ◆ Detach: removes the file from the attachment.

For more information on customizing ArcSight operation to integrate with external case management systems such as Remedy, refer to the README.txt file located in the ArcSight Manager ARCSIGHT_HOME\utilities directory.

Viewing a Case Attachment

Once a file is attached to a case, anyone viewing the case can view details about the file and download it. To do this, open a case and click the Attachments tab, which lists files attached to the selected case. Right-click a file name and choose **Open** to open the file or **Download** to download the file to your local system.

If you click **Download**, you get a file browser in which to navigate to the local directory where you want to store the file. In the **File Name** field, type the name under which you want to store the file on your local system and click **Save**. The file is saved as specified.

If the case attachment was also added as a shared resource, the file will be available in the ArcSight Manager Files resource folders. To access a shared file, choose **Files** in the Navigator and browse the folders, or choose **Edit > Find Resource** from the menus, enter the file name in the **Search query** field, and click **Find**. (See [“Finding Resources” on page 534](#) for more information on this utility.)

Adding Events to a Case

- 1 In the **Cases** resource tree, right-click a case and choose **Edit Case**.
- 2 In a Viewer panel grid view, select one or more events.
- 3 Right-click and choose **Add To Case**.

- 4 Click **OK**.

Showing Event Details for Cases in Channels

- 1 In the Cases resource tree, right-click a case and choose **Case Details Channel**. The events associated with the case appear in an active channel grid view in the Viewer panel.
- 2 In the grid view, use any of the Viewer panel's features to further analyze the events.

Deleting Events from a Case

- 1 In the Cases resource tree, right-click a case and choose **Edit Case**.
- 2 In the Case Editor, select the **Events** tab.
- 3 Select one or more events.
- 4 Right-click and choose **Remove from Case**.
- 5 In the dialog box, click **Yes**.

Creating a Channel for a Case

In the Cases resource tree, right-click a case and choose **Case Details Channel**. A new channel is created and displayed in the Viewer. The channel filters for events associated with the selected case.



You can create a channel based on a case only if the case has one or more events associated with it. See [“Adding Events to a Case” on page 400](#).

Exporting a Case to an External System

If Remedy integration is enabled, cases can be transferred from the Cases resource tree to an external system by doing the following. For more information on Remedy integration, see [ARCSIGHT_HOME\utilities\README.txt](#).

- 1 Choose the Cases resource tree in the Navigator panel.
- 2 Right-click a case and choose **Export to External System**.

The Case Editor displays a message informing you of a successful transfer. Exported cases will also display a flagged icon indicating the case has been exported.

Moving or Copying a case

- 1 In the Cases resource tree, navigate to a case and drag and drop it into another group.
- 2 Choose **Move** to move the case, **Copy** to make a separate copy of the case, or **Link** to create a copy of the case that is linked to the original case.

If you choose **Copy**, you create a separate copy of the case that will not be affected when the original case is edited. If you choose **Link**, you create a copy of the case that is linked to the original case. Therefore, if you edit a linked case, whether the original or the copy, all links are edited as well. When deleting linked cases, you can either delete the selected case or all linked case copies.

Deleting a Case

- 1 In the Cases resources tree, right-click a case and choose **Delete Case**.
- 2 In the dialog box, click **Yes**.

Managing Case Groups

Case groups are created to store similar groups or cases in a single location. Groups can be created within groups to meet enterprise needs.

Groups and cases can be managed with drag and drop functionality. You can move or copy groups and cases into other groups from the Cases window. If a group is deleted, the cases within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Case Group

- 1 From the **Navigator Panel** drop-down menu, select **Cases**.

Cases are displayed in different colors based on the assigned "Consequence Severity" in the case. The severity descriptions are Catastrophic (Dark Red), Critical (Red), Marginal (Orange), Insignificant (Green), or None (Gray).



Before being able to edit a case that has already been saved, you need to lock the case by selecting the **Lock Case** check box, so other users can not modify the case while you're editing it.

- 2 In the **Cases** resource tree, right-click a group and choose **New Group**.
- 3 A **Name** text field appears under the group you selected.
- 4 In the name text field, type in a name.
- 5 Press **Enter**.

Renaming a Case Group

In the Cases resource tree, right-click a group and choose **Rename**.

- 6 In the **Name** text field, rename the group.
- 7 Press **Enter**.

Editing a Case Group

- 1 In the Cases resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying a Case Group

- 1 In the Cases resource tree, navigate to a group and drag and drop it into another group.

ArcSight Console displays a dialog box with drag-and-drop options.

- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Case Group

- 1 In the Cases resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Running Case Queries

You can create groups in the Cases resource tree that automatically query every case change that occurs. If a case change results in a state that meets the criteria for such a group, the case is listed in that group.

Setting Up an Automatic Case Query Group

- 1 Choose the **Cases** resource tree in the Navigator panel.
- 2 Right-click a group in the tree and choose **New Search Group**.
- 3 Select the **Attributes** tab and enter values as you always do when [Editing Groups](#).
- 4 Select the **Conditions** tab and construct query statements as you do when [Creating Filters](#).
- 5 Click **Apply** to save your changes and keep editing, or **OK** to save and close.

Chapter 18

Integration Commands

These topics cover ESM Integration Commands, a new feature introduced in ESM v.4.5.

[What are Integration Commands?](#)
[Planning Checklist and Workflow](#)
[Navigating to Integration Command Resources](#)
[Quick Example](#)
[Adding and Editing Commands](#)
[Creating and Editing Configurations](#)
[Specifying Targets](#)
[Setting User Login Parameters](#)
[Setting Logins and Other Parameters to Prompt for Values at Runtime](#)
[Access Control Lists \(ACLs\) on Integration Commands](#)
[Running Integrated Commands](#)
[Network Tools as Integration Commands](#)

Starting with ESM v.4.5, the Console offers better application integration capabilities.

With the help of ArcSight Professional Services, you can configure and launch commands, tools, and views in custom and third party applications and other ArcSight products from within the ESM Console. Role and access list (ACL) based use of the tools and commands can be configured and managed in the Console.

Integration with these ArcSight Network Synergy Platform (NSP) components is supported:

- Threat Response Manager (TRM)
- Network Configuration Manager (NCM)
- CounterACT SmartConnector

ArcSight NSP is an appliance-based solution that easily integrates with your existing network infrastructure and provides a way to secure, monitor, and manage network devices available from most network vendors. The integration feature in ESM Console allows you to integrate ArcSight NSP configurations, targets, and commands into the Console. This provides a central location for defining, managing, and launching TRM actions.

Please contact ArcSight Professional Services if you need assistance in authoring tools integrations with ArcSight products or other applications.

For information on integrating basic network tools such as Ping, Nslookup, or ArcSight specific “SendLogs”, see [“Using the Network Tools” on page 72](#).

What are Integration Commands?

Integration commands give you a lightweight way to link to information between the ESM Console into other views and tools, similar to using Web page links.

You can configure and launch commands, tools, and views in custom and third party applications and other ArcSight products from within the ESM Console.

Operations Synergy Scenarios

ESM integration commands leverage the power of ESM security and event management, and broaden its view to show external, snap-in views from applications like ArcSight NSP as well as third-party applications. Both automated (rule-driven) and manual (ESM user-driven) scenarios are supported. With a more flexible and powerful way to integrate ESM with other applications, you can use the ESM Console as a central command hub for all security-related operations and reconnaissance.

Examples of common scenarios that drove the introduction of this new feature are described below.

TRM and CounterACT Scenarios

One can imagine many scenarios where customers can leverage ESM integration with TRM and CounterACT commands. Here are a few popular ones:

- Select an IP address in ESM and investigate the associated node using TRM
- Select an IP address in ESM and quarantine the associated node using TRM
- Manually quarantine a node using CounterACT from resource contexts on the Console. (Integration commands offer a new, contextual way of sending TRM commands via CounterACT, in addition to automatically by a rule action firing or manually by running Connector commands directly.)

Console Integration Scenarios

These examples focus specifically on getting ESM Console embedded views and control of TRM features.

- Find an attacker in an ESM Console active channel

Third-Party Integration Scenarios

Typical activities for which you might want to build and run commands in the ESM Console that connect to other applications and tools include:

- Launch third-party Web interfaces
- Launch scripts
- Run external searches
- View submitted tickets
- Get Asset/Vulnerability information
- Get Payload Information

How it Works

Integration commands provide resources for **tools integration authors** to:

- Build “ESM context-sensitive” commands that can run locally or on multiple, remote target servers, and can be mixed, matched, and re-used with configurations.
- Associate parameters with commands to leverage/read the ESM resources and contexts in which the commands are called. Command parameters make use of velocity expressions to pick up values from a wide range of ESM fields and resources.
- Define configurations (“families of commands”) for various external applications to specify relevant ESM contexts, commands, and, optionally, remote targets

Once integration commands and configurations are in place, **analysts and operators** working with the ESM Console can **use the pre-built commands** to manage and monitor networks and assets with an extended reach into other views and toolkits, including ArcSight applications like NSP TRM and NCM. (See [“Operations Synergy Scenarios” on page 406.](#))

Both **manual** and **automated** (rule-driven) actions are possible. For example, analysts and operators can right-click on an event and define an action to be taken directly from an active channel viewer. When investigating an event, an analyst can execute a manual action or define an automated action to take against the event.



Audit events associated with ArcSight Threat Management Response (TRM) commands indicate whether actions are performed manually or automatically.

Authorization to send commands to the external application is configured through new **integration parameters** on the **user resource**. (See [“ESM Contexts and Parameters” on page 408](#) and [“Setting User Login Parameters” on page 428.](#))

Supported Command Types

You can build these types of commands into the ESM Console:

Command Type	Output Results
URL commands provide links to Web page URLs or URIs	<ul style="list-style-type: none"> • ESM Console internal browser • External Web browser
Script commands defines an executable script	Script/executable output result (e.g., action)
CounterAct Connector commands are derived from the CounterACT configuration XML	CounterACT structured result

For more information on working with commands, see [“Adding and Editing Commands” on page 413.](#)

Understanding Integration Configurations

An integration **configuration** resource represents a family of commands of the same type. A configuration holds contexts, contains commands, specifies how command result are rendered (e.g., Web browser, text, XML), and in some cases has targets. Commands in a configuration share the same context, rendering method, and targets.

Typically, each integration maps to a single product; for example, one resource each for ArcSight Threat Response Manager (TRM) and ArcSight Network Configuration Manager (NCM). However, you can distribute sets of commands across multiple configurations, if needed. This is useful when the same product has different types of interfaces. For example, ArcSight TRM-Web takes URL based commands whereas TRM-CLI requires shell script commands.

For more details on how integration configurations are constructed, see [“Creating and Editing Configurations” on page 421](#).

ESM Contexts and Parameters

As a part of constructing these commands, you can configure **contexts** for where in the Console certain commands are available. At the same time, you can define **parameters** for picking up and passing the value in any selected cell, row, or event field

For example, you could configure a URL command for a Google search as a right-click command on any cell in a Console grid view. By using a parameter as the argument to the search command, you could pick up the text from the selected cell or value from any selected field to use as your search term. (In the Commands editor, all ESM fields, provided as a list of velocity expressions, are available for use as command parameters.)

Once they are configured, integration commands are available on right-click context menus from a variety of contexts in ESM including:

- Relevant fields in active channels (e.g., IP address, host name, MAC address)
- Relevant resources (for example, assets)
- Active Lists, sessions lists, query viewers and channels

Also, you can configure **user login parameters** on ESM Console users (via a new Integration Parameters tab in the Users resource editor), thereby binding user login information to commands for third-party or ArcSight applications that require secure logins. (See [“Setting User Login Parameters” on page 428](#) for more information.)

You can configure a command to prompt for parameter information, which is often useful for login scenarios and as well as others. (See [“Setting Logins and Other Parameters to Prompt for Values at Runtime” on page 429](#) for more information.)

Rendering Command Output

You can specify how command results will be rendered. Appropriate rendering formats typically depend on command type, the application and targets, and so forth. Options include rendering command output in an external or ESM Console embedded Web browser, text renderer (for textual scripts), or XML result renderer. (See [“Creating and Editing Configurations” on page 421](#), and specifically about choosing a renderer, the [related information on page 423](#).)

Target Servers Where Commands Run

You can identify targets for commands where needed. A target describes a remote server on which to run a command. If you have multiple remote servers, you might want to configure multiple targets on which to run a single command with the same or different parameters. (See [“Specifying Targets” on page 427](#).)

For example, you can configure any of the following as command targets.

- Web Servers like...
 - ◆ ArcSight Threat Response Manager (TRM) servers

- ◆ ArcSight Logger servers
- ◆ Search providers (e.g., Google, Yahoo, ask.com)
- ◆ IT/Security portals
- ◆ Asset/Vulnerability information
- ◆ Ticketing Web servers
- CounterACT SmartConnector
- ◆ TRM CounterACT

Planning Checklist and Workflow

High-level steps for integrating tools and applications into the ESM Console include planning and collecting information; creating and binding together commands, targets, and configurations; configuring user accounts with appropriate login parameters; and testing. The following topics give a little more detail about this workflow.

We suggest taking some time to plan out your integration commands first. Identify the tool or application you want to integrate, and collect the information needed to build the integration. Some other points to consider are as follows:

- What commands do you want to run on the external application? Is there a subset of commands you want to integrate?
- What is the command type? (Web URL, local, executable script, CounterACT for TRM)



Prerequisites for CounterACT Commands

If you plan to use **TRM CounterACT commands**, you need:

- access to an NSP TRM server
- One or more CounterACT SmartConnectors deployed and registered with the Manager to which your Console is connected. When you set up the CounterACT connector, it verifies its connection to the TRM server and asks for authentication credentials.

We suggest that you test connectivity and authentication among your local machine, CounterACT SmartConnector(s), and TRM server(s) first, before setting up TRM integration commands.

- What is the syntax of the commands?
- How do you want to render output results of commands? (This largely depends on the command type; e.g., URL commands are rendered in an external or embedded browser.)
- How many integration configurations do you need?
Does the application you are integrating have more than one type of interface? (e.g., Web and CLI, like TRM) If so, you'll need a configuration for the each interface and associated command type.
- Which ESM users (analysts and operators) will work with these integrated tools or applications?
 - ◆ Are there authentication parameters required on the integration targets? If so, collect or establish user names and passwords for ESM users who will work with the integrated applications.
 - ◆ Plan for configuring integration parameters on user accounts for ESM users who will work with the external applications. These users will need login credentials for both ESM and the target applications.

- ◆ If a group of ESM users will be using the same authentication parameters for a target server, the author can create a target resource with those parameters (instead of duplicating the parameters in each user account). Then the ACL of that target resource can be configured so that only those users have access to it. When a command is triggered in the right context, only the target that the user has access to will be displayed. A similar ACL approach can be used for commands. For example, a single configuration can contain groups of commands, where some commands require special privileges.

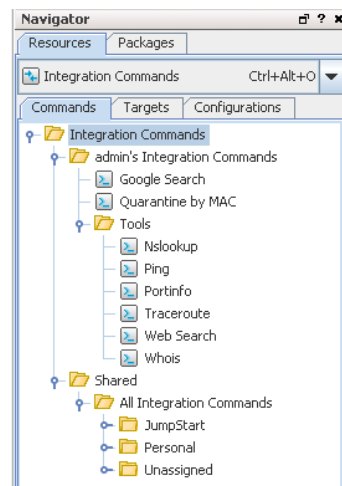
Once you have a plan, you might try configuring the commands and testing in this order:

- 1 Add the commands, including naming the command, specifying the command type, providing the command itself in the appropriate syntax, and defining any parameters needed.
- 2 Specify the targets (remote servers where commands will run), if any.
- 3 Create one or more named configuration(s), including binding one or more commands to the configuration, choosing how command results are rendered, and defining ESM Console UI contexts where these commands will be available for use.
- 4 Add Integration Parameters to User Accounts. If authentication is required on the integration targets, configure integration parameters on user accounts for ESM users who will work with the external applications. These users will need login credentials for both ESM and the target applications.
- 5 Test the commands by running them. See [“Running Integrated Commands” on page 430](#)

Navigating to Integration Command Resources

Integration command authoring resources live under Integration Commands in the Navigator. (Users can access existing integration commands and configurations through right-click commands on the Console in various contexts. The contexts depend on how the commands are configured.)

To create or edit integration commands and configurations, start by navigating to **Integration Commands** resources.



Quick Example


To start experimenting with building integration commands, you need, at a minimum, one **command** and one **configuration**. You'll need to create the command(s) first because the configuration references the commands.

The configuration also defines how command results will be rendered, and references **contexts** where your new Integration Commands will appear in the ESM Console right-click menus (e.g., Viewers, Resource Panel, Editors, and more specifics within those contexts).

If you want to define **targets** (remote servers where commands will run), you will need to add these into the configuration as well in order to implement them.

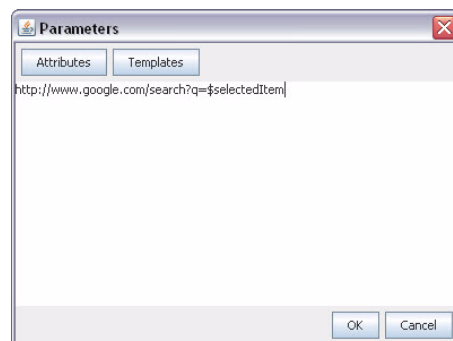
Here is an example of how we would set up a command to do a Google Search on a selected cell in the Console. This example does not require a "target" so we will just set up a command, add it to a configuration, and run it. The details of this and other types of commands and configurations are discussed further in the topics that follow. This is just a quick preview.

Constructing the Example Command

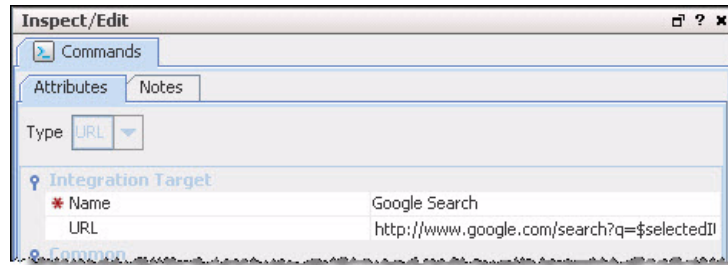
- 1 Start by getting the format of the Google search. Do a Google Search in a Web browser. Copy the first part of the URL (everything *before* or *to the left of* the search term) from the Address bar, so you have it on your clipboard. (You will be using this to paste in to the Parameters dialog in [Step 4](#).)
- 2 Now let's *set up the command*. In the ESM Console Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Commands** tab.
- 3 Right-click the group (folder) where you want to create the command and select **New Command**.
- 4 On the Commands Editor, fill in these attributes:
 - ◆ For command Type, choose **URL**.
 - ◆ For Name, provide a user-friendly name like "Google Search".
 - ◆ For URL, click the browse button  to get the Parameters dialog. Paste the Google search prefix (from [Step 1](#)) into the Parameters dialog scratch pad: `http://www.google.com/search?q=`

Next, click **Attributes** on the Parameters dialog to get a list of velocity expressions. Select the first option, `$selectedItem`. The expression is added as a parameter to the search:

`http://www.google.com/search?q=$selectedItem`



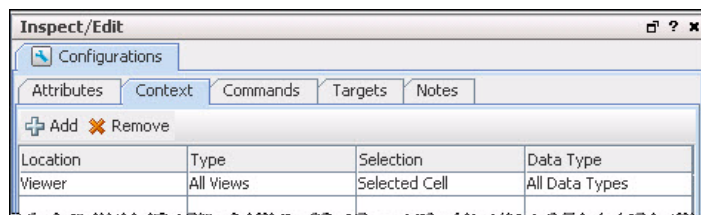
- ◆ Click **OK** to close the Parameters dialog and save your changes.
- ◆ Click **Apply** or **OK** on the Commands editor to save the command.



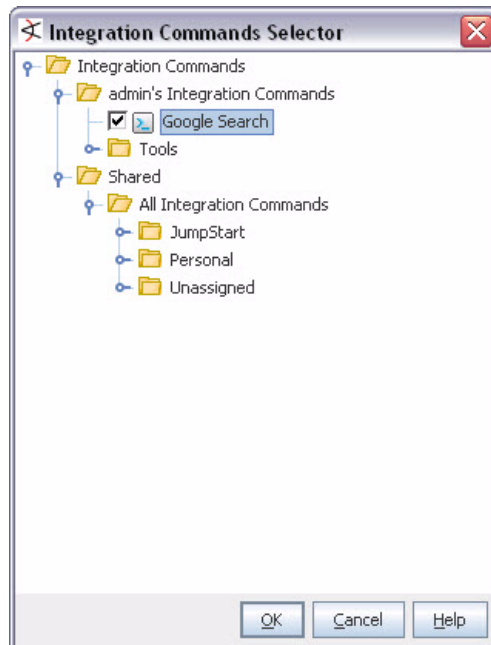
- Now, let's *set up the configuration and add the command to it*. Click the **Configurations** tab.
- Right-click a group and select **New Configuration**.
- On the Configurations Editor, select **URL** as the configuration Type, and fill in these other attributes:
 - ◆ For Name, provide a user-friendly name like "My Searches".
 - ◆ For Renderer, click to select either Internal Browser or External Browser.
- Still on the Configurations Editor, click the **Context** tab. (This sets where in the Console the command will be available.) Click **Add** to get a set of context fields, then click into each field to select a location, type, selection, and data type. (You can add multiple contexts by clicking Add again.) Let's add one context to show in the Viewer in all "views" and to take the selected cell as the "selection":

Location	Type	Selection	Data Type
Viewer	All Views	Selected Cell	All Data Types

When the search command is deployed as part of this configuration, and run via a right-click command in the context of the Console, it will search on the text in the "cell" (i.e., Viewer table cell) the user selects in the Console.



- 9 Finally, let's add the command to the configuration. On the Configuration Editor, click **Commands**. Click **Add** to get the command selector, select your Google Search command, and click **OK**.



- 10 Click **Apply** or **OK** on the Configurations Editor to save the configuration.

Running the Example Command

Now let's try running the Search command we just built (in ["Constructing the Example Command" on page 411](#)):

- 1 Open any active channel, list, data monitor, or query viewer with a table style view.
- 2 Right-click on any cell in the Viewer that contains a term you would like to search on, and select **Integration Commands > Google Search** (or whatever you named the command).

The command runs a search using the text from the selected cell as the search term, and returns search hits in the browser (either the embedded browser or an external Web browser, depending on which you selected for the Renderer for the command.)

This concludes this quick example of how to build and run commands. The following topics provide more information and examples on how to build all types of commands, how to add user authentication, how to use targets for TRM commands, how the standard ESM network tools are implemented as integration commands, and more.

Adding and Editing Commands

With the ESM *commands* feature, you can configure URL, Script, and TRM CounterACT commands for custom and third party applications and other ArcSight products. Setting up *commands* is the first step in a multi-part process to providing a set of integration commands. (Other tasks include setting up configurations, targets, and user login parameters).

This topic explains how to add and edit the command portion of an integration command solution. For an overview of the integration commands feature, see ["Integration"](#)

[Commands](#) on page 405. For more details on the relationship between commands, configurations, and targets, see [“How it Works”](#) on page 407.

To add a new command, do the following:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Commands** tab.
- 2 Right-click a group (folder) where you want to create the command, and select **New Command**. This launches the Command Editor in the Inspect/Edit panel. (As a general rule, it is best to create new content in the user's own folder.)
- 3 On the **Command Editor**, select the command **Type** and fill in the fields for command Name, and other attributes.

The screenshot shows the 'Inspect/Edit' window for a 'Command: Google Search'. The window has tabs for 'Attributes' and 'Notes'. The 'Attributes' tab is active, showing a 'Type' dropdown set to 'URL'. Below this are several sections of attributes:

- Target:** Name (Google Search), URL (http://www.google.com/search?q=\$selectedCell)
- Common:** Resource ID (/bFuL+xsBABCFFDxEFPj0A==), External ID, Alias, Description, Version ID, Deprecated (checkbox)
- Assign:** Owner, Notification Groups
- Parent Groups:** Samantha's Integration Commands (/All Integration Commands/Personal/Samantha's ...)
- Creation Information:** Created By (admin), Creation Time (25 Aug 2008 13:25:51 PDT), Time Since Creation (9 day(s) 5 hour(s) 5 min(s) 21 sec(s))
- Last Update Information:** Last Updated By (admin), Last Update Time (26 Aug 2008 17:12:01 PDT), Time Since Last Update (8 day(s) 1 hour(s) 19 min(s) 10 sec(s))

At the bottom, there are fields for '(Name)' and '(Description)', and buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

Table 18-1 Command Types

Command Type	Description
Script	Executable script that runs <i>locally</i> in terms of the ESM Console where the command is launched.
URL	Web URL for which you can define parameters.
CounterACT	Command for CounterACT SmartConnector.

See [“Command Types and Attributes”](#) on page 415 for more details on attributes.

- 4 Click **Apply** or **OK** to add the new command.



Command Types and Attributes

The command attributes will vary, depending on the type (Script, URL, or CounterACT), as described below.

Script Commands




Script commands (like the other commands) can be made available for use by multiple ESM users and user groups. Users will probably run the ESM Console on many different machines (i.e., their own). Integration **script commands will always run "local to the Console"**; i.e., on the same machine as the ESM Console used to launch them. Therefore, the Working Directory and Program path names need to reflect where commands will be found in Console users' environments

Attribute	Description
Name	User-friendly Name for the command.
Working Directory	<p>Directory containing the executable script.</p> <p>For example, <code>\$systemRoot\system32\</code></p> <p>You can type the directory path in the Program field, or click the Browse Directory button  to get a file browser. Use the file browser to navigate to and select the command.</p> <p>Note: Be sure this path reflects the location of the script on machines used by ESM Console users for whom you are building these commands.</p>
Program	<p>Full path to the executable command.</p> <p>For example, <code>\$systemRoot\system32\ping.exe</code></p> <p>You can type the full path to the command in the Program field, or click the Browse Directory button  to get a file browser. Use the file browser to navigate to and select the command.</p> <p>Note: Be sure this path reflects the location of the script on machines used by ESM Console users for whom you are building these commands.</p>
Parameters	<p>Provide parameters for the command. (See "Adding and Editing Command Parameters" on page 418.)</p> <p>The Attributes list provides velocity expressions for all event fields and an option to add <code>\$selectedItem</code> as an attribute.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields"](#) on page 552.

URL Commands


Attribute	Description
Name	User-friendly Name for the command.
URL	<p>The URL for the command, along with any parameters provided as arguments to the URL.</p> <p>Click the browse button  to get the Parameters dialog. (See “Adding and Editing Command Parameters” on page 418 for information on how to add the URL along with parameters or <i>arguments</i> to the URL.) You can copy/paste URLs onto the Parameters dialog scratch pad or type them directly. The Attributes link provides velocity expressions you can add as parameters (attributes) to the URL.</p> <ul style="list-style-type: none"> Type or paste URL directly in the Parameters dialog scratch pad Click Attributes to add a velocity expression as a parameter to the URL <p>Determine the URL by first accessing it from a Web browser address bar. This will also show you where in the URL the parameters (if any) should be added.</p> <p>Example: Web Search</p> <p>To set up a Google Search on a parameter, do a Google Search in a Web browser. Extract the first part of the URL (everything <i>before</i> or <i>to the left of</i> the search term) from the Address bar, and paste it into the Parameters dialog scratch pad: http://www.google.com/search?q=</p> <p>Next, click Attributes on the Parameters dialog to get a list of velocity expressions. Select the first option, <code>\$selectedItem</code>. The expression is added as a parameter to the search:</p> <p>http://www.google.com/search?q=\$selectedItem</p> <p>Click OK to close the Parameters dialog and save your changes. (Also, click Apply or OK on the Command Editor when you are satisfied with all settings.)</p> <p>When this search command is deployed as part of an integration configuration, and run via a right-click command in the context of the Console, it will search on the text in the “cell” (i.e., Viewer table cell) the user selects in the Console.</p> <p>Example: TRM Web Client</p> <p>You can also configure URL type commands to interact with NSP TRM Web servers. In order to do this, you need to know the syntax of the TRM command URL and then deconstruct it to add in parameters, similar to the Google Search URL example above. Start with a TRM Web client, send a command, copy and paste the URL into the command URL field, and then substitute parameters for hard-coded values (such as TRM server IP address and authentication/password) in the URL.</p>
Parameters	Parameters for URL commands are <i>added as attributes to the URL</i> as described above in URL .



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

CounterACT Commands

As mentioned in [“Prerequisites for CounterACT Commands” on page 409](#), integrating CounterACT commands requires access to an NSP Threat Response Management (TRM) server, and a TRM CounterACT SmartConnector deployed and registered with the Manager to which your Console is connected.

Attribute	Description
Name	User-friendly Name for the command.
Group	If the command type is set to CounterACT, the group is set to counteract by default. This is not editable.
Command	<p>Choose a CounterACT command from the drop-down list. The following commands are available:</p> <ul style="list-style-type: none"> Quarantine node (by IP address or MAC address) Add rules for various actions based on user name or IP address (e.g., require authorization for user(s), deny action for an IP range, and move targeted user(s) to VLAN) Enable or Disable a rule Block an IP range Authorize a TRM action Simulate a quarantine node action (by IP, MAC address, host name, or Netbios name) Investigate a quarantined node (by IP, MAC address, host name, or Netbios name) ARP dump of a device Resolve MAC address from an IP address <p>See “TRM Command Syntax and Examples” on page 419 for references, examples, and details on TRM commands and parameters.</p>
Parameters	<p>Parameter “templates” are provided as a guide for using the correct parameters for whichever CounterACT command you choose. To select parameters:</p> <ol style="list-style-type: none"> Click the browse button  to get the Parameters dialog. Click Templates. Select the template that matches the command you chose. (For example, if you chose the command Quarantine Node, select Quarantine Node from the Templates drop-down. This would give you a default expression: <code>ip=\$ip,length=\$length,overwrite=\$overwrite</code>) Modify the default expression provided by the template with either hard-coded values or velocity expressions. (For example, <code>ip=\$ip,length=\$length,overwrite=\$overwrite</code> could be edited to set IP address to a velocity expression for attacker address, length could be set to 1 hour, and overwrite set to “yes” as follows: <code>ip=\${attackerAddress},length=1,overwrite=1</code>) Click OK on the Parameters dialog to save your changes. <p>See “TRM Command Syntax and Examples” on page 419 for references, examples, and details on TRM commands and parameters.</p> <p>You can use velocity expressions for the values as described in “Adding and Editing Command Parameters” on page 418. The Attributes list provides velocity expressions for all event fields and an option to add <code>\$selectedItem</code> as an attribute.)</p>




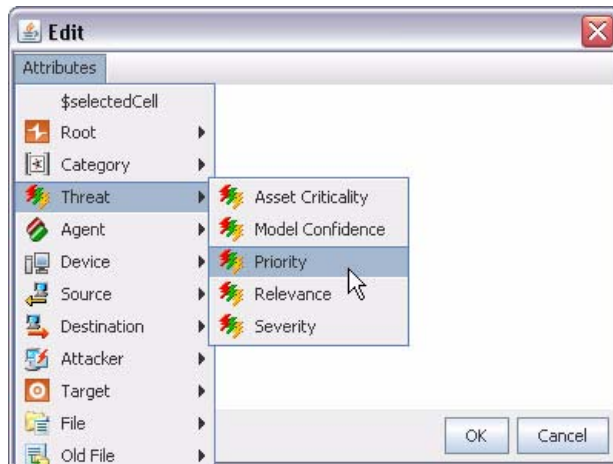
Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

Adding and Editing Command Parameters

The Attributes list includes velocity expressions for all event fields and an option to add `$selectedItem` as an attribute.

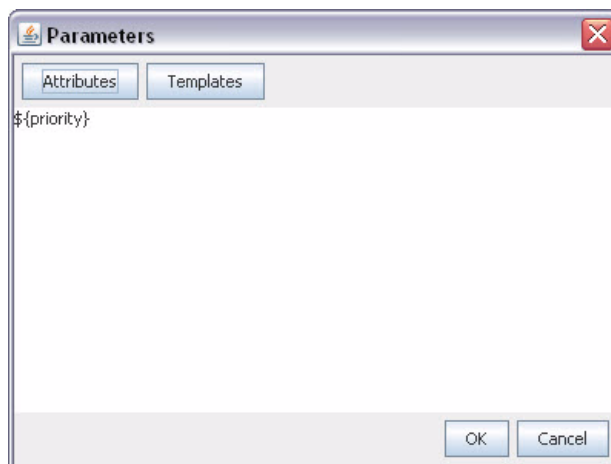
Provide **Parameters** for a command as follows:

- 1 Click the browse button  to get the Parameters dialog.
- 2 Click **Attributes** to get a list of variables and velocity expressions.



- 3 Select the expression you want to add.

The expression is added to the Edit Attributes scratch pad as a parameter.



- 4 You can continue adding expressions, which will be chained together.

For example, selecting Threat > Priority from the Attributes list results in this parameter being placed on the scratch pad:

`${priority}`

Subsequently selecting Attacker > Address, updates the scratch pad entry with chained-together expression:

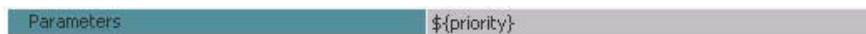
```
${priority} ${attackerAddress}
```



The Parameters dialog is an editable scratch pad. In addition to adding velocity expressions from the Attributes menu and Templates for CounterACT command parameters, you can type new expressions directly into the dialog. Also, you can select (with the mouse) and edit existing expressions (with keyboard commands) manually. (See also ["Removing a Command Parameter" on page 419](#))

- 5 When the Parameters scratch pad reflects the expression(s) you want to include as command parameters, click **OK**.


The parameter(s) you added are reflected on the Attributes tab in the Command Editor.



Be sure to click **Apply** or **OK** on the **Command Editor** to save changes to command parameters along with any other changes to the command that you want to retain.

Removing a Command Parameter

To remove a command parameter:

- 1 Click the browse button  to get the Parameters dialog
- 2 Select the parameter in the scratch pad and hit the Delete key on your keyboard.
- 3 Optionally, if you want to add a new parameter to replace the one you are deleting, do so by following steps described in ["Adding and Editing Command Parameters" on page 418](#).
- 4 Click **OK** on the Parameters dialog.
- 5 Click **Apply** or **OK** on the **Command Editor** to save your changes.

TRM Command Syntax and Examples

The [Parameters Templates](#) provided for CounterACT commands give you a start at including appropriate parameters, but in order to construct workable TRM commands, you need to understand TRM command syntax so that you can modify the template defaults appropriately.

The best reference is the *NSP SOAP API Reference Guide for ArcSight NSP*. A number of Simple Object Access Protocol (SOAP) calls for TRM actions have been enabled in common event format (CEF), and these are the TRM CounterACT commands currently available in the ESM Console as integration commands. (See ["TRM Commands and Parameters Reference" on page 419](#))

Another option is to look at the configuration XML for your CounterACT connector to get a quick view of the TRM commands and parameters. This XML file is commented and can provide some help. (See ["CounterACT XML Files" on page 420](#) and ["Example of CounterACT Command XML" on page 420](#).)

TRM Commands and Parameters Reference

For a complete description of TRM commands and parameters, please refer to the *NSP SOAP API Reference Guide for ArcSight NSP* appendix on "Common Event Format",

specifically the “CEF-Enabled NSP Actions”. Event names are listed in a table next to the associated SOAP call. Find the TRM commands in the list of SOAP calls and take the link to its SOAP call reference page. (For example, the event “Quarantine Node” is associated with the SOAP call “TRM: Quarantine Node - Simple Quarantine Node”.)

CounterACT XML Files

You can use the CounterACT configuration XML files as a rough guide for how to define values for TRM command parameters. To access the CounterACT configuration XML file, select Connectors in the Navigator, right-click on the CounterACT SmartConnector and do one of the following:

- Choose **Send Command > Tech Support > Get Configuration XML** and save the file. (This gets a copy of this file directly from the SmartConnector. In some cases, this file might be more up-to-date than the one on the Manager.)

Or

- Choose **Export Connector Configuration As XML** and save the file. (This gets the version of this file that is currently on the Manager.)

Example of CounterACT Command XML

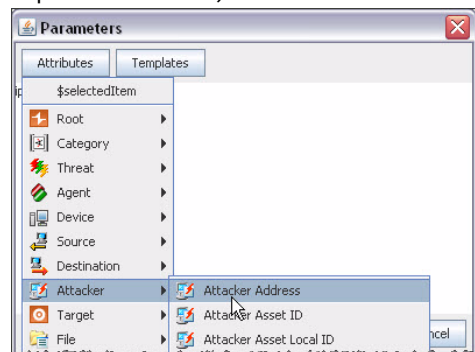
Here is the configuration XML for the CounterACT “Quarantine Node” command, which you can use as a guide to provide appropriate values for the CounterACT parameters you get from the parameter templates:

```
<Command Description="Quarantine Node"
  DisplayName="Quarantine Node" Name="quarantine">
  <Parameters>
    <Parameter ContentType="-1"
      Description="IP to quarantine" Name="ip" Prompt="IP to quarantine"/>
    <Parameter ContentType="-1"
      Description="Time to quarantine" Name="length" Prompt="Time to quarantine"/>
    <Parameter ContentType="-1"
      Description="Overwrite(0:No,1:Yes)" Name="overwrite" Prompt="Overwrite(0:No,1:Yes)"/>
  </Parameters>
</Command>
```

The TRM command in this example is used to quarantine a node by IP address. This command has three parameters: `ip`, `length`, and `overwrite`. In the Parameters field for this command, we use hard-coded values for `length` and `overwrite`, but use a velocity expression to derive the attacker address for a selected event:

```
ip=${attackerAddress},length=1,overwrite=1
```

The velocity expression `${attackerAddress}` is obtained from choosing **Attacker > Attacker Address** on the Parameters dialog available on the Parameters field. (Click the browse button to get the Parameters dialog, then click Attributes to get the velocity expression chooser.)



We are choosing to quarantine for 1 hour (`length=1`) and to overwrite the value (`overwrite=1`). The XML file provides some guidance in its comments, but for a full explanation of CounterACT command syntax (including appropriate parameter values), please refer to the *NSP SOAP API Reference Guide for ArcSight NSP*, as explained in [“TRM Commands and Parameters Reference” on page 419](#).

Creating and Editing Configurations

Configurations provide a way of grouping similar commands and specifying common options for where on the Console UI the commands will be available (*contexts*), how command results will be displayed (*renderer*), and where commands will run (scripts run locally; others, like CounterACT TRM commands, can have one or more remote *targets*). This is partly a matter of preference (about how you want to group, organize, and present commands to ESM Console users), and partly a matter of which commands belong together.



Configurations can include only commands of the same type (script, URL, or CounterAct). Commands that share a configuration use the same renderer, contexts, and (if relevant) targets. You might want to make finer-grained groupings; for example, sub-groups of scripts or CounterACT commands.

For example, you might group a set of CounterAct TRM commands that deal with quarantine of nodes into a single configuration. Or you might group a set of URL-based commands used for searching and researching on particular types of events (via Google Searches, Knowledge Base articles, and so forth).

Setting up *configurations* is a step in a multi-part process of making a set of integration commands available to Console users. (Other tasks include setting up commands, targets, and user login parameters).

This topic explains how to add and edit the *configuration* portion of an integration command solution. For an overview of the integration commands feature, see [“Integration Commands” on page 405](#). For more details on the relationship between commands, configurations, and targets, see [“How it Works” on page 407](#).

To create a configuration:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Configurations** tab.
- 2 Right-click a group (folder) where you want to create the configuration, and select **New Configuration**. This launches the Configurations Editor in the Inspect/Edit panel.
- 3 Fill in the fields on Attributes, Context, Commands, and Targets tabs as described in:
 - ◆ [“Configurations Attributes” on page 423](#)
 - ◆ [“Configurations Contexts” on page 424](#)
 - ◆ [“Configurations Commands” on page 425](#)
 - ◆ [“Configurations Targets” on page 426](#) (for configurations where commands will run on remote targets)

Inspect/Edit

Configuration: Google Search

Attributes Context Commands Targets Notes

Type

Configuration

Name	Google Search
Renderer	Internal Browser
Allow Multi Select	<input checked="" type="checkbox"/>

Common

Resource ID	eHZ2J+xsBACE-zxEFPjb0A==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

Assign

Owner	
Notification Groups	

Parent Groups

Samantha's Integration Configurations	/All Integration Configurations/Personal/Samanth...
---------------------------------------	---

Creation Information

Created By	admin
Creation Time	25 Aug 2008 13:25:03 PDT
Time Since Creation	9 day(s) 5 hour(s) 12 min(s) 21 sec(s)

Last Update Information

Last Updated By	admin
Last Update Time	26 Aug 2008 16:36:31 PDT
Time Since Last Update	8 day(s) 2 hour(s) 53 sec(s)

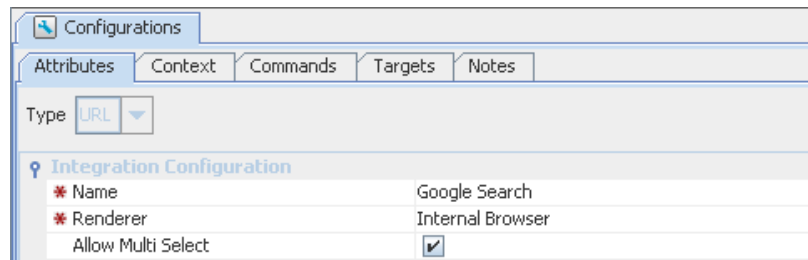
(Name)
(Description)

OK Cancel Apply Help

- 4 Click **Apply** or **OK** to add the new configuration.

Configurations Attributes

Define the configuration name, renderer and other basic details for the configuration on the Configurations **Attributes** tab.



Integration Configuration	
Name	Google Search
Renderer	Internal Browser
Allow Multi Select	<input checked="" type="checkbox"/>

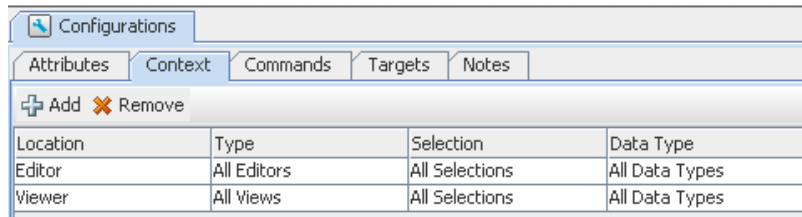
Attribute	Description
Type	<p>Choose the type of configuration from the drop-down menu:</p> <ul style="list-style-type: none"> • Script • URL • CounterACT <p>Note: The configuration type must match the command types you plan to include in the configuration. (See “Command Types” on page 414.) Once the configuration is saved, the configuration type is not editable. This setting influences choices on other options for the configuration, such as the Renderer.</p>
Name	A user-friendly, informative name for the configuration that (preferably, one that indicates the commands contained in it).
Renderer	Select how the output of the command will be rendered. The renderers available depends on the configuration Type chosen.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552.](#)

Configurations Contexts

Use controls on the Configurations **Context** tab to add, edit, or remove contexts in a configuration.

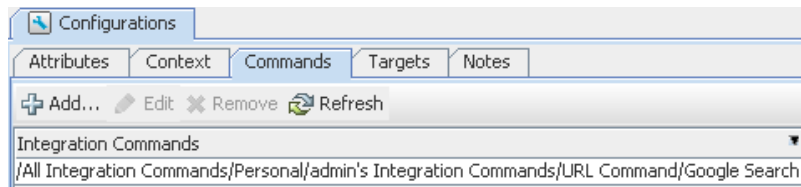


- Click the fields under Location, Type, Select, and Data Type to get drop-down menus with which to select contexts in the Console UI where the command will be available and to which selections it will apply.

Attribute	Description
Location	View where in the ESM Console the command will be available. For example: <ul style="list-style-type: none"> • Viewer, for the Viewer panel where Views of active channels, dashboards, and so on are shown • Resource, for the Navigator Panel resource tree • Editor, for resource editors
Type	Contexts in the Console panels where the command will be available. Available types vary depending on the location you choose. For example, if you choose Viewer for the location, you can specify types of “views” where you want the command to display, such as Grid View, Chart View, various List entries, Dashboards, Query Viewers, and so on.
Selection	User selection or subset of it that will be fed into the command. Options can include All Selections, Selected Cell, Selected Row, Selected Attribute.
Data Type	Data type for the parameters fed into the command (derived from the Selection). Options include: <ul style="list-style-type: none"> • All Data Types • IP Address • MAC Address • Date • Double • Integer • Long • Resource • String

Configurations Commands

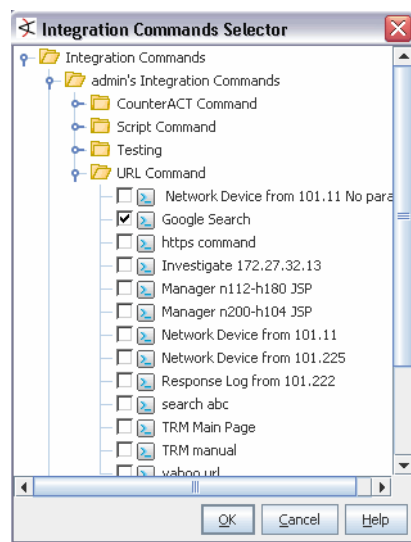
Use controls on the Configurations **Commands** tab to add, edit, or remove commands in a configuration.



Adding a Command to a Configuration

On the Configurations **Commands** tab:

- Click **Add** to bring up the Commands Selector dialog.



- Navigate to and click (checkmark) the commands you want to add, and click **OK**.
The commands are added to the list. (You can add multiple commands to a single configuration.)

Editing Commands in a Configuration

On the Configurations **Commands** tab:

- Select the command you want to edit and click **Edit**.
- This provides a shortcut into the **Command Editor** for the selected command. See [Step 3 on page 414](#) and ["Command Types and Attributes" on page 415](#) for information on editing the command.

Removing Commands from a Configuration

On the Configurations **Commands** tab, select a command in the list and click **Remove**.

Configurations Targets

Use controls on the Configurations **Targets** tab to add, edit, or remove targets in a configuration.



If you plan to add remote targets to a configuration, you need host information for the remote servers and login credentials if authentication is required.

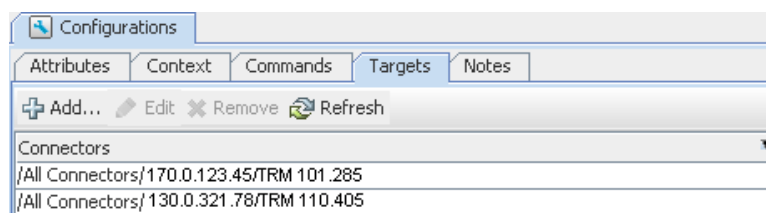
If you plan to add remote NSP TRM targets to a configuration, you need the following:

- Access to deployed TRM servers
- *If you plan to access TRM via CounterACT commands*, you need one or more CounterACT SmartConnectors installed and configured to connect to your TRM servers
- *If you plan to access TRM via URL commands*, you need a TRM Web client to derive URL commands. For TRM URL commands, you also need to define a target separately as described in [“Specifying Targets” on page 427](#).
- *If you plan to access TRM via URL commands*, you also need TRM user login credentials for the TRM servers you plan to use. If you are an ESM Administrator configuring TRM commands for multiple users who will send TRM commands each using their own TRM logins, you will need the TRM login credentials for all those users in order to configure them as ESM integration commands. (See [“Setting User Login Parameters” on page 428](#).)

See also, [“Configuring the SmartConnector” on page 498](#), the *CounterACT SmartConnector User Guide*, and also the ArcSight™ Network Synergy Platform (NSP) documentation.

Adding a Target to a Configuration

Targets are applicable to Threat Response Manager (TRM) commands sent to a TRM server via a CounterACT SmartConnector (which is treated as the “target” for TRM commands), and any other commands that you want to send to a remote server.



- Click **Add** to bring up the Connectors Selector dialog.
- Navigate to and click (checkmark) the target server you want to add, and click **OK**.

Editing Targets in a Configuration

- Select the target you want to edit and click **Edit**.
- This provides a shortcut into the **SmartConnector Configuration** Editor for the selected connector or target. (See [“Configuring the SmartConnector” on page 498](#), and also the *CounterACT SmartConnector User Guide*.)

Removing Commands from a Configuration

On the Configurations **Contexts** tab, select a target in the list and click **Remove**.

Specifying Targets

Optionally, you can specify targets (remote servers where one or more commands will run). For example, Threat Response Manager (TRM) commands can be sent to a TRM server via a Web URL.

Setting up *targets* is a step in a multi-part process of making a set of integration commands available to Console users. (Other tasks include setting up commands, configurations, and user login parameters).

This topic explains how to add and edit the *configuration* portion of an integration command solution. For an overview of the integration commands feature, see [“Integration Commands” on page 405](#). For more details on the relationship between commands, configurations, and targets, see [“How it Works” on page 407](#).

To add a new target, do the following:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Targets** tab.
- 2 Right-click a group (folder) where you want to create the target, and select **New Target**. This launches the Command Editor in the Inspect/Edit panel.
- 3 Fill in the fields as described below.
- 4 Click **Apply** or **OK** to add the new target.

Target Attributes

The only target attribute you need to provide is a user-friendly name for the server.

Attribute	Description
Name	Name for the remote server where the command will run.

Target Integration Parameters

Targets are used only for URL configurations, where you parameterize the Web host target of the URL, and sometimes login credentials. Type directly into the fields to define a parameter, as described below.

Parameter	Type	Value
TRM_HOST	Text	TRM
TRM_AUTHENTICATION	Password

Field	Description
Parameter	Parameter name, as specified in the command definition related to this target. For example: <ul style="list-style-type: none"> • TRM_HOST could be a parameter for the name of a TRM server • TRM_AUTHENTICATION could be a parameter for a TRM password
Type	Parameter type. Choose Text or Password from the drop-down menu. Password type parameters are automatically encrypted.

Field	Description
Value	Hard-coded value for the parameter. For example: <ul style="list-style-type: none"> a host name or IP address if the parameter is for a server a password if the parameter is for login credentials

To add a new parameter, click **Add**. This gives you a new row in which to enter Parameter, Type, and Value information. You can add multiple parameters to a target.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 552](#).

Setting User Login Parameters

Login credentials to remote targets servers can be specified.

- For URL commands on remote targets, login credentials can be defined as part of the Target definition, as described in [“Specifying Targets” on page 427](#). (Choose Navigator > Integration Commands > Targets tab, select and edit a target or create a new one, then click the **Integration Parameters** tab on the **Targets Editor**.)

Parameter	Type	Value
TRM_HOST	Text	TRM
TRM_AUTHENTICATION	Password	*****

If login information is defined here, everyone who uses the command will be using the same credentials to log in to the remote target server.

- For URL commands on remote targets (including TRM Web commands) and script commands that run locally, you can define login credentials as a part of ESM User configurations. (Choose Navigator > **Users**, select and edit a user or create a new one, then click the **Integration Parameters** tab on the **User Editor**.)

Parameter	Type	Value	Targets
TRM_AUTHENTICATION	Password	*****	TRM Server

Defining login information as part of user accounts gives you the flexibility to configure multiple users in ESM, each with different logins. In this case, login credentials are not tied to the command target, but rather associated with individual users.

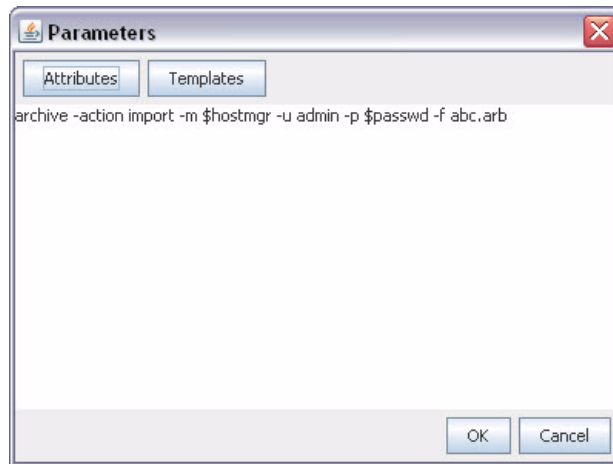
Setting Logins and Other Parameters to Prompt for Values at Runtime

You can set parameters for which you would like to prompt users to specify values at runtime (e.g., user name and password, host names, IP addresses, and other command options).

When an integration command runs (i.e., when a user selects an integration command in some context on the Console), the command first looks for any required parameter values in a variety of sources, including in the command statement itself, in the defined context, on the user account, on the target (if there is one), and so forth. If it doesn't find parameter values in any of these places, the system prompts the user to type in the values.

You can include login and other parameters as flags on a script command that runs against a server, as shown here for the ESM archive command which runs on a Manager. When this command is run, it will prompt the user for an ESM Manager host name and administrator password. (It will not prompt for the user name, `admin`, since this already is provided in the command statement.)

```
archive -action import -m $hostmgr -u admin -p $passwd -f abc.arb
```



Please refer to [“Entering/Saving Command Parameters at Runtime” on page 431](#) (in [Running Integrated Commands](#)), for an example of the run-time prompts users will see when they run this command.

Access Control Lists (ACLs) on Integration Commands

You can configure access control lists (ACLs) on integration commands, since they are resources in ESM (and ACLs can be configured on resources). For details on how this works in general, please see [“Granting or Removing Resource Permissions” on page 444](#).

You can grant or limit read/write access to integration commands, integration configurations, and integration targets down to the *grouped resource* level for particular *user groups* by setting the setting ACL permissions on the resource group for any set of commands. Note that both the resources themselves and the users must both be in groups in order to work with them in this way.

For example, suppose you have a group of TRM CounterACT commands. The commands are grouped in a command group called “CounterACT Investigate Commands”, and associated with a configuration called “CounterACT Investigate Configurations”. You have

two users (Darren and Larry) in a group called “Analyzers” to whom you want to give permissions to simply *run* these commands (not edit them). To do this, you would choose **Users** in the Navigator, select the Analyzers group, right-click and choose **Edit Access Control**. On the Resources tab, add both the CounterACT Investigate commands and configurations groups, and give read access on both. (Add the resource Integration Command and select the appropriate command group in the selector, and add the resource Integration Configuration and select the appropriate configuration group in the selector, then click the *Read* checkboxes for each under Resource Targets and save the ACLs for the user group.)



- User group ACLs with *read* permissions on the integration command and configuration resources groups can *run* commands.
- User groups with *read and write* permissions on integration command and configuration resource groups can *run and edit* these commands.
- Commands can be configured to prompt for input parameter values when the command runs. If you want to give users permissions to *save the parameter values* required at command runtime, then you also must give *read and write* permissions to the associated *Integration Targets* groups on the ACL editor for the user group.

You can organize users and the commands, configurations, and targets into various groups to fit with the permissions schemes you want to create. You might, for instance, want to create one set of TRM *Investigate* commands/configurations and give those permissions to one set of users (e.g., Darren and Larry in the Analyzers group). Then you could create another set of TRM *Quarantine* commands/configurations and give those permissions to a different group of users (e.g., Samantha, Endora, and Arthur in Analyzer Administrators group). It might be appropriate for this second group to have more authority, and therefore you would grant a broader set of permissions to it (e.g., both Investigate and Quarantine permissions per the ACL settings on the Analyzer Administrators group).

Running Integrated Commands

After commands are configured, they are available in various contexts in the Console.

For example, suppose you have a configuration for a set of commands with the contexts set as follows:

Location	Type	Selection	Data Type
Viewer	Grid View	Selected Cell	IP Address

This means that the given commands will be available on right-click context menus on any row in a Viewer “grid view” (e.g., active channels, list views, and so on), and that the value of an IP address in the selected cell will be provided as a parameter to the command.

If one of the commands in this configuration was an NSP TRM “Quarantine Node” command, then to use the command you would do the following:

- 1 Bring up an active channel, session list, active list, dashboard, or other resource in the viewer that shows, for example, a suspicious device, machine, or user that you want to quarantine.
- 2 Find the row on the Viewer display that contains the suspicious entity, and select a cell in that row that contains the source IP address (e.g., Attacker Address).

- 3 Right-click over the cell with the source IP address (e.g., Attacker Address), and choose **Integration Commands > Quarantine Node**.

This launches the selected command, using the IP address for the selected cell as the parameter for the command.

In general, a right-click on any context in the Console UI for which integration commands have been configured will show all integration configurations.

You can also create a new integration configuration from within a context. To do this, right-click anywhere in the UI,

Entering/Saving Command Parameters at Runtime

Commands can be configured to prompt for parameter values at runtime (as described in [“Setting Logins and Other Parameters to Prompt for Values at Runtime” on page 429](#)). For example, parameters might ask for a particular host name as command input, an IP address against which to run a command, or login credentials to a target server.

Parameter	Type	Value
passwd	Text	
hostmgr	Text	

If you launch a command that prompts for input, enter the appropriate text in the “Value” field for each required parameter.

If you have appropriate permissions, you have the option to save parameter values with the target or with your user account so that you don’t have to re-type them each time you run the command.



In order to save parameter values at runtime, you need to belong to a group with *read and write permissions* to the associated *targets*.







Network Tools as Integration Commands

For ESM v.4.5, the following standard network tools (see [“Using the Network Tools” on page 72](#)) are also provided as integration commands. Eventually the legacy network tools will be phased out but for this release the Console still includes both.

This new set of network tools provided as integration commands differ from the legacy tools in a number of ways. With network tools integrated commands you can:

- **Define contexts for where tools show up on the Console.** Integrated network tools can be customized and configured for availability in all types of views (charts, graphs, tables), and in the navigator, editors, and so on. Legacy network tools are available only on grid views; you cannot define the context.
- **Select and run commands on navigator tree items, all types of views, and editors items.** With integrated network tools, you can select various items in chart and graph views, on the editors, and in the navigator tree. Legacy network tools are limited to running only on the selected cell in a grid view (table) in the Viewer.

- **Configure access control lists (ACLs).** You can grant or limit access to integrated network tools commands for particular user groups by setting the setting ACL permissions on the tools resource group. The integrated network tools reside under /All Integration Configurations/ArcSight System/Tools. You can control access to the tools commands and configurations groups (select the Tools group, right-click, and choose **Edit Access Control**) as described in [“Granting or Removing Resource Permissions” on page 444](#). You can organize users and the tools themselves into various groups to fit with the permissions scheme you want to create. With the legacy network tools, you do not have this ACL option. See [“Access Control Lists \(ACLs\) on Integration Commands” on page 429](#) for more information.

Tree	Icon	Resource
Nslookup		Resolves an IP address to a host or domain name or vice versa.
Ping		Determines whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response.
PortInfo		Lists standard usage, for example, WWW, FTP, and so on for a specified port number.
Traceroute		Shows the path from the ArcSight Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between.
WebSearch		Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells.
Whois		Looks up who is behind a given domain name; information might include addresses and telephone numbers.

These are configured with default velocity expressions for parameters. You can edit the commands and configurations for these network tools as needed (and add new ones of your own).

To add a tools command or re-configure one of the provided network tools, choose **Tools > Local Commands > Configure**, select a tool and click **Edit**.

To run a network tool, select an IP address in a grid view (e.g., active channel, list, data monitor) and select **Integration Commands > <Network Tool>** from the context menu (e.g., **Integration Commands > ping**).



The Send Logs command is not configured as an integrated command. See [“Using the Network Tools” on page 72](#) and [“Send Logs” on page 758](#) for information on that command.

Chapter 19

Knowledge Base Authoring

These topics explain how to do the basic tasks of managing Knowledge Base articles.

[“Managing Knowledge Base Articles” on page 433](#)
[“Managing Knowledge Base Article Groups” on page 435](#)
[“Getting Knowledge Base Updates” on page 436](#)
[“Associating Knowledge Base Articles” on page 436](#)

Managing Knowledge Base Articles

Creating Knowledge Base Articles

- 1 On the Navigator panel's drop-down menu, choose the Knowledge Base resource tree.
- 2 Right-click a group and choose **New Article**.
- 3 In the Knowledge Base Editor, select the **Article** tab.
- 4 On the Article tab, type in the **Name** text field.
- 5 Optionally use the **Summary** field to add a brief description of the article.
- 6 Optionally enter a different name for the information source in the **Author/Credits** field. Your user name is the default.
- 7 The **Origin URL** text field contains the URL or directory path to the page or file that contains the article's information. Use one of these methods to provide this string:
 - a Type the URL or directory path to the page or file, or
 - b Click **Upload File** to select and save an HTML file, with a .htm or .html extension, from your local drive, or
 - c Click **Launch Editor** to use an editor to create a new file. If an editor was not set prior to using the **Launch Editor** button, the Preferences dialog box appears so you can point to one.
 - d In the **Preferred text/HTML Editor** text field, type the path to a text editor or click the **Browse** button to select a text editor.
 - e In the editor, create a new file containing information on the article.
- 8 Choose the **Import** or **Reference** option, depending on how you want the Original URL page or file to appear in the article.

Use **Import** to copy the HTML file into the Knowledge Base. The page or file will remain linked to, and continue to be updated from, its original location.



When you select **Import**, only the content between the body tags of the HTML page appear. Therefore, you should use **Reference** when the HTML page uses JavaScript, uses frames, or includes images. Choose **Import** when you use an editor to create a file specified in the **Origin URL** text field.

Choose **Reference** if you want the page or file to remain static. The URL or the directory path to the page or file appears as a link in the article.

- 9 Enter a summary of the article in the **Summary** text field.

- 10 Click **Preview** to see the article as it will appear in a browser window.

Use the **Preview** button to assist you in selecting either the **Import** or **Reference** radio button for HTML pages.

- 11 Click **Apply** to enter the changes and keep editing or click **OK** to save and close.

Showing a Knowledge Base Article

In the Knowledge Base window, right-click an article and choose **Show Article**.

Editing a Knowledge Base Article

- 1 In the Knowledge Base window, right-click an item and choose **Edit Article**.

- 2 In the Knowledge Base Editor, select the **Article** tab.

- 3 On the Article tab, make edits.

For more information, see [“Creating a Knowledge Base Article Group” on page 435](#).

- 4 Click **Preview** to see how the article will appear in a Web Viewer tab.

- 5 Click **OK**.

Moving or Copying a Knowledge Base Article

- 1 In the Knowledge Base window, navigate to an article and drag and drop it into another group.

- 2 Choose **Move** to move the article, **Copy** to make a separate copy of the article, or **Link** to create a copy of the article that is linked to the original article.

If you choose **Copy**, you create a separate copy of the article that will not be affected when the original article is edited. If you choose **Link**, you create a copy of the article that is linked to the original article. Therefore, if you edit a linked article, whether the original or the copy, all links are edited as well. When deleting linked articles, you can either delete the selected article or all linked article copies.

Deleting a Knowledge Base Article

- 1 In the Knowledge Base window, right-click an item and choose **Delete Article**.

- 2 In the dialog box, click **Yes**.

Managing Knowledge Base Article Groups

Knowledge Base article groups can be used to organize similar or related articles in a single location. For example, you could create a Denial of Service group to store specific articles about Denial of Service attacks such as a Ping Flood attack.

Groups and articles can be managed with drag and drop functionality. You can move or copy groups and articles into other groups within the Knowledge Base resource tree. If a group is deleted, the articles within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Knowledge Base Article Group

- 1 In the Navigator panel's drop-down menu, choose the Knowledge Base resource tree.
- 2 In the Knowledge Base window, right-click a group and choose **New Group**.
A name text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Rename**.
- 2 In the name text field, rename the group.
- 3 Press **Enter**.

Editing a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, type in the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Knowledge Base Article Group

- 1 In the Knowledge Base window, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Delete Group**.

- 2 In the dialog box, click **Yes**.

Getting Knowledge Base Updates

In the Knowledge Base resource tree, the **Refresh** right-click option refreshes the tree from the selected level, showing changes made to the sub-trees below that group. Supposing a group or article name was modified through another ArcSight Console, or a group or article was deleted, renamed, or moved from another ArcSight Console, refresh will show those changes.

Refreshing the Knowledge Base Tree

In the Knowledge Base resource tree, right-click the **Knowledge Base** group or article and choose **Refresh**.

Associating Knowledge Base Articles

Knowledge Base groups and articles can be associated with other resources such as cases, reports, or filters.

Associating resources with Knowledge Base groups or Articles

- 1 Use the Navigator panel to locate an individual or group target resource, e.g., a case or case group.
- 2 Right-click the resource and choose **Knowledge Base > Associate with**.
- 3 Use the Knowledge Base Article Selector to find and select an article to associate with the resource.
- 4 Click **OK**.

Associating Grid View Elements with Knowledge Base Articles

- 1 In a Viewer panel grid view, right-click an event attribute and choose **Knowledge Base > Associate > Cell/Row/Column with**.
- 2 Use the Knowledge Base Article Selector to find and select an article to associate with the grid view's selected cell (data), row (event), or column (attribute).
- 3 Click **OK**.

Chapter 20

Managing Resources (for Administrators)

This chapter discusses the administrator tasks necessary to manage ArcSight ESM.

- [“Managing Users” on page 438](#)
- [“Managing Permissions and Resources” on page 443](#)
- [“Locking and Unlocking Resources” on page 454](#)
- [“Modeling Your Network and Managing Assets” on page 456](#)
- [“Managing Filters” on page 480](#)
- [“Managing Notifications” on page 482](#)
- [“Managing File Resources” on page 488](#)
- [“Managing Packages” on page 491](#)
- [“Managing SmartConnectors” on page 498](#)
- [“Selecting Resources” on page 533](#)
- [“Finding Resources” on page 534](#)
- [“Visualizing Resources” on page 537](#)
- [“Viewing Resources in Grids” on page 540](#)
- [“Validating Resources” on page 540](#)
- [“Extending Audit Event Logging” on page 547](#)
- [“Managing Partitions” on page 547](#)
- [“Managing Customers” on page 551](#)
- [“Saving Copies of Read-Only Resources” on page 552](#)
- [“Using the Image Editor” on page 552](#)
- [“Common Resource Attribute Fields” on page 552](#)

Managing Users

You manage numbers of users by organizing them into groups based on roles or other logical groupings, setting their permissions and passwords, and enabling or disabling their login functionality. Permissions to access specific ArcSight resources (for example, to create rules or reports) are granted to specific groups by editing the access control lists (ACLs) for those groups.

All ArcSight user group memberships and permissions are stored in the ArcSight Database. When users log in, they are allowed to perform any operations for which they are granted permission through their membership in one or more groups.

Handling Users

When you create an ArcSight user, that person automatically receives access to a set of resource groups. Users can store, create, edit, or delete resources within their groups without jeopardizing other users' resources.

Creating a User

- 1 In the Navigator panel drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click the group in which to place the new user and choose **New User**.
- 3 In the **User Editor**, fill in these fields on the **Attributes** tab in the **Login** section:

User Fields	Description
User ID	User name for login ID. This is a required field.
User Type	<p>Choose a user type from the drop-down menu. This is a required field.</p> <p>The currently supported user types are:</p> <ul style="list-style-type: none"> • Normal User: Has full privileges to use the ArcSight Console or ArcSight Web client, and all tools. Only apply this user type to accounts that actually need access to the ArcSight Manager. • Management Tool: Has only the privileges needed to run certain management tools used in conjunction with network management products. • Forwarding Connector: Has only the privileges needed by the ForwardingConnector. • Archive Utility: Has only the privileges needed to run the archive utility. Access to specific resources is controlled through ACLs. • Connector Installer: A specialized identity used only to add SmartConnectors to the system. • Web User: Has privileges to use the ArcSight Web client only (not the ArcSight Console or other tools). <p>See also "About the System User" on page 441.</p> <p>For more information on users and user types, see "Users" on page 783 and "User Types" on page 783 in the Reference Guide.</p> <p>Note: Only users with "Normal User" accounts can log in to the Console or an ArcSight Web client.</p>

User Fields	Description
Login Enabled	<ul style="list-style-type: none"> Select the Login Enabled checkbox to <i>give the user login privileges</i> (a checkmark indicates this feature is on): <div> Login Enabled <input checked="" type="checkbox"/> </div> Or leave it deselected and off (no checkmark showing) to <i>disable logins</i> for this user: <div> Login Enabled <input type="checkbox"/> </div> <p>Note: A user account login must be <i>enabled</i> to allow login access to the ESM Console. If you disable a login for a user account, the user cannot log into the Console with the credentials associated with the disabled account.</p>
External User ID	Optionally, provide an alternate, external user ID. (An external user ID might be relevant if you have user accounts from other applications feeding into ESM user database.)
Password	<p>Enter a password for this user. This is a required field.</p> <p>By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.</p> <p>(Passwords can be modified later as a part of editing user information. See "Resetting User Passwords" on page 440.)</p>
Confirm	Re-type the password to confirm it. This is a required field.

4 Fill in these fields on the **Attributes** tab in the **User** section:

User Fields	Description
Last Name	The user's last name.
First Name	The user's first name.
Title	The user's job title.
Department	The user's department.
Phone	The user's phone number.
Fax	The user's fax number.
E-mail	The user's e-mail address. Use the format user@host.domain. The "@" sign and host domain are required. E-mail addresses are not case-sensitive.
Pager	The user's pager number



For phone, fax, and pager numbers, parentheses (), dashes (-), and periods (.) are allowed. Alphabetic characters are not allowed.

5 In the **UserID** text field, enter a user login name. This field is required.

6 Click **OK**.

Editing a User

- 1 In the **Users** resource tree, right-click the user and choose **Edit User**.
- 2 In the **User Editor**, edit the text fields as described in the table above.
- 3 Grant or withhold login permission by selecting or deselecting the check box next to **Login Enabled**.
- 4 In the **Password** and **Confirm** text fields, edit the user password and confirm it by typing it again. These fields are required.

By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.

- 5 Click **OK**.

Resetting User Passwords

Administrators may also reset user passwords; for example, if a user's original password has been compromised or you want to make users update their passwords.

- 1 While logged into the Console as an administrator, choose the **Users** resource in the Navigator panel.
- 2 Right-click the user whose password you want to reset and choose **Reset Password**.

The ArcSight Manager assigns a new random password (8 characters, including numbers and letters) and sends it to the selected user's assigned e-mail address.



Be aware that sending a password by email can be dangerous as emails can be intercepted.

Alternatively, the following command on ArcSight Manager can be used to reset a user's password:

```
arcsight resetpwd
```

Moving or Linking a User

- 1 In the **Users** window, navigate to a user and drag and drop it into another group.
- 2 Choose **Move** to move the user or **Link** to create a copy of the user that is linked to the original user.

If you choose **Link**, you create a copy of the user that is linked to the original user. Therefore, if you edit a linked user, whether it is the original or the copy, all links are edited as well. When deleting linked users, you can either delete the selected user or all linked user copies.

Deleting a User

- 1 In the **Users** resource tree, right-click the user and choose **Delete User**.
- 2 In the dialog box, click **Delete** to delete the user and the listed user's resources or click **Disable Login** to disable the user.



By default, only ESM Administrators have permissions to delete users in a group. If you want to grant non-Administrator users permission to delete users in a particular group, you first need to provide *Write* access to the group by editing access to **User Groups** in the ACL Editor.

Starting with ESM v.4.5 GA, an additional step (providing *Write* access to user Reports) is necessary.

To grant non-Administrator users permissions to delete other users in a group, do the following:

- 1 In the `server.default.properties` file, set the `user.allowmodification=true`.
- 2 Restart the ESM Manager.
- 3 Log into the Console as Administrator, and select the **Users** resource in the Navigator.
- 4 Select the non-administrators group for which you want to provide permissions, right-click, and choose **Edit Access Control** to bring up the ACL Editor.
- 5 On the ACL Editor, click the **Resources** tab.
- 6 Select **Report** in the Resource drop-down menu, and click **Add** to bring up the Reports Selector dialog.
- 7 In the Selector dialog, select all users under `Reports/Shared/Personal/` and click **OK**. All users are shown as Resources targets.
- 8 Click to set **Read (R)** and **Write (W)** permissions as desired (e.g., a checkmark indicates the permission is granted or "on"). Any user in the group now has Edit access to Report groups showing **Write** access (i.e., where **W** is checkmarked), and therefore can delete users in this group.
- 9 Click **Apply** or **OK** to save your changes.

With *Write* permissions enabled on Reports for users you want to delete, members of this group can log into the Console and delete those users.

For more information, see ["Granting or Removing User Group Permissions" on page 447](#).

About the System User

Starting with ESM v4.0, a special user called the system user is created automatically when ArcSight ESM is installed. This user can lock and unlock ArcSight System Core content. (For more information about System Core content, see the *ESM Administrator's Guide*.)

The system user is configured as 'systemuser' by default. ArcSight recommends that you change this name to a non-standard name. This name can be changed only once. For example, once you change the name to 'coreuser', you cannot change this name again.



ArcSight strongly discourages you from logging in as the system user for regular ArcSight system administration tasks. The purpose of this user is special and its capabilities are limited. For example, the system user cannot use channels or dashboards, install ArcSight SmartConnectors, or log in to ArcSight Web.

Handling User Groups

User groups associate related users or groups of users. When a group is created within a group, the new group inherits the existing group's permissions.

Groups and users can be managed with drag-and-drop functionality. You can move or copy groups and users into other groups from the Users resource tree. If a group is deleted, the users within that group are also deleted, unless they are also contained by other groups.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.



You can grant or block non-administrator user access to deploy or un-deploy data monitors. These permissions are configured at the user group level.

For information on how to set user group permissions to enable or disable data monitors, see ["Controlling Who Has Permissions to Deploy Data Monitors" on page 452](#).

Creating User Groups

- 1 On the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click a group and choose **New Group**.
A name text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Linking User Groups

- 1 In the **Users** resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group or **Link** to create a copy of the group that is linked to the original group.

If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it is the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Setting Startup Views

You can define the set of active channel and dashboard resource groups that members of a given ArcSight user group will see by default when they first log in. This includes both Console and ArcSight Web users. These channels and dashboards are initial defaults only: once users begin changing the content of the Viewer panel, the Console and ArcSight Web follow their normal behavior of remembering the most recent state.

The default active channels and dashboards you select for user groups are listed in the User Group Editor on the Startup Views tab.

- 1 Right-click a user group in the Navigator panel's Users resource tree, and choose **Edit Group**.
- 2 In the User Group Editor, click the **Startup Views** tab, then the **Active Channels** or **Dashboards** tabs.
- 3 In either resource tab, click **Add** to open a resource selector dialog box.
- 4 Navigate to and select the appropriate active channels or dashboards to set as users' start-up resources, and click **OK**. Repeat this step to add more resources.
- 5 Click **Refresh** to update the current list of resources, or click **Remove** to take a selected resource off the list. Click **Edit** to change a selected resource in its own editor.
- 6 Click **Apply** to make changes and leave the editor open, or click **OK** to apply your changes and close the editor.

Managing Permissions and Resources

The subject of managing users is largely that of managing their access to and use of resources.

Editing Access Control Lists (ACLs)

The user groups ACL Editor has these tabs for viewing or editing permissions on resources, operations, user groups, events, and sortable field sets:

- Resources tab - Lists all resources available to the user group with either inspect or edit permissions, and lets you add/edit resource permissions.
- Operations tab - Lists operations for which this user group has permissions, and lets you add/edit operations permissions. (For example, a user group can have permissions to enable or disable data monitors.)
- User Groups tab - Lists the user groups with either inspect or edit access to the user group itself, and lets you add user groups.
- Events tab - Lists event filters for which this group has permissions, and lets you add/edit event filter permissions. This user group is permitted to see only events from the filters listed on the Events tab.
- Sortable Field Sets tab - Lists sortable field sets for which this user group has permissions. Lets you add/edit field set permissions.

See also, ["Access Control Lists" on page 571](#).



Always remember to have both ArcSight Console and ArcSight Web users log out and back in after changing user or resource access permissions, so they can see those changes.



The Resource ACL display shows relationships between users and groups, and how permissions are acquired for each of the user groups. Child groups inherit permissions from parent groups.

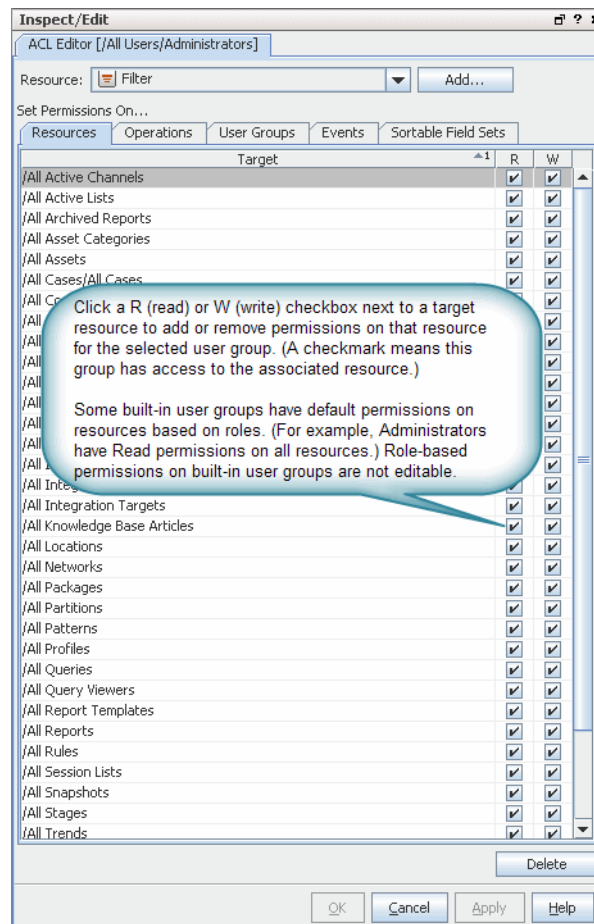
For example, consider the following scenario.

- A user logged in as Administrator (belonging to the group /All Users/Administrators) has read and write permissions by virtue of being in the Administrators group.
- All users have read permissions because they belong to the group /All Users/Default User Groups by default.
- A user logged in as an Analyzer Administrator has both read and write permissions because they inherit read permissions from the parent group (/All Users/Default User Groups) and get write permissions per the Analyzer Administrators child group.

Granting or Removing Resource Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Resources** tab.

The Resources tab lists all resources available to this user group with either inspect (**Read**) or edit (**Write**) permissions, and lets you add/edit resource permissions. Available resources are listed based on *user permissions*, so some might not show.



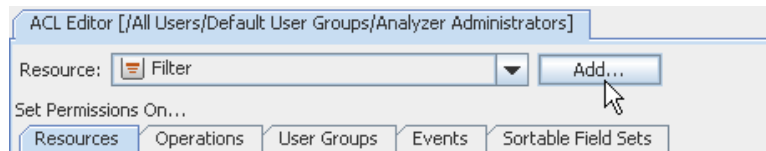
- 5 Add or remove permissions on a resource for this user group as follows.

- ◆ **To edit permissions on a resource *shown in the current list***, click the **(R)** read or **(W)** write checkbox next to a target resource to add or remove permissions on that resource.

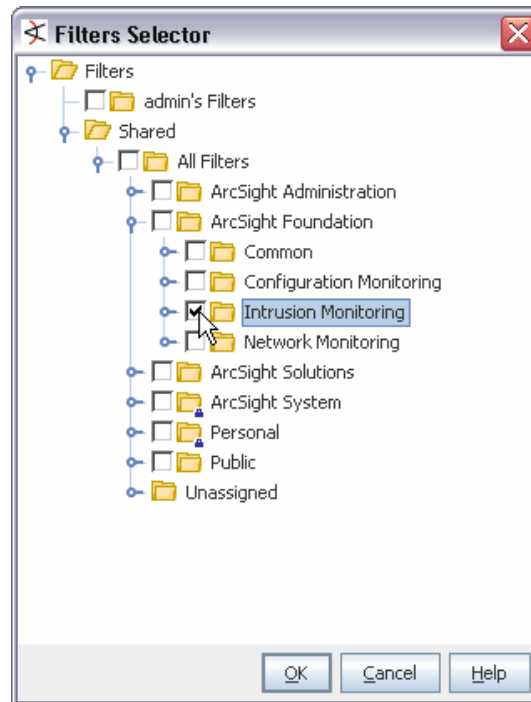
A checkmark means that this user group has access to the associated resource. A blank checkbox means this group does not have access to the resource.

Target	R	W
/All Active Channels	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/All Active Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ◆ **To add permissions for a resource *not shown in the current list***, select a resource from the Resource drop-down menu at the top of the Resources tab and click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the resources you want to add permissions for and click **OK**.



The resource you added will be listed as a target on the Resources tab and then you can edit its **Read/Write** permissions as needed.

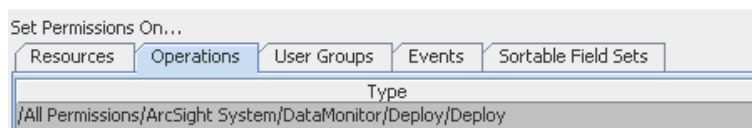
- ◆ To remove a resource from the list (and **remove all permissions on it** for this group), select the resource in the list and click **Delete**. (The Delete button is at the bottom of the Resources tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Resources permissions.

Granting or Removing Operations Permissions

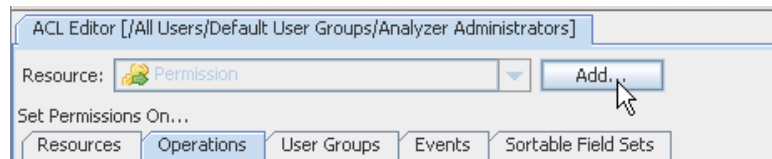
Starting with ESM 4.5, data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions by setting permissions on this particular "operation". For ESM v.4.5, the only operation available to set permissions on is data monitor deployment. It is likely that fine-grained permissions control will be added for other operations as needed. (See also, ["Controlling Who Has Permissions to Deploy Data Monitors" on page 452.](#))

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Operations** tab.

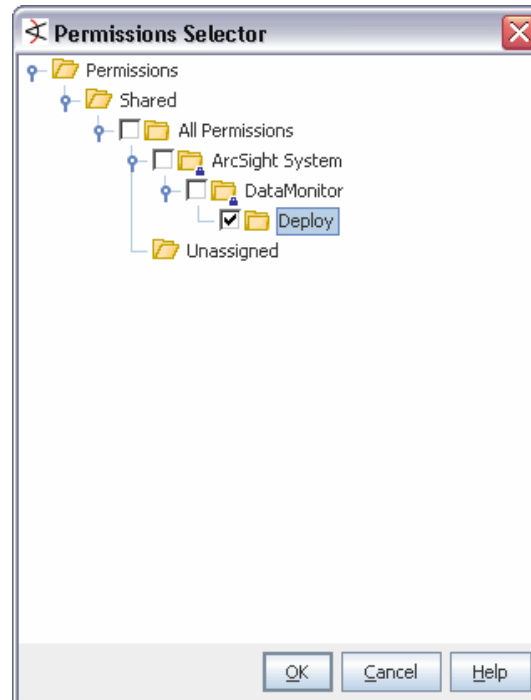
The operations for which this user group has permissions (if any) are listed.



- 5 Add or remove user group permissions to perform an operation as follows.
 - ◆ To add permissions to perform an operation not listed, click **Add**.



Select the operations you want to add permissions for and click **OK**.



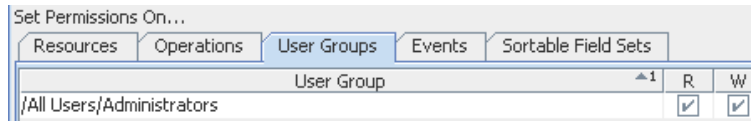
The list of Operations is updated to include the one you added. Operations listed are those this user group has permissions to perform.

- ◆ **To remove permissions to perform an operation**, select the operation in the list and click **Delete**. (The Delete button is at the bottom of the Operations tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

Granting or Removing User Group Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **User Groups** tab.

The User Groups tab lists all user groups for which members of the selected group have inspect (**Read**) or edit (**Write**) permissions, and lets you add/edit group permissions.



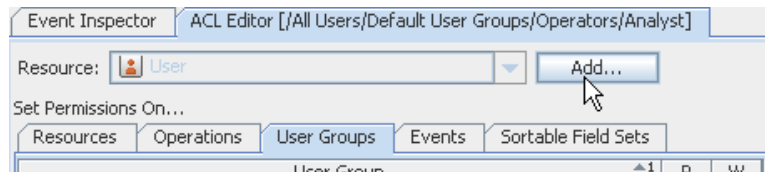
This is where you grant or deny members of the group you are editing permissions to edit their own user groups. Depending on your own user permissions, some user groups may or may not be shown, and Read/Write checkbox options may or may not be editable.

- 5 Add or remove permissions on a user group as follows.
 - ◆ **To edit permissions on a user group *shown in the current list***, click the **(R)** read or **(W)** write checkbox next to a target resource to add or remove edit permissions on that user group.

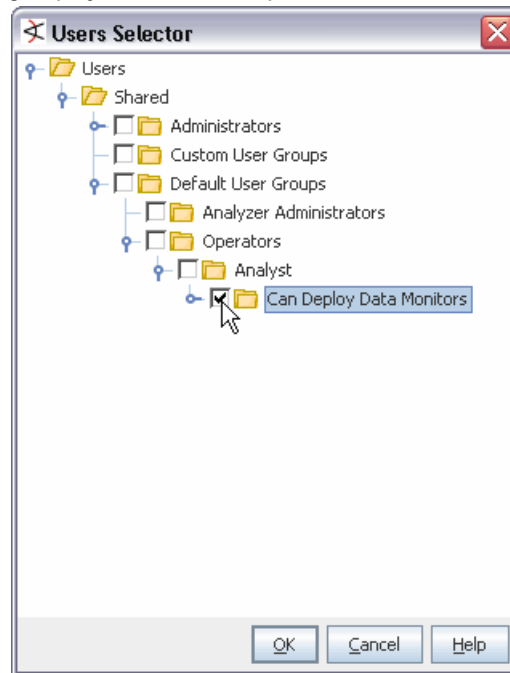
A checkmark means that this user group can edit permissions on the associated group. A blank checkbox means this group does not have edit permissions on it.

User Group	R	W
/All Users/Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ◆ **To add permissions on a user group *not shown in the current list***, click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the groups you want to add permissions for and click **OK**.



The user group you added is now listed on the User Groups tab and then you can edit its **Read/Write** permissions as needed.

User Group	R	W
/All Users/Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Users/Default User Groups/Operators/Analyst/Can Deploy Data Monitors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

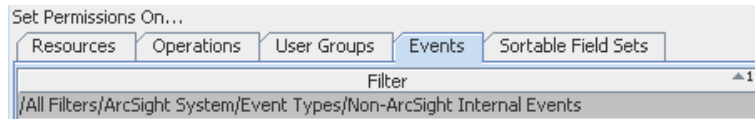
- ◆ To remove a user group from the list (and **remove all edit permissions on it**), select the user group in the list and click **Delete**. (The Delete button is at the bottom of the User Groups tab).

- 6 Click **OK** on the User Group ACL Editor to save changes to User Group permissions.

Granting or Removing Event Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Events** tab.

The *event filters* that return the types of events for which this user group has permissions are listed.



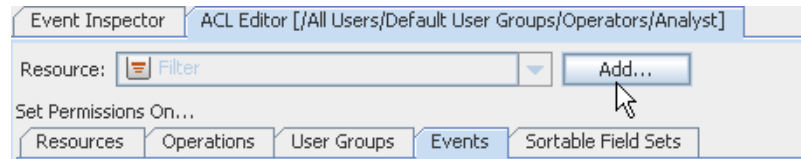
User groups are granted permissions to events by means of event *filters* applied to groups. The event filters limit the types of events group members can access through the ESM Console.

For example, members of the ESM Administrators group can view all events, as indicated by the event filter assigned to the Administrators group by default: `/All Filters/ArcSight System/Core/All Events`.

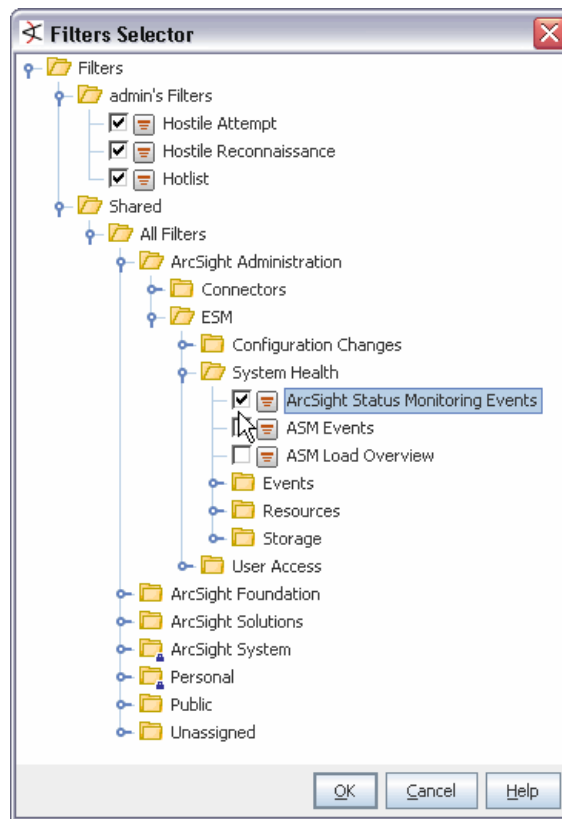
For more information about filters, see [Chapter 9, Filtering Events, on page 147](#). For more information about events, see ["Events" on page 722](#).

5 Add or remove user group permissions to view events as follows.

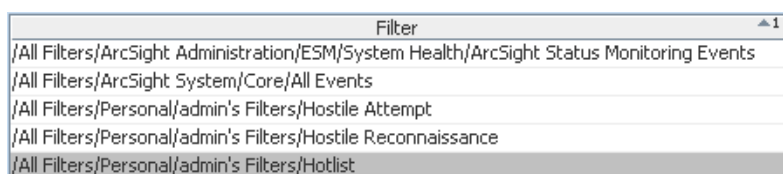
- ◆ **To add permissions to view events** captured by a filter not shown in the current list, click **Add**.



Select the event filters you want to add permissions for and click **OK**.



The list of event filters is updated to include the ones you added. Filters listed capture and allow all event types this user group has permissions to view.



- ◆ **To remove event filters** (permissions to view certain types of events), select a filter in the Events “Filter” list and click **Delete**. (The Delete button is at the bottom of the Events tab).

- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

Granting or Removing Sortable Field Sets Permissions

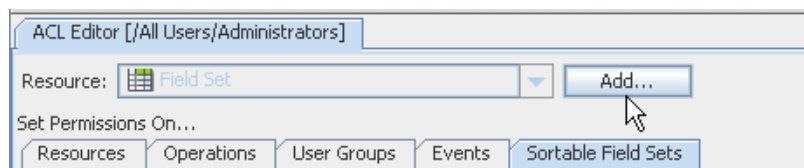
- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Sortable Field Sets** tab.

The event field sets for which this user group has access permissions are listed.

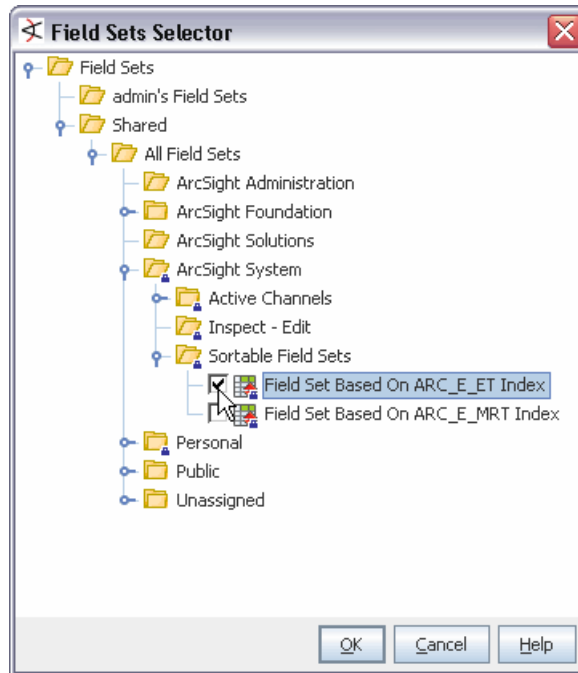


- 5 Add or remove user group permissions on sortable field sets as follows.

- ◆ **To add permissions to use a field set** not shown in the current list, click **Add**.



Select the sortable field sets you want to add permissions for and click **OK**.



The list of sortable field sets is updated to include the ones you added. Field sets listed represent those this user group has permissions to use.

- ◆ **To remove sortable field sets**, select a field set in the list and click **Delete**. (The Delete button is at the bottom of the Sortable Field Sets tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Sortable Field Sets permissions.

Sharing Resources

You can share your resources with other users by moving, copying, or linking your resource to or into another resource's Public group; for example, to share a filter you would move it into the Public Filters group in the Filters resource tree.

To share a resource

- 1 In a resource tree, drag a resource and drop it into the Public group (this can be a single resource or a resource group).
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the resource that will not be affected when the original resource is edited. If you choose **Link**, you create a copy of the resource that is linked to the original resource. Therefore, if you edit a linked resource, whether the original or the copy, all links are edited as well. When deleting linked resources, you can either delete the selected resource or all linked resources.

You can also multiple-select resources with the **Shift** key, and drag-and-drop or keyboard copy-and-paste, to move, copy, or link them in another group.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Controlling Who Has Permissions to Deploy Data Monitors

Starting with ESM 4.5, data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions.

Depending on the permissions associated with the user group to which they belong, users may or may not have options available on their consoles to **Enable** (*deploy*) or disable (*un-deploy*) data monitors. (See also [“Enabling or Disabling a Data Monitor” on page 118.](#))

Administrators (all users belonging to the `admin` user group) have permissions to deploy/undeploy data monitors.

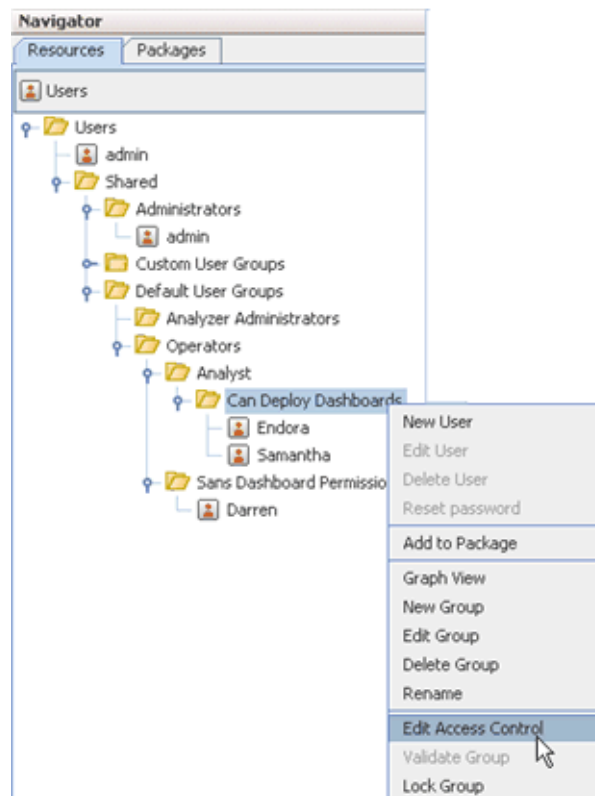
Administrators can grant permissions to deploy/undeploy data monitors to other non-Administrator through the Users resource Access Control Lists (ACLs) editor, as described in [“Granting or Removing Operations Permissions” on page 446.](#) As with user permissions for other resources, these are applied at a user group level. As an administrator, you can grant all users in a given group permission to deploy data monitors. Once user groups are set up and appropriate permissions applied to those groups, you can add new users to appropriate groups, and change access permissions for existing users by moving them in or out of various groups. If you want to allow or disallow a particular user the option to deploy data monitors, move the user in or out of a group that has that permission.

To configure data monitor deployment permissions:

- 1 If needed, set up one or more user groups for non-admin users to whom you want to control permissions to deploy data monitors. (For example, at the simplest level you might have a group for analysts and operators who are allowed to deploy data monitors and another for those you want to block from this option.)

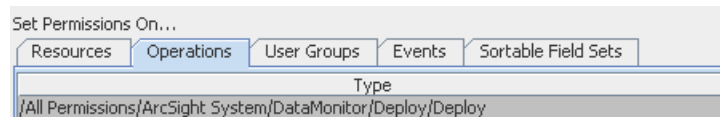
See [“Handling Users” on page 438](#) and [“Handling User Groups” on page 441](#) for information on adding, deleting, and editing users and user groups.

- 2 Follow the instructions provided in [“Granting or Removing Operations Permissions” on page 446](#) to grant or remove permission to deploy data monitors to a particular group. As a part of these instructions, you'll select the **Users** resource in the navigator, right-click a group and choose **Edit Access Control**.



- 3 In the ACL Editor, click the Operations tab, and click **Add**.
- 4 On the Permissions Selector, select **Deploy** under **Permissions\Shared\All Permissions\ArcSight System\Data Monitor** and click **OK** to save the settings and close the dialog.

The list of Operations is updated to include deployment permissions on data monitors.



(To remove the permission for this group, select the permission and click **Delete**.)

- 5 Click **OK** on the ACL Editor to save your changes.

For information on deploying or undeploying data monitors, see [“Enabling or Disabling a Data Monitor” on page 118](#).

For more information on administrator tasks of working with user permissions and ACLs, see [“Managing Permissions and Resources” on page 443](#).

How Upgrades Affect Data Monitor Deploy Permissions

Upon installation and deployment of a different version of ESM software (e.g., version or service pack upgrades), only administrators ([admin](#) users) will keep permissions to

deploy/undeploy data monitors. Non-[admin](#) users will not have deploy permissions on data monitors even if they had such permissions as part of the previous ESM configuration.

After upgrades, all users will have access to already-deployed data monitors. But, initially, non-[admin](#) users will not have permissions to enable/disable data monitors, nor have access to new data monitors unless an administrator enables (deploys) these.

To re-establish data monitor deployment permissions for non-[admin](#) users after an upgrade, administrators can reconfigure fine-grained permissions. They can re-group users and perhaps link non-[admin](#) users into existing or new groups with more permissions (like data monitor deployment), as described in [“Controlling Who Has Permissions to Deploy Data Monitors” on page 452](#).

Deployment Permissions on Imported Data Monitors

If a user without data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import will succeed but the data monitor will be disabled (*undeployed*). After the import, the user will not have permissions to deploy the data monitor unless an administrator reconfigures permissions for that user.

If a user with data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import will succeed and the data monitor will keep its enabled (*deployed*) setting. After the import, this user will be able to view the data monitor and re-set its deployment state as needed.

Locking and Unlocking Resources

The locking and unlocking capability applies to the following ArcSight content:

- System core content
- User created content

System Core Content

When you install the ArcSight ESM system, a set of predefined content called the System Core content is installed by default. This content provides the foundation building blocks for the ArcSight ESM to work.

System Core content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in [/All Filters/ArcSight System/Core](#).

The modification of System Core content can adversely impact the operation of ESM, therefore, it is locked by default. ArcSight strongly recommends against unlocking or modifying this content. If there is a need to unlock this content, contact ArcSight Customer Support.



Use the resources available in ArcSight Foundation packages or ArcSight Administration to create content to suit your needs.

User Created Content

ArcSight users can lock any resource or a group of resources to which they have write access privileges. Locking prevents a resource from being modified or deleted. Once locked, such resources or groups can be unlocked only by these users:

- The user who applied the lock—the lock owner.
- Any user who has write permissions to the lock owner. That is, a user who has privileges over the user who applied the lock. For example, the administrator user has write permissions over all users by default. Therefore, if user joe locks a resource, the user administrator can unlock it.
- The system user.



You can make a copy of a locked resource even if you do not have the privileges to unlock it.

You can edit resources in a locked group if you have write access privileges to the resource, however you cannot do the following:

- Delete or remove resources from it.
- Add a new resource to it.

Unlocking a User-locked Resource

To unlock a resource, right click the locked resource and select **Unlock** from the drop-down menu. For detailed instructions, see the Console online Help.

Modeling Your Network and Managing Assets

ArcSight ESM operates on a data model that enables you to build a business-oriented view of data derived from physical information systems. These distinctions help ESM clearly identify the events in your network, and provide more layers of detail to ESM correlation capabilities. Modeling your network and the assets it includes is part of ESM setup and ongoing maintenance.

The following topics provide a conceptual overview of network asset modeling, and describe how to configure, update, and maintain a network model in ESM.



- For a description of techniques for dealing with hundreds of thousands of assets, see [“Asset Scalability” on page 475](#) in this guide.
- For a more detailed conceptual overview, information about configuring each type of ESM asset and modeling your network, refer to the *ArcSight ESM 101* chapter on the “ESM Network Model.”

Network Model

The network model is a representation of the nodes (*assets*) on your network and certain characteristics of the network itself.

Before you can make an informed decision about what to do about a particular event, it helps to know something about the event's source and destination. Is the source a previous attacker, does it come from a hostile region of the world, or is it a trusted server that has suddenly become the source of a hostile attack? Does the destination expose relevant vulnerabilities, does it host critical applications, or is it a known server of forbidden services?

ESM captures this kind of information by modeling the assets on your network and particular attributes of the network itself that are pertinent to ESM. The network model represents information for individual assets and whole zones.

For critical assets on the protected network, network modeling captures important facts that will help inform your decisions, such as:

- All open ports
- The operating system running on that host
- Known vulnerabilities that might be exposed
- Applications present
- The missions these applications support and their criticality to your operation

For less critical assets, such as a particular block of addresses on the Internet, it may be sufficient to just know general information about them, such as the country in which those assets reside.

Populating the Network Model with Assets

There are several ways you can populate the network model with assets. Most enterprises use a combination of these methods:

- **Manually, using ESM network modeling tools (assets resources):** Set every parameter for every asset manually using ESM's network modeling tools.

- **Use the ESM Network Model wizard:** Starting with ESM v.4.5, a Network Model wizard is provided on the ESM Console (menu option **Tools > Network Model**). For more information, see [“Populating the Network Model Using the Wizard” on page 459](#).
- **Automatically, from a vulnerability scanner:** Use the output of a vulnerability scan, such as FoundStone, ISS Internet Scanner, or Nessus, as reported to the ESM Manager from a scanner SmartConnector. You can configure an SmartConnector to import the data from the vulnerability assessment tool. ESM converts the data into the ESM format.

You can use a vulnerability scanner to populate the baseline network model, or you can import network model data as a `.csv` file. Scanners cannot populate zones or asset ranges, however, so once scanner data is imported, you can use the ESM network modeling tools to manually fill in the model with these distinctions.

For details about how to import an existing network model as a `.csv` file, see [“Uploading Files and Creating a File Resource” on page 488](#).

- **Import network model from an existing configuration database:** Many enterprise networks have third-party systems that already model the properties of the assets on your network. You can export these network models, translate the format into the ESM schema using a utility supplied by ArcSight, and import it to the ESM Manager as a resource archive with the help of ArcSight Professional Services.

ESM uses the following objects to model the network. These are represented as *resources* on the ESM Console, as described in [“Understanding ESM Asset Resources” on page 457](#).

- **Assets** represent individual nodes on the network, such as servers, routers, and laptops.
- **Asset ranges** represent a set of network nodes addressable as a contiguous block of IP addresses.
- **Zones** represent portions of the network itself and are also characterized by a contiguous block of addresses.
- **Networks** provide an additional distinction to differentiate between two private address spaces with overlapping IP address ranges.
- **Customers** describe the internal or external cost centers or separate business units associated with networks, if applicable to your business environment. Customer tagging is a feature developed mainly to support Managed Service Security Provider (MSSP) environments, although it can also be used by private organizations to denote cost centers, internal groups, or subdivisions. The Customer designation keeps event traffic from multiple cost centers and/or business units clearly identified and separate. A customer can be thought of as the “owner” of an event, rather than the source or target of an event.

Understanding ESM Asset Resources

The **Assets** resource in the Navigator panel contains subtabs for the following network modeling resources:

Assets

An asset is any network endpoint with an IP address, MAC address, host name, or external ID. For network modeling purposes, an asset is any endpoint you consider significant enough to characterize with details that will make ESM correlation and reporting more meaningful.

ESM automatically creates assets to model the network nodes that host ArcSight components (Managers, Databases, Consoles, and SmartConnectors). It also automatically creates assets for events received from device endpoints on your network that do not

already have assets modeled in ArcSight. This auto-asset creation feature could require configuration, depending on the assets reporting in to ESM. For more about this feature and how to configure it see:

- **For ESM:** [“Configure Asset Auto-Creation Filters” on page 18 in Chapter 3, Standard Content, on page 9.](#)

Assets can be populated using any of the following methods:

- Manually using the Console
- Using the Network Model wizard
- Dynamically from scanner data

Locations

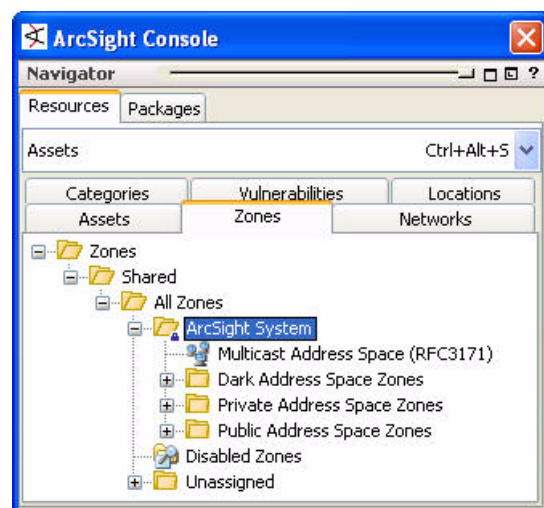
The locations designated to help sort out and identify the physical deployment of various assets are usually set during ArcSight deployment. Ordinarily, you do not need to change these assignments unless you need to reflect a reorganization or a renaming project. While you create locations through the Location Editor, you assign them to assets through the Asset Editor. Each asset can be assigned to only one location. You can also assign locations to zones and networks. Private address-space zones, in particular, should be associated with locations.

Zones

Zones are ArcSight resources that represent a functional part of the network with contiguous IP addresses, such as DMZ, VPN, wireless LAN, or DHCP.

With ArcSight v4.0, every asset or address range is associated with a zone. ArcSight comes configured with the standard global IP address ranges already represented as zones, so if your network uses only these public IP addresses, ArcSight can resolve them without setting up any additional zones.

ESM comes with the following standard zones:



You would need to create your own zones if you have overlapping private networks. Private networks usually model a functional group within your network or a subnet, such as a wireless LAN, the engineering network, the VPN or the DMZ.

For details about using the zone editor, see [“Zone Editor” on page 471 in “Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 470.](#)

Networks

Networks are ArcSight resources that are used to differentiate between zones whose IP ranges overlap, such as when branch locations assign the same private address spaces to resources in their locations.

ESM comes configured with two standard networks: Local and Global.

The standard “Global” network automatically recognizes the available zones and provides the correct addressing information to ArcSight SmartConnectors when they are installed. Custom Networks are also used to compartmentalize customer entities in MSSP situations. When you associate a customer or a location with a network in the Network Editor, zones automatically access this information. (See [“Network Editor” on page 472](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 470.](#))

Vulnerabilities

The asset vulnerabilities on your network are normally discovered and updated automatically by scanners. The most common manual change to a vulnerability resource is to associate it with a Knowledge Base article. You can associate assets with vulnerabilities from either the Vulnerabilities or Assets editors. (See [“Vulnerability Editor” on page 472](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 470.](#))

Asset Categories

Asset categories are ArcSight resources that describe the properties of an asset in terms of how it is used. Asset categories are one of the key ways that ESM adds differentiation, relevance, and context to the millions of events passing through your network.

Asset categories establish identity, ownership, and criticality of the assets on your network. Asset categories present an extensible schema that adds value to the business properties of your assets. The root of a particular category (for example, **Criticality** in the group [/All Asset Categories/System Asset Categories/Criticality](#)) defines the property itself, whereas the members of the category (for example, the criticality levels [Very High](#), [High](#), and so on) define the possible values for that property.

You can create new categories through the Group Editor, and associate categories with assets through the Asset Editor. One asset can fall into multiple categories. You can also apply categories to zones. (See [“Categories” on page 472](#) in [“Working with Locations, Zones, Networks, Vulnerabilities, and Categories” on page 470.](#))



Always exercise caution when deleting or changing existing asset categories. For safety, create new categories in new folders.

For more information about asset categorization and categories in ESM, see [“Categories” on page 606.](#)

Populating the Network Model Using the Wizard

Starting with ESM v.4.5, a Network Model wizard is provided on the ESM Console (menu option **Tools > Network Model**). The Network Model wizard provides the ability to quickly populate the ESM network model by batch loading asset and zone information from Comma Separated Files (CSV) files. The following data can be imported into an ArcSight ESM Manager from CSV files:

- **Zones** define functional parts of a network, such as a wireless LAN, an engineering network, a VPN or a DMZ. For the column types of the zones CSV file, see [“Zones CSV File Format” on page 462](#).
- **Assets** represent individual nodes on the network, such as servers and routers. For the column types of the assets CSV file, see [“Assets CSV File Format” on page 464](#).
- **Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. Asset ranges should be a subset of the IP address ranges defined for zones. For the column types of the asset ranges CSV file, see [“Asset Ranges CSV File Format” on page 466](#).

You can import combinations of input CSV files at one time using the Network Model wizard but only one file of each type can be imported during a single import. For example, if you only have assets to import, you can import only an assets CSV file. If you have a zones CSV file, an assets CSV file, and an asset ranges CSV file to import, you can import all three at once using the Network Model wizard.

Specifying CSV Column Types

Each CSV file type defines a set of required column(s) and optional columns. In addition, the CSV file can contain columns that are not used by the Network Model wizard. The columns can be in any order but the Network Model wizard requires that you specify the types of each column so the wizard knows how to interpret each column. You can specify the column type using one of the following methods:

- Specify the column type in the header of the CSV file itself, prior to launching the Network Model wizard. For instructions, see [“Specify the Column Type Using a Header” on page 460](#).
- While running the Network Model wizard, assign the appropriate column type for each column in the Select Column Headers panel. For instructions, see [“Assign the Column Type in the Wizard” on page 461](#).

Columns not used by the Network Model wizard must be assigned the column type [Ignore](#). Only columns of type [Ignore](#) and [Category URI](#) can be repeated in the CSV file. For all other column types, only one instance of the column type can be assigned in the file. For example in a zones CSV file, only one column should be assigned the [Name](#) column type. If duplicate columns of a non-repeatable column type exist in the CSV file, one of the columns should be assigned the [Ignore](#) column type. For example if two name columns appear in the CSV file, one should be assigned the [Name](#) column type and the other should be assigned the [Ignore](#) column type.

Specify the Column Type Using a Header

In this method, you specify the column type in the first row (header) of the CSV file itself before importing the CSV file using the wizard. The column name in the header must match the column type specified in the [Table 20-1, “Zones CSV File Format,” on page 463](#), [Table 20-2, “Assets CSV File Format,” on page 464](#), or [Table 20-3, “Asset Ranges CSV File Format,” on page 466](#).

As shown in following sample zones CSV file, the column names in the first row (highlighted in **bold**) match the column types specified in [Table 20-1, “Zones CSV File Format,” on page 463](#). The wizard determines how to interpret each column using the column type specified in the header.

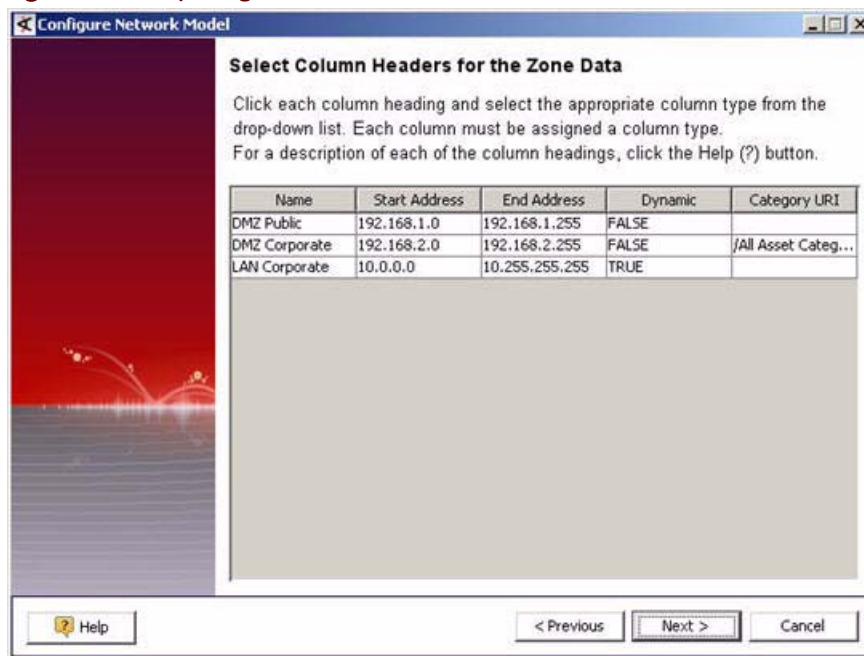
```
Name,Start Address,End Address,Dynamic,Category URI
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
```



```
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```

When this zones CSV file is imported into the wizard, the wizard correctly matches the column types because the column types have been correctly specified in the header, as shown in [Figure 20-1](#).

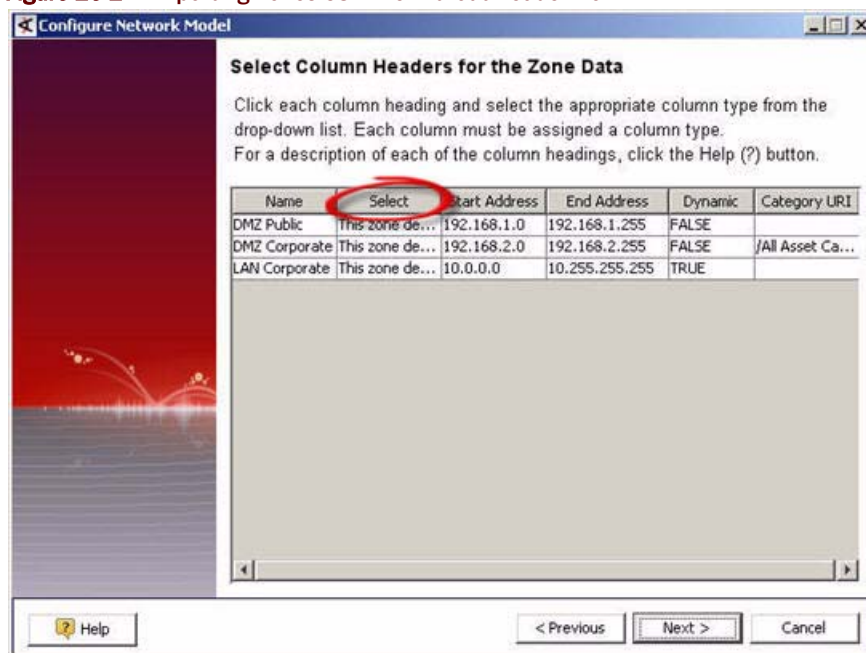
Figure 20-1 Importing Zones CSV File with Header Row



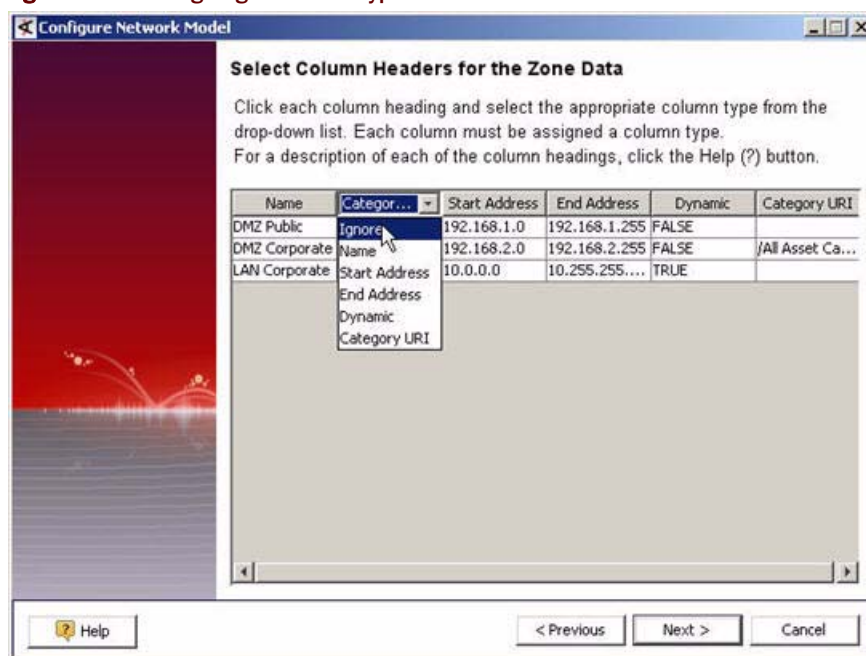
Assign the Column Type in the Wizard

In this method, you assign the column type in the Select Column Headers panels while running the wizard. When the following sample zones CSV file (which does not contain a header row) is imported, the wizard does not know how to interpret all the columns as shown in [Figure 20-2](#).

```
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```

Figure 20-2 Importing Zones CSV File without Header Row

By default, when this sample data is imported into the wizard, the second column is automatically assigned to the **Select** column type but the second column is a description of the zone and should be assigned the **Ignore** column type. To change the column type, click the title of the column and from the drop-down menu select the appropriate column type as shown in Figure 20-3.

Figure 20-3 Assigning a Column Type

Zones CSV File Format

Zones define functional parts of a network, such as a wireless LAN, private networks, or subnets. For example, the following network areas could be identified as a zone: the VPN,

the DMZ, or an engineering network. Zones are identified with a contiguous block of addresses.



Each zone should specify a unique range of IP addresses. The IP addresses specified by zones should not overlap. If you import a zone that overlaps with a zone already specified on the ArcSight ESM Manager and the new zone has a different name than the existing zone, the following occurs:

- the new zone is created
- the existing zone is invalid and displays with the broken zone icon in the ArcSight ESM Console

You can define a set of zones in ArcSight ESM by batch loading zone definitions from an zones CSV file. Zone CSV files contain the columns listed in [Table 20-1 on page 463](#). When a zones CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Zone Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 467](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 460](#).

When the Next button is clicked in the Summary of Data to Import panel, the zone data is imported into the ArcSight ESM Manager. The new zones are created in the [/All Zones/Site Zones](#) group. For example, if a zone called [DMZPublic](#) was specified in the imported zones CSV file, a new zone is created at the following URI: [/All Zones/Site Zones/DMZ Public](#). The new zones are assigned to the default network called [Local](#).

Table 20-1 Zones CSV File Format

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the zone such as the purpose or geographical location.	Yes	No	DMZ Public
Start Address	The start of the range of IP addresses that defines the zone.	Yes	No	192.168.1.0
End Address	The end of the range of IP addresses that defines the zone.	Yes	No	192.168.1.255
Dynamic	Determines whether the devices defined in the zone use dynamic addressing: <ul style="list-style-type: none"> • true—devices in the zone use dynamic addressing (DHCP) • false—devices in the zone use static IP addressing 	No Default is false	No	false

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Category URI	The asset category to assign to zone. NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes This column can be repeated because a zone can be categorized into more than one asset category.	/All Asset Categories/All Site Asset Categories/Business Impact Analysis/Business Role/Service/Web/
Ignore	The column contains data that is not used by the Network Model wizard when creating zones. For example, this column could contain a description of the zone.	No	Yes	This zone defines the public subnetwork of the DMZ.

Assets CSV File Format

Assets represent individual nodes on the network, such as servers and routers. For more information, see [“Understanding ESM Asset Resources” on page 457](#).

You can define a set of assets in ArcSight ESM by batch loading asset definitions from an Assets CSV file. Asset CSV files contain the columns listed in [Table 20-2 on page 464](#).

When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 467](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 460](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset data is imported into the ArcSight ESM Manager. The new assets are created in the [/All Assets/Site Assets](#) group. For example, if an asset called `DMZCorpEmailServer` was specified in the imported assets CSV file, a new asset is created at the following URI: [/All Assets/Site Assets/DMZCorpEmailServer](#). When imported, the new assets are auto-zoned. For more information, see [“Auto-zoning of Imported Assets” on page 468](#).

Table 20-2 Assets CSV File Format

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the asset. This name must be unique. It is recommended to specify a name. However, if a name is not specified, a unique name is generated using the other fields.	No	No	DMZ Corp Email Server 1

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Host Name	The host name of the network device represented by the asset.	No	No	dmz_corp_eml1
IP Address	<p>The IP address of the network device represented by the asset.</p> <p>NOTE: If no value is specified for this column (,) the asset is created with an IP address of 0.0.0.0.</p>	Yes	No	192.168.2.1
MAC Address	The MAC address of the network device represented by the asset. The MAC address is made up of six groups of two hexadecimal digits can be separated by colons (:) or hyphens (-).	No	No	21-4D-5B-2A-3B-FF
Static Addressing	<p>Defines if the network device is statically addressed even though the IP address of the asset is in a dynamic zone:</p> <ul style="list-style-type: none"> true—asset uses static IP addressing false—device uses dynamic addressing (DHCP) <p>For more information, see “Static Addressing in a Dynamic Zone” on page 465.</p>	No Default is false	No	false
Category URI	<p>The asset category to assign to network device.</p> <p>NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.</p>	No	Yes This column can be repeated because a network device can be categorized into more than one asset category.	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Network Domains/Email/
Ignore	The column contains data that is not used by the Network Model wizard when creating assets. For example, this column could contain a description of the asset.	No	Yes	This asset defines the Corporate Email Server in the DMZ.

Static Addressing in a Dynamic Zone

Set the **Static Addressing** column to [true](#) if the network device is statically addressed even though the IP address of the asset is in a dynamic zone. For example, set this column to [true](#), for the following conditions:

- A dynamic zone is defined with the following IP range: [192.168.2.1 - 192.168.2.255](#).
- A network device with an IP address of [192.168.2.15](#) is statically addressed even though it is defined in the dynamic zone.

Asset Ranges CSV File Format

Asset ranges represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have a number of network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. An asset range can define a group of assets that are not addressed individually. Asset ranges should be a subset of the IP address ranges defined for zones.



Each asset range should specify a unique range of IP addresses. The IP addresses specified by asset ranges should not overlap. If you import an asset range that overlaps with an asset range already specified on the ArcSight ESM Manager and the new asset range has a different name than the existing asset range, the following occurs:

- the new asset range is created
- the existing asset range is invalid and displays with the broken asset range icon in the ArcSight ESM Console

You can define a set of asset ranges in ArcSight ESM by batch loading asset range definitions from an asset range CSV file. Asset range CSV files contain the columns listed in [Table 20-3 on page 466](#). When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Ranges Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 467](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 460](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset range data is imported into the ArcSight ESM Manager. The new asset ranges are created in the [/All Assets/Site Assets](#) group. For example, if an asset range called [DMZCorpHR](#) was specified in the imported asset range CSV file, a new asset range is created at the following URI: [/All Assets/Site Assets/DMZCorpHR](#).

Table 20-3 Asset Ranges CSV File Format

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the asset range. This name must be unique.	Yes	No	DMZ Corp HR
Start Address	The start of the range of IP addresses that defines the asset range.	Yes	No	192.168.2.11
End Address	The end of the range of IP addresses that defines the asset range.	Yes	No	192.168.2.20

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Category URI	The asset category to assign to asset range. NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes This column can be repeated because an asset range can be categorized into more than one asset category.	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/HR Data/
Ignore	The column contains data that is not used by the Network Model wizard when creating asset ranges. For example, this column could contain a description of the asset range.	No	Yes	This asset range defines the all the corporate human resources assets.

Increasing the Number of Rows Displayed

By default, only the first fifteen rows of data are displayed in Select Column Headers for the <Resource Type> Data panels. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported.

To increase the number of rows displayed, add the property `usecase.networkmodeling.maxrowfortable` to the `<ARCSIGHT_HOME>/config/console.properties` file and set the value of the property to a number greater than fifteen. Restart the ArcSight ESM Console.

Summary of Data to Import

In the Summary of Data to Import panel, a summary of the network modeling data ready to import into the ArcSight ESM Manager is displayed. If you click **Cancel** in this panel or any of the preceding panels, no data is imported into the ArcSight ESM Manager.

- 1 Click **Next** to start the import process.

A temporary Archive Resource Bundle (ARB) file with the import data is created and the Install Packages dialog displays.

- 2 To install the data from the temporary ARB file, in the Update Packages dialog, click **OK**.

The network modeling data is imported into the ArcSight ESM Manager and the Data Imported pane displays. In addition, the Installing Packages and the Importing Packages dialogs display.

- 3 Close the open dialogs:

- a In the Installing Packages dialog, click **OK**.
- b In the Importing Packages dialog, click **OK**.

Network Data Imported into Manager

When network modeling data is imported from the network modeling data CSV files, new resources are created in the following groups on the ArcSight ESM Manager:

- New **zones** are created in the `/All Zones/Site Zones` group. For example, if a zone called `DMZPublic` was specified in the imported zones CSV file, a new zone is created at the following URI: `/All Zones/Site Zones/DMZ Public`.
The new zones are assigned to the default network called `Local`.
- New **assets** are created in the `/All Assets/Site Assets` group. For example, if an asset called `DMZCorpEmailServer` was specified in the imported assets CSV file, a new asset is created at the following URI: `/All Assets/Site Assets/DMZCorpEmailServer`. When imported, the new assets are auto-zoned. For more information, see [“Auto-zoning of Imported Assets” on page 468](#).
- New **asset ranges** are created in the `/All Assets/Site Assets` group. For example, if an asset range called `DMZCorpHR` was specified in the imported asset range CSV file, a new asset range is created at the following URI: `/All Assets/Site Assets/DMZCorpHR`.

In the Data Imported dialog, click **Finish** to close the wizard.

Auto-zoning of Imported Assets

When new assets are imported into the ArcSight ESM Manager using the Network Model wizard, an attempt is made to assign the assets to the appropriate zone from the default network called `Local`. This process is called auto-zoning.

When the asset is imported, if a zone is found with an address range that includes the imported asset and that zone is located in the `Local` network, the matching zone is assigned to the asset. For the asset to find the matching zone, the matching zone must either:

- Already exists on the ArcSight ESM Manager prior to the import.
- Be imported with the asset as part of the same import process—part of the same transaction. Zones are created before assets in the import process.

If no matching zone is found in the network, no zone is assigned.

The following example illustrates the auto-zone process. A zone called `DMZCorporate` is defined in the `Local` network on the ArcSight ESM Manager with a starting address of `192.168.2.0` and an ending address of `192.168.2.225`. If an asset called `DMZCorpDatabase` with an IP address of `192.168.2.11` is imported by the wizard, the `DMZCorporate` zone is assigned to `DMZCorpDatabase` asset because the IP address of the `DMZCorpDatabase` asset is in the range of addresses specified in the `DMZCorporate` zone and the `DMZCorporate` zone is located in the `Local` network.



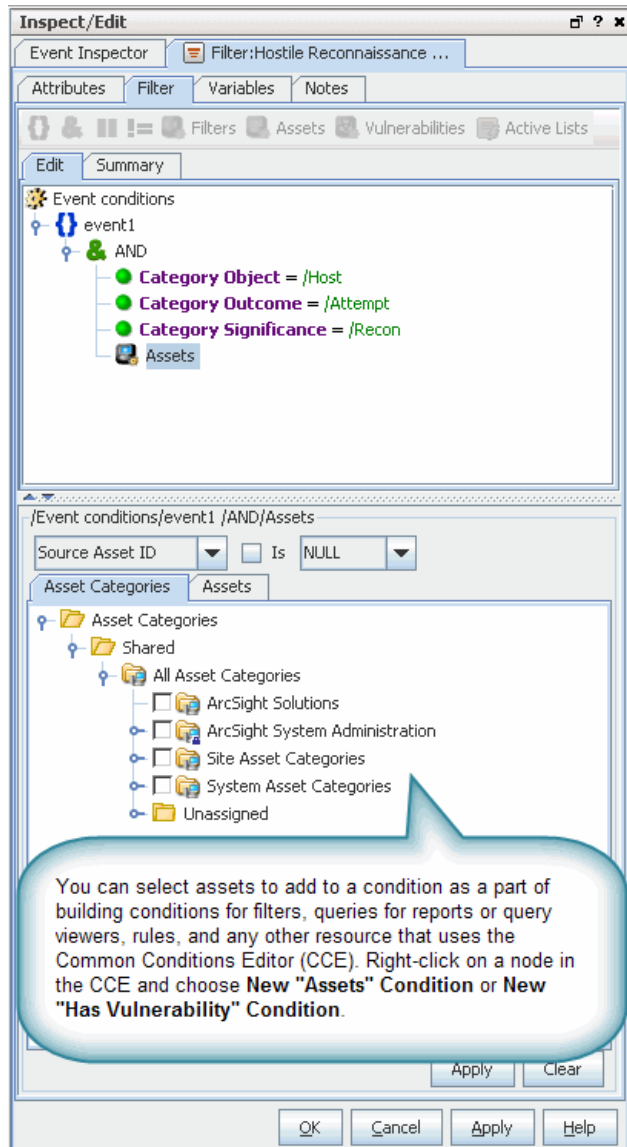
Only one asset with a given host name is allowed in a given zone on a network. When two assets with the same host name are imported, and if the ArcSight ESM Manager assigns them to the same zone in the same network, both assets are imported but one of the assets is disabled and displays with the broken-asset icon in the ArcSight ESM Console.

Selecting Assets in the Common Conditions Editor

Once assets are added to your network model, you can select them in order to write conditions that help you analyze their role in the event traffic they process.

The Asset Selector appears in the Query Editor (in Reports), Rules Editor, Filters Editor, and in the Filter Settings panel, when creating an asset condition. In the Asset Selector, select the assets to add as a new condition.

Right-click on a node in the Common Conditions Editor (CCE) and choose **New "Assets" Condition**. (For more about using the CCE, see ["Common Conditions Editor" on page 616.](#))



Managing Assets

This topic explains how to create, edit, move, add to, and delete assets. Before making assets changes, however, please first see the overview in ["Understanding ESM Asset Resources" on page 457.](#)

Creating an Asset

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 Right-click a group and choose **New Asset**.
- 3 Select the **Attributes** tab and enter values in the fields described below.
- 4 Click **OK**.

Table 20-4 Asset Attribute Fields

Asset Attributes	Description
Name	The asset's friendly name. This field can default to the asset's host name or IP address.
IP Address	The asset's IP address, in dotted-decimal notation.
MAC Address	The unique hardware ID for the network device.
Host Name	The asset's DNS name.
Location	As described in Assets and Changing Assets.
Zone	As described in Assets and Changing Assets.

After you fill in the attribute fields, use the other tabs in the Asset Editor as necessary to add resources.

Table 20-5 Additional Asset Editor Tabs

Asset View	Contents
Categories	Use the Add button on this tab to select network categories with which to associate the asset.
Alternate Interfaces	Use the Add button on this tab to select a second asset ID if this asset has an additional ID on another network. Alternate interfaces usually apply only to network boundary devices, such as bridges, that have two MACs.
Vulnerabilities	Use the Add button on this tab to select certain vulnerabilities with which to associate the asset.
Notes	Use the text box and Save button on this tab to write and file additional information concerning the asset.

Working with Locations, Zones, Networks, Vulnerabilities, and Categories

As a part of identifying assets and configuring ESM to recognize them, you need to provide detail about networks, zones, and locations where assets reside. Additionally, you can list vulnerabilities separately, and group assets into categories based on which you can set up user access controls and monitoring channels.

You can create and edit descriptions of networks, zones, locations, and particular assets considered to be *vulnerabilities*. Editors for these are provided as right-click options on the resources in the Assets subtabs for Networks, Zones, Locations, Vulnerabilities. Each has

slightly different attributes and configuration information on sub-tabs, depending on the type of asset resource.

Location Editor

Asset Attributes	Description
Name	A descriptive name for the geographical location (required)
Latitude	Latitude for the location. The format for this measurement is a preference setting for the Console (menu option Edit > Preferences , click Latitude and Longitude). For more information, see "Latitude and Longitude Options" on page 561 in "Changing User Preferences" on page 556 .
Longitude	Longitude for the location The format for this measurement is a preference setting for the Console (menu option Edit > Preferences , click Latitude and Longitude). For more information, see "Latitude and Longitude Options" on page 561 in "Changing User Preferences" on page 556 .
Address	Provide details for City , Region Code , Postal Code , and Country

Zone Editor

Asset Attributes	Description
Name	A descriptive name for the geographical location (required)
Start Address	Provide an IP address that identifies the start of the network scope.
End Address	Provide an IP address that identifies the end of the network scope.
Dynamic Addressing	Click this option on or off to indicate whether this network uses dynamic addressing <ul style="list-style-type: none"> • Checkmark (toggle on) this option to indicate that the network you are describing uses dynamic addressing (Dynamic Host Configuration Protocol or DHCP server) • Leave this option unchecked (toggle off), if the network you are describing does not use dynamic addressing (but, rather, uses static IP addresses)
Location	Select a location for this zone.
Network	Select the network in which this zone resides.

In addition to zone **Attributes** (described above), the Zone Editor includes subtabs for adding **Assets** and **Categories** into the *zone* you are configuring.

Network Editor

Asset Attributes	Description
Name	A descriptive name for the network (required)
Customer	Customer name This option is typically used if configuring assets for a customer on behalf of a managed security service provider (MSSP) or similar scenario.
Location	This is an optional field for a descriptive name of the geographical location of the network.

In addition to network **Attributes** (described above), the Network Editor includes subtabs for adding **Connectors** and **Zones** into the selected *network* you are configuring.

Vulnerability Editor

Asset Attributes	Description
Name	A descriptive name for the vulnerable asset (required)
Knowledge Base Article	Optionally, provide a link to a relevant knowledge base article.
External ID	Provide an alternate identifier for the vulnerability.

In addition to vulnerability **Attributes** (described above), the Vulnerability Editor includes a subtab for selecting and adding assets as **vulnerabilities**.

Categories

The Asset Categories subtab in the Navigator provides options to organize assets into groups based on *categories*. From the Navigator right-click menu on Asset Categories, you have several views and tools to help manage and monitor assets. For example, from this menu, you can:

- Create channels to show asset categories and assets
- Move assets into and out of category groups
- Create new category groups
- Configure access control lists (ACLs) to limit or allow user access to groups of assets (see [“Managing Permissions and Resources” on page 443](#))

One asset can be categorized in more than one asset category. You can also assign asset categories to groups of resources. This transfers the asset category onto all the members of the group and its sub-groups. To assign an asset category:

- 1 In the Navigator drop-down menu, go to **Assets**. Select the **Assets** tab. Go to [ArcSight System Administration/Agents](#), where you will find the SmartConnectors installed for your environment.
- 2 Right-click the asset or asset group you wish to categorize and select **Edit Asset** (or **Edit Group**).

- 3 In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen.
- 4 In the Asset Categories Selector pop-up window, select the asset categories that apply to this asset and click **OK**. For example:
 - a The usage category that applies to the asset (for example, /All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation)
 - b The criticality level that applies to the asset (for example, /All Asset Categories/System Asset Categories/Criticality/Very High)
- 5 Repeat steps 3 and 4 for every asset or group of assets you wish to classify in one of the ESM asset categories.

For more information about asset categorization and categories in ESM, see [“Categories” on page 606](#).

Editing an Asset

- 1 In the Assets resource tree, right-click an asset and choose **Edit Asset**.
- 2 On the **Attributes** tab, edit the text fields as described above.
- 3 On the other tabs, add or delete information as necessary.
- 4 Click **OK**.

Moving or Copying an Asset

- 1 In the Assets resource tree, navigate to an asset and drag and drop it into another group.
- 2 Choose **Move** to move the asset, **Copy** to make a separate copy of the asset, or **Link** to create a copy of the asset that is linked to the original asset.

If you choose **Copy**, you create a separate copy of the asset that will not be affected when the original asset is edited. If you choose **Link**, you create a copy of the asset that is linked to the original asset. Therefore, if you edit a linked asset, whether the original or the copy, all links are edited as well. When deleting linked assets, you can either delete the selected asset or all linked asset copies.

Deleting an Asset



Never delete System Asset resources of any type without consulting an ArcSight administrator. System Asset resources are usually necessary for correct operation.

- 1 In the Assets resource tree, right-click an asset and choose **Delete Asset**.
- 2 In the dialog box, click **Yes**.

Showing Assets in a Channel

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Show Assets**.

The asset(s) are displayed in an active channel grid view.

- 2 If applicable, you can also show assets recursively. To do so, right-click an asset group, and choose **Show Assets Recursively**. This will show assets not only in the selected group but also all children in an active channel.

Auto Zoning an Asset

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Auto Zone**.

The Network Selector dialog displays.

- 2 Browse for the network that contains the zone with an IP address range that includes the asset.
- 3 Select the network and click **OK**.

If a matching zone with an address range that includes the selected asset can be found in the network, the zone is assigned to the asset. For example, a zone called **DMZCorporate** is defined in the **Local** network on the ArcSight ESM Manager with a starting address of **192.168.2.0** and an ending address of **192.168.2.225**. If an asset called **DMZCorpDatabase** with an IP address of **192.168.2.11** is selected for auto zoning in the **Local** network, the **DMZCorporate** zone is assigned to **DMZCorpDatabase** asset because the IP address of the **DMZCorpDatabase** asset is in the range of addresses specified in the **DMZCorporate** zone.

If no matching zone is found in the network, no zone is assigned.

An asset can be selected for auto zoning manually by right-clicking and choosing the **Auto Zone** option as described above. In addition, auto zoning can automatically occur when assets are imported using the Network Model wizard. For more information, see ["Auto-zoning of Imported Assets" on page 468](#).

Managing Asset Groups

Asset groups are created to store similar groups or assets in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's permissions. If a group is deleted, the assets within that group are also deleted. ArcSight provides these groups:

- **Shared**: this group lists assets to which the user has permission.
- **Unassigned**: this group lists assets not assigned to a group.

If you have Administrator access you will also see another group named "All Assets" that contains all asset groups and assets.

Creating an Asset Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 In the Assets resource tree, right-click a group and choose **New Group**. A "name" text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Edit Group**.

- 2 In the **Group Editor**, edit the Name and Description text fields.
- 3 Click **OK**.

Moving or Copying an Asset Group

- 1 In the Assets resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Asset Scalability

ArcSight stores information about hosts and network devices in resources called Assets. These resources can be automatically created by vulnerability scanner SmartConnectors. Asset Scalability refers to ArcSight's ability to manage hundreds of thousands of assets or more without adversely affecting security event throughput.

Viewing Assets in Active Channels

Starting with ArcSight ESM v4.0, the Console shows assets, vulnerabilities, asset categories, scanner reports, and cases in active channels (rather than static grid views, as in previous releases). Now you can leverage the power of channels for asset management, including use of filters, field sets, better sorting capabilities, and dynamic display of an unlimited number of items (continually updated).

To start working with assets in active channels, choose **Assets** in the Navigator, and see [“Modeling Your Network and Managing Assets” on page 456](#).

Note also that you can create an “asset channel”. For more information on active channels, see [“Monitoring Active Channels” on page 91](#).

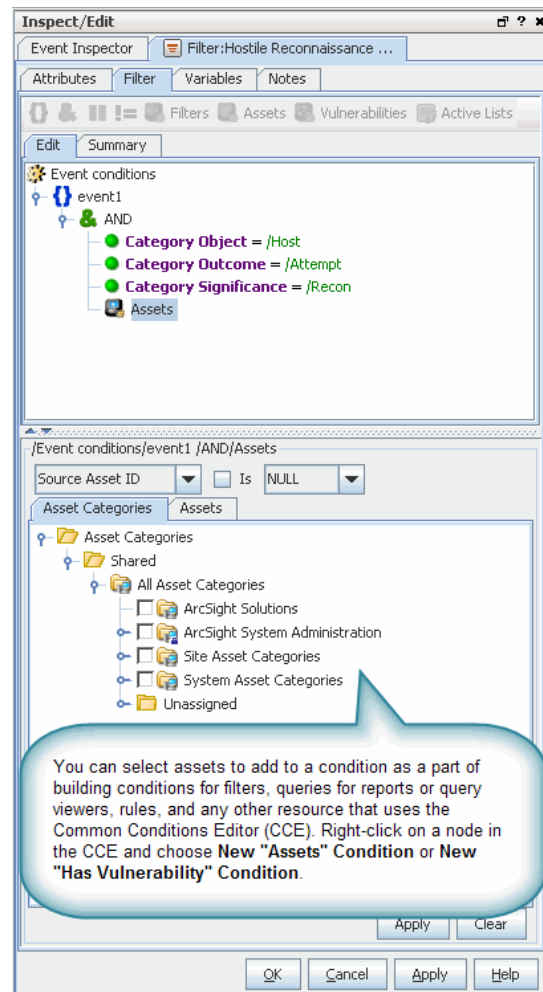
Finding Assets

Resource search helps you find one asset in a potentially large set, avoiding the resource tree in the Navigator.

Selecting Vulnerabilities

You can open the Vulnerability Selector from the Reports Query Editor, Rules Editor, Filters Editor, and in the Filter Settings panel. In the Vulnerability Selector, you select vulnerabilities to add to reports, rules, or filters as a new condition.

Right-click on a node in the Common Conditions Editor (CCE) and choose **New "Has Vulnerability" Condition**. (For more about using the CCE, see ["Common Conditions Editor"](#) on page 616.)



You use the Vulnerability Selector when performing these tasks:

- Adding a vulnerability condition to a report query (see ["Query Conditions"](#) on page 239)
- Specifying rule conditions (see ["Adding Vulnerability Conditions to Rules"](#) on page 306)
- Using filters (see ["Using Filters"](#) on page 480)

Managing Vulnerabilities

This topic describes how to perform the authoring and management tasks for vulnerabilities. See also ["Modeling Your Network and Managing Assets"](#) on page 456.

Note also that you can create a "vulnerability channels". For more information on active channels, see ["Monitoring Active Channels"](#) on page 91.

Creating a Vulnerability

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.

- 2 Right-click a group and choose **New Vulnerability**.
- 3 On the Vulnerabilities Attributes tab, type in the following text fields:

Vulnerability Attribute	Description
Name	The vulnerability's name. It can be generated by the ArcSight Manager in response to vulnerability scanners. If so, this field will be identical to the External ID field except that the pipe () will be replaced with a dash (-), such as CVE - CVE-1999-200.
Knowledge Base Article	A Knowledge Base article that further describes the vulnerability.
External ID	An ID of the format <standards body> <id>, such as CVE CVE-1999-200.
Owners	ArcSight users who are interested in the vulnerability.
Notification Groups	ArcSight users who are notified of events involving the vulnerability.

- 4 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 5 Click **OK**.

Editing a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 On the Attributes tab, type in the text fields as described above.
- 3 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 4 Click **OK**.

Moving or Copying a Vulnerability


- 1 In the Vulnerabilities tree, navigate to a vulnerability and drag and drop it into another group.
- 2 Choose **Move** to move the vulnerability, **Copy** to make a separate copy of the vulnerability, or **Link** to create a copy of the vulnerability that is linked to the original vulnerability.

If you choose **Copy**, you create a separate copy of the vulnerability that will not be affected when the original vulnerability is edited. If you choose **Link**, you create a copy of the vulnerability that is linked to the original vulnerability. Therefore, if you edit a linked vulnerability, whether it be the original or the copy, all links are edited as well. When deleting linked vulnerabilities, you can either delete the selected vulnerability or all linked vulnerability copies.


Retrieving Vulnerable Assets

- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 Select the **Vulnerable Assets** tab.


If you used a vulnerability scanner, all vulnerable asset discovered by the scanner are listed on this tab.

- 3 To refresh the vulnerabilities list, click the **Refresh** button ().

Adding an Asset to a Vulnerability

- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Click the **Add** button ().
- 4 Select an asset in the Assets Selector and click **OK**.
- 5 In the Vulnerability Editor, click **OK**.

Deleting an Asset From a Vulnerability

- 1 In the Vulnerabilities tree, right-click an asset and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Select an asset and click the **Delete** button ().
- 4 In the dialog box, click **Yes**.
- 5 In the Vulnerability Editor, click **OK**.

Deleting a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Delete Vulnerability**.
- 2 In the dialog box, click **Yes**.

Managing Vulnerability Groups

This topic describes the tasks involved in managing vulnerability groups.

Creating a Vulnerability Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then the **Vulnerabilities** tab.
- 2 In the Vulnerabilities resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

Renaming a Vulnerability Group

- 1 In the Vulnerabilities resource tree, under Assets, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing a Vulnerability Group

- 1 In the Asset resource tree's Vulnerabilities tab, right-click a group and choose **Edit Group**.

- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Vulnerability Group

- 1 In the Vulnerabilities tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Vulnerability Group

- 1 In the Vulnerabilities tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Reporting on Scanners

You can conveniently review the output of asset-vulnerability scanners in active channels and in the Vulnerabilities tab of the Asset Editor.

- 1 Choose the Assets resource tree in the Navigator panel.
- 2 In the Assets tab of the Assets tree, right-click an individual asset and choose **Scanner Reports**. If scanner asset-vulnerability reports are available for the selected asset, they appear in a Viewer panel grid view as an active channel.
- 3 You can use the standard controls described in Using Grids and Active Channels to review the reports collectively.
- 4 Also in the channel view, you can double-click vulnerability scanner events to open them in the Asset Editor, where the Vulnerabilities tab lists the vulnerability details.

For information on creating and editing assets, see [“Modeling Your Network and Managing Assets” on page 456](#).

You can create an active channel for selected scanner reports. For information on using active channels, see [“Monitoring Active Channels” on page 91](#).

Reporting Vulnerable Assets

You can create reports to show which assets are vulnerable to particular vulnerabilities or threats. ArcSight also provides Asset Reports that can be run from the Reports resource tree in the Navigator panel. For more information, see [“Using Report Templates” on page 209](#).

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.
- 2 In the Vulnerabilities tree, right-click a vulnerability and choose **Vulnerable Assets Report**.

- 3 In the Report Parameters dialog box, accept the vulnerability listed in the **Vulnerability URL** text field or click the **Vulnerability** button to run the report on another vulnerability.
- 4 Choose a Report File Format from the drop-down menu.
- 5 Click **OK**.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and will appear differently. In addition, Excel format is more memory intensive than PDF.

Managing Filters

The Filters resource tree in the Navigator panel is pre-populated with some typical event filters you can use directly, or as templates for more specific purposes.

Using Filters

The maintenance tasks for filters include editing, moving, copying, importing, exporting, and deleting. (Tasks described here are considered administrator tasks. For information on using filters, see also [Chapter 9, Filtering Events, on page 147](#), including information on [“Debugging Filters to Match Events” on page 151](#) and [“Investigating Views” on page 156](#).)

Editing a Filter



Understanding how to use the Common Conditions Editor (CCE) is integral to creating and editing filters. Please refer to [“Common Conditions Editor” on page 616](#), [“Conditional Statements” on page 625](#), and [“Conditions” on page 626](#) for more information.

- 1 In the Filters resource tree, right-click a filter and choose **Edit Filter**.
- 2 In the Filters Editor, edit the filter name.
- 3 In the conditions editor, edit logical operators and condition statements by doing the following:
 - ◆ To edit a logical operator, right-click the logical operator and choose **Edit**, then choose a logical operator and click **OK**. (For more information, see [“Logical Operators” on page 727](#).)
 - ◆ To edit a condition statement, right-click the condition statement and choose an operator, condition editor, or selection operation. For more information, see [“Creating Filters” on page 147](#) and [“Common Conditions Editor” on page 616](#) (CCE). (Search fields and undo/redo features are now available, as described in [“Editor Features” on page 616](#) in the CCE topic.)
 - ◆ To delete a logical operator, right-click the operator and choose **Delete**. In the confirmation dialog box, click **Yes**. The logical operator and all its condition statements are removed.
 - ◆ To delete a condition statement, right-click it and choose **Delete**. In the confirmation dialog box, click **Yes**.
 - ◆ To edit or delete a filter, right-click the filter and choose **Edit** or **Delete**.
- 4 Click **OK**.

Importing and Exporting filters



To import and export filters, use the packages feature. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. For more information on packages, see [“Managing Packages” on page 491](#).

For information on how to import and export filters on SmartConnectors, see [“Importing and Exporting SmartConnector Configurations” on page 527](#) (especially the topics on [“Creating SmartConnector Filters” on page 515](#) and [“Adding SmartConnector Filter Conditions” on page 516](#)).

Moving or Copying Filters

- 1 In the Filters resource tree, navigate to a filter and drag and drop it into another group.
- 2 Choose **Move** to move the filter, **Copy** to make a separate copy of the filter, or **Link** to create a copy of the filter that is linked to the original filter.

If you choose **Copy**, you create a separate copy of the filter that will not be affected when the original filter is edited. If you choose **Link**, you create a copy of the filter that is linked to the original filter. Therefore, if you edit a linked filter, whether it be the original or the copy, all links are edited as well. When deleting linked filters, you can either delete the selected filter or all linked filter copies.

Deleting Filters

- 1 In the Filters resource tree, right-click a filter and choose **Delete filter**.
- 2 In the dialog box, click **Yes**.

Using Filter Groups

Filter groups are created to store similar groups or filters in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's access control list (ACL).

Groups and filters can be managed with drag and drop functionality. You can move or copy groups and filters into other groups. If a group is deleted, the filters within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating Filter Groups

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a group and choose **New Group**.
- 3 In the Name text field, type in a name.
- 4 Press **Enter**.

Renaming Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.

- 2 In the Name text field, rename the group.
- 3 Press **Enter** and click **OK**.

Editing Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields, and press **Enter** after each.
- 3 Click **OK**.

Moving or Copying Filter Groups

- 1 In the Filters resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.


If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.


Deleting Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Managing Notifications

Managing Received Notifications


When the Notifications button in the Console toolbar indicates that new notifications have arrived (), you click that button to open the Notifications tab in the Viewer panel. This is your central notification repository.

You can open the Notifications manager at any time by clicking the toolbar button, even if no new notifications are present ().

To use the Notifications manager you first choose a category tab for the type of notification received.

Notification Category	Use
Pending	These are notifications that you have not yet handled (reassigned to one of the following categories). Pending notifications older than 24 hours are automatically refiled as Not Acknowledged.
Undelivered	These are notifications that were not delivered.
Acknowledged	These are notifications to which you have replied.
Not Acknowledged	Pending notifications that go unacknowledged or unresolved for more than 24 hours are automatically refiled as Not Acknowledged.

Notification Category	Use
Resolved	These are notifications for which you or a colleague have found a resolution and so have marked the notification accordingly.
Informational	These are notifications that are provided for information purposes only and do not require resolution or intervention.




If you don't see notifications appearing, make sure your ArcSight user identity (not just your e-mail address) is set as a destination in the Notifications Editor.

In a category, click **Acknowledge** to mark a selected notification as acknowledged. Click **View Event** to see the event that triggered a notification. Click **Resolve** to reclassify the notification as Resolved.

For each category of notification there is a common set of columns of information concerning them..

Notification Column	Definition
Priority	This is the same priority set by the SmartConnector and modified by the current threat level formula (and seen in grid views), unless modified by the rule that triggered the notification.
Triggering Event	The event that caused the rule to trigger the notification.
Notification Group	The branch of the Notifications resource tree to which this destination belongs.
Escalation Level	The Escalation Level (and implied destinations) the notification has reached while waiting for resolution.
Create Time	The time at which the notification was created



Also note that you can set a severity threshold for notification pop-ups and sounds in Console Preferences, and also manage your notifications from an ArcSight Web browser client.

Managing Notification Groups and Levels

This chapter describes how to handle the tasks required for managing notification groups and levels.

Creating Notification Groups

- 1 On the Navigator panel drop-down menu, choose the **Notification** resource tree.
- 2 In the Notification panel, right-click **All Destinations** and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.

- 4 Press **Enter**.



As a user, you can create new groups under **All Destinations**, but not new subgroups under existing system-defined groups.

Renaming Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Deleting Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Adding Escalation Levels

In the Notifications resource tree, right-click a notification group and choose **Add Escalation Level**.

New escalation levels are added in sequential order. If you want to add a level between two existing levels, add another level then move destinations accordingly. For example, if you have **Level 1** and **Level 2** and you want to add a level between them, add another level, **Level 3**. Then, move all destinations from **Level 2** to the new **Level 3**.

Deleting Escalation Levels

- 1 In the Notifications resource tree, select the last escalation level in a notification group.



All destinations within this escalation level will also be deleted. If you want to save the destinations, make sure you move them to another level **before** deleting.

- 2 Right-click the escalation level and choose **Delete Escalation Level**.

Managing Notification Destinations

The task descriptions in this topic explain how to manage notification destinations.

Creating Destinations

- 1 In the Notification resource tree in the Navigator panel, right-click an escalation level (such as **Level 1**) and choose **Add New Destination**.
- 2 In the Notification Editor, enter a label for the notification in the **Name** field.
- 3 Set a **Start Time** and **End Time** during the day within which the notification will be active. The default is all day (12:00:00 AM to 11:59:59 PM).

- 4 For destinations other than the ArcSight Console, select that **Destination Type** and enter the **Address**, **PIN**, or **Provider** for that device.
- 5 For the ArcSight Console, choose a **User/Group** identity.



Always set the ArcSight **User/Group** identity. If not set, notifications cannot be sent to users' Consoles.

- 6 Click **OK**.

Editing Destinations

- 1 In the Notification resources tree, right-click a notification destination and choose **Edit Destination**.
- 2 In the Notification Editor, edit the Value fields for the necessary destination attributes.
- 3 Click **OK**.

For more information, see ["Changing Notification and Acknowledgement Settings" on page 485](#).

Moving or Copying Destinations

- 1 In the Notification resources tree, find a destination and drag it to a different escalation level. You can drag across groups if needed.
- 2 Right-click the destination and choose **Move** to move it, **Copy** to make a separate copy, or **Link** to create a copy of the destination that is linked to the original destination.

If you choose **Copy**, you create a separate copy of the destination that will not be affected when the original destination is edited. If you choose **Link**, you create a copy of the destination that is linked to the original destination. Therefore, if you edit a linked destination, whether the original or the copy, all links are edited as well. When deleting linked destinations, you can either delete the selected destination or all linked destination copies.

Deleting Destinations

- 1 In the Notification resource tree, right-click a notification destination and choose **Delete Destination**.
- 2 In the dialog box, click **Yes**.

Changing Notification and Acknowledgement Settings

Administrators can configure notifications, acknowledgements, and wait-time settings. The escalation time window or wait-time depends on the event's severity.



If notifications and/or acknowledgements were disabled during Manager setup, mail server settings made through the Console will not take effect until you re-run the Manager setup to enable notifications and/or acknowledgements on the Manager side.

To run the Manager setup: (1) stop the Console and Manager, (2) re-run the Manager setup wizard from the Manager's `/bin` directory ([arcsight managersetup](#)). See the *ArcSight ESM Installation and Configuration Guide* for more information.

Changing E-mail Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit E-mail Settings**.
- 2 In the Notification Editor, type in the following text fields:

Notification Fields	Definition
From Address	The e-mail address from where the notification messages are sent. It is important that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses. For notifications sent by cell phone, any cell phone must be e-mail enabled.
Outgoing Mail Server	The host name of the local outgoing mail server. This is the SMTP server ArcSight uses to send e-mail. The Outgoing Mail Server must be accessible from the ArcSight Manager for e-mail notifications to be sent. SMTP is used to send e-mail. An SMTP server must be configured either at install time or set here.
Incoming Mail Server	The local incoming mail server host name.
Incoming Mail Protocol	Select either IMAP or POP3 mail protocols.
E-mail Account	The e-mail account name. For notifications sent by e-mail, you need to add an address to the e-mail Address field.



POP3 and IMAP can be used to check for e-mail acknowledgments. You can specify these options at install time, or set them here. For acknowledgements, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

- 3 Type the **E-mail Account** password in the Password text field and confirm it in the Confirm **Password** text field.
- 4 Click **OK**.

Adding New Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings**, **Edit Pager Providers**, then **New Service Provider**.
- 2 In the Notification Editor, type in the following text fields:

Pager Notification Field	Description
Provider Name	The name of the service provider, such as Skytel.
Host	The host name for the service provider's server, such as snpp.skytel.com. SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager provider host and port information.
Port	The port number for the service provider's server.

- 3 Click **OK**.



For notifications sent by pager, firewalls must be configured so that the pager can connect directly to the paging service provider. ArcSight currently supports any provider that supports SNPP.

Editing Pager Service Provider Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, edit the text fields.
- 3 Click **OK**.

Deleting Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, click **Delete**.

Changing Wait Time Settings

The default wait-time values for Very-High severity is set for 2 minutes, High is set at 5 minutes, Medium is set for 30 minutes, and Low is set for 2 hours.

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit Escalation Wait Time**.
- 2 In the Notification Editor, type in the wait time for the hour (**Hr**) and minute (**Min**) text fields for **Very-High**, **High**, **Medium**, or **Low** severity.
- 3 Click **OK**.

Testing Notification Groups and Destinations

This topic describes how to test notification groups and destinations.

Testing Group Notifications

In the Notification resource tree, right-click a populated notification group and choose **Test Group Notification**.

A test notification message is sent to the notification destination. Test notifications are not sent to group notification destinations if the End Time has expired. For example, if you test group notification at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message will not be sent to the group.

Testing Destination Notifications

In the Notification resource tree, right-click a notification destination and choose **Test Destination Notification**.

A test notification message is sent to the notification device. Test notifications are not sent to notification destinations if the End Time has expired. For example, if you test a notification destination at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message will not be sent to the device.

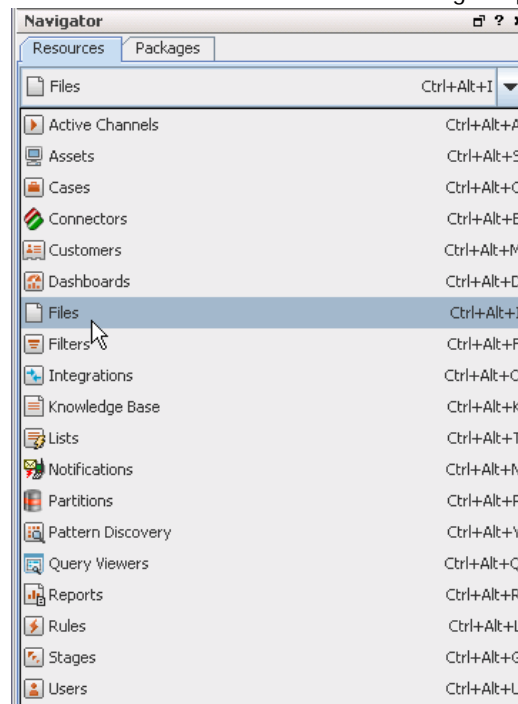
Managing File Resources

The Files resource tree, when populated, lists various files that have been saved as resources so that they are accessible to all users of the system who are authorized for such access. File resources include Case file attachments, templates, and general-purpose shared files.

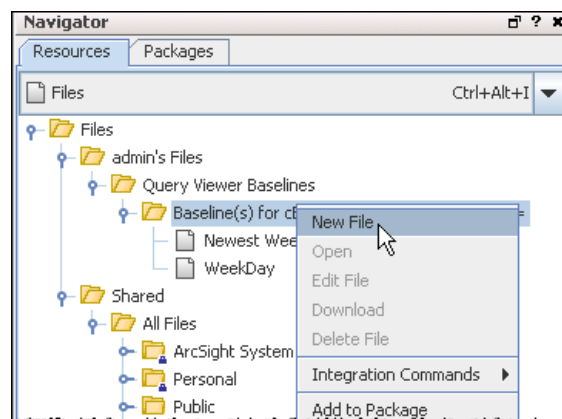
In addition to the tasks detailed below, you can also rename or lock a file, get a Graph View of a file, and so forth. Simply select the file in the Navigator, right-click, and choose a menu option. Operations on groups are also available. Options may vary depending on which file or folder you have selected in the Navigator.

Uploading Files and Creating a File Resource

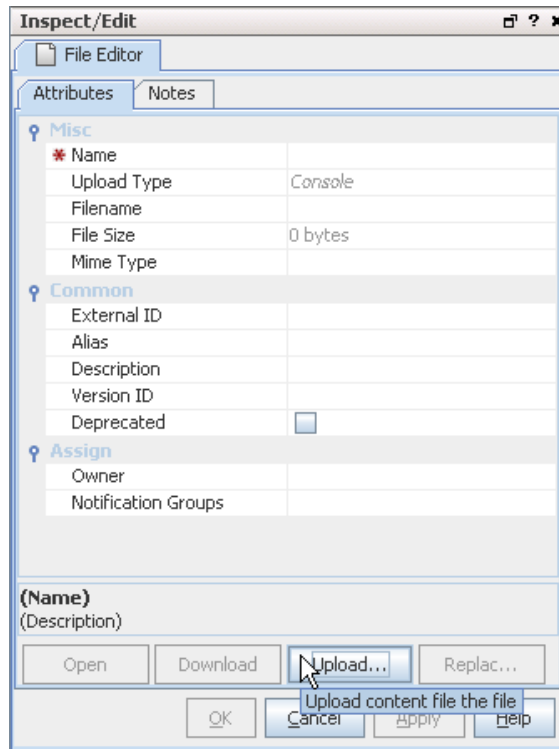
- 1 Choose the **Files** resource tree in the Navigator panel.



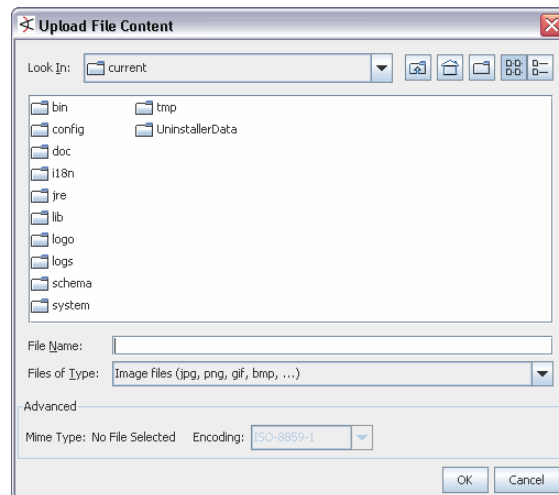
- 2 Right-click a file group and choose **New File**.



This brings up the File Editor in the Inspect/Edit panel.



- 3 Click the **Upload** button on the File Editor and select the local file to add.



- 4 On the File Editor Attributes tab, enter values for the attributes that identify the file.
The Name attribute is initially the same as the Filename attribute, but you can change the Name.
Certain attributes are read-only: Upload type is Console, and Filename, File size, and Mime type are set based on the selected file.
- 5 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Viewing Files

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Open**.
- 3 The file will be downloaded to a temporary directory (in a sub-directory called **arcsight-files**) and will launch in an appropriate viewer, usually a web browser.

You can also open a file resource from the File Editor by clicking the **Open** button.

Downloading Files Locally

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Download**.
- 3 Specify a location and file name for the new local file.



File resources can be downloaded as often as needed by any console user authorized to access the file resources. Downloading a file does not change the file resource, or the shared file contents on the server.

You can also Download a file resource from the File Editor by clicking the Download button.

Editing File Resource Attributes

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Replacing File Resource Contents

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Click **Replace** and select the local file containing the new contents for the file resource. The file resource name will change if the selected local file has a different name.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Deleting File Resources

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Delete File**.
- 3 Click **Yes** to confirm the deletion.

Adding a File or Folder to a Package

From the Files resource Navigator, you can add a file or folder to an existing package or create a new package and add the file to it.

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file or folder and choose **Add to Package**.
This brings up the Package Selector dialog.
- 3 In the Package Selector dialog, do one of the following:
 - ◆ Navigate to a package to which you want to add the file or folder, and click **OK**. (The file is saved to the selected package.)
 Or
 - ◆ Navigate to a location where you want to create a new package and click **New Package**. (This brings up the Package Editor where you can name and configure the new package. The selected file or folder will be included in the new package.)

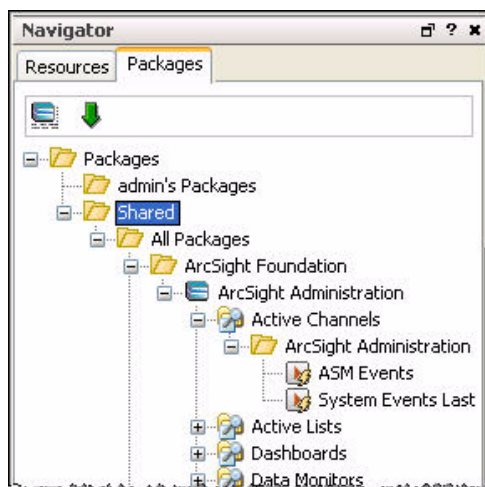
Finding Files


To find files stored on the Manager, choose **Files** in the Navigator and browse the folders or choose **Edit > Search** from the menus, enter a file name in the **Search query** field, and click **Find**. (See ["Finding Resources" on page 534](#) for more information on this utility.)

For more information, see ["Managing Packages" on page 491](#).

Managing Packages

Packages are collections of resources that can be installed into the system resource tree.




To access available packages, click the **Packages** tab of the Navigator panel. The tree of all packages is displayed along with the resources within each package. The  button toggles between Normal and Advanced view of the package tree. In the Advanced view, uninstalled packages are visible and package dependencies are shown.



Please do not import or install older, pre-v4.x system content into ArcSight ESM version 4.x systems. Doing so can cause unpredictable consequences on the ArcSight Manager and associated Console clients. (In this release, the Packages feature does not prevent import or install of older system content.) For more information, see ["Managing Pre-v4.x Content" on page 498](#).


Viewing Installed Packages

Click the **Packages** tab in the Navigator panel. If the  button is highlighted, click it to return to Normal view. The tree view is like the tree view of any other resource except that the resources contained within packages may be of many different types.




The Packages tree view is independent of which resource you have selected in the Navigator. Regardless of which resource is selected, when you click on the **Packages** tab, you will see the same set of packages. These include the ArcSight stock content packages installed on the Manager along with any custom packages administrators have created on this Manager.

Viewing all Packages (with Dependencies)

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view. In the Advanced view, all packages (including uninstalled packages) and package dependencies are shown.

Showing Package Archive Contents

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view (to show all packages including uninstalled packages). Right-click a package and choose **Show Package Archive Contents** or **Show Current Package Archive Contents** (available only on installed packages). This lists all resources in the package, including details such as resource name, type, and full path to location in the tree.

Creating Packages

- 1 Right-click the **Package Group** in the Packages tree that will contain the new Package. Choose **New Package**.
- 2 In the Package Editor that opens in the Inspect/Edit panel, enter the following fields

In this field...	...enter this
Name	Enter a name for the new package.
Required Packages	Specify the packages that must be installed for this package to function.
Optional Packages	Specify packages that are related to this package, but which are not required for it to function.
Required Features	Enter any ArcSight ESM features that must be available for this package to function. The pick list of features includes Pattern Discovery, for example.
Installed	(Read-only.) Check this box to indicate that the new package is installed. Unchecking this box is a good way to preview a new package before making its resources visible to all users of the system.
Update Available	(Read-only.) Check this box to indicate to other users that a newer version of the package exists.

In this field...	...enter this
Author Name	Enter the name of the author or source for the new package.
Package Version	The package version can be any string, but by convention, ArcSight recommends a format of 0.0.0.0, with numbers in decreasing importance (major, minor, release, build).
ArcSight Version	(Read-only.) The minimum ArcSight Version needed to support this package.
Format	<p>(Advanced) if you need a specific behavior, choose one of the choices other than default. Otherwise, leave this field set to default.</p> <p>Default - Appropriate format for backing up resources on a Manager. This format captures more information than the other options, including information specific to a Manager installation.</p> <p>Export - A portable format appropriate for packaging resources for transport between systems in which Manager-specific information is excluded from the exported package for resources with attributes that would otherwise retain such information upon a "default" export.</p> <p>For example, a trend packaged in "export" format does not include Start Time or End Time trend attributes nor original table IDs. Instead, the imported trend uses Start and End times that correspond to the time the package is installed on a new system. Also at time of package install, a new trend table is created. (See also, descriptions of Imported Trend Start Time and Imported Trend End Time fields under advanced Trend Attributes in "Building Trends" on page 241.)</p> <p>Similarly, active lists and session lists packaged in "export" format do not include locked by attributes, table IDs, or session/active list entry attributes, respectively. New tables are created when the lists are imported, and the other attributes are tracked starting with launch of these resources on the new system.</p> <p>The package "export" format packages other resources similarly as a means of optimizing portability for content distribution.</p> <p>ArcSight system content is packaged using the "export" format. Also, Managed Service Security Providers (MSSPs) who provide content to ArcSight ESM installations at various customer sites might typically package resources in this format.</p> <p>Exportuser - Highly portable format appropriate only for exporting user accounts with no permissions, personal group information, or relationships to other resources. If you want to export user accounts that include permissions and groups, use the default format instead.</p> <p>Upgrade - For use by ArcSight Professional Services only. This format might be used for ArcSight initiated incremental resource upgrades of older systems in particular circumstances. (In most cases, standard upgrade utilities and processes are used instead.)</p>
Obfuscated	(Advanced) Check this box to scramble the package contents to prevent unauthorized viewing or modification.

In this field...	...enter this
Exclude Reference IDs	(Advanced) Check this box to remove reference IDs from the package when it is exported. Generally, you would exclude reference IDs only when you plan to import the package into a different ArcSight system. Leave the box unchecked to include reference IDs, which improve performance for packages that are imported to the same Manager from which they were exported.

- 3 Click the **Resources** tab in the Package Editor. Click the **Add** drop-down menu to select the resources that this package will contain. You can select groups or individual resources.

Check the Children Only box to include resources below the specified resource in the tree. For example, selecting the group /All Session Lists/ArcSight Administration/User and checking Children Only would include only the session list resources in that group, not the group itself.


Check the Only If Referenced box to conditionally include resources if they are referenced by other resources without the Only If Referenced box checked.

- 4 To exclude resources from the new package by resource type or by specifying actual resources to be removed, use the Removed Resources panel in the lower half of the Resources tab. To exclude resources by type, click the **Excluded Resource Types** tab and select from the list of available types. To exclude specific resources, click the **Removed Resources** tab, click the **Add** drop-down menu, then choose the resource(s) you wish to exclude using the resource picker.



The only way to exclude Asset Category resources from a package is to specify the Asset Categories explicitly using the Removed Resources tab.

Importing Bundles

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Click the  icon to import a bundle.
- 3 Choose an .arb file to import and click **Open**.
- 4 Review the Import dialog for any conflicts. Each conflict will display one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window.
- 5 Click **OK** to continue. When the import is done, a Summary Report is displayed describing the packages that were imported.
- 6 By unchecking the box next to each package, you can choose to import a package without installing it. The default is to install all imported packages.



Please do not import older, pre-v4.x system content into ArcSight ESM version 4.x systems. Doing so can cause unpredictable consequences on the ArcSight Manager and associated Console clients. (In this release, the Packages feature does not prevent import of older system content.) You can import any custom content with no problems, including pre 4.x content, as long as it does not reference pre-v4.x system content. For more information, see ["Managing Pre-v4.x Content" on page 498](#).



Packages, like other resources, are always displayed under the user folder in which they were created. Upon import, the Summary Report shows the URI or full path into which the package was imported (for example, "Packages Imported: /All Packages/Personal/Vicky's Packages/VPN Logins Reporting"). The import location is not configurable. If you log in with a different username and import a package, you may or may not have write access to the package (depending on permissions). If you import the package with a different username on a Manager that does not include an account for the package originator, you will not see the imported package. If you recreate an account on the Manager with the same username as the package originator, the imported package will be visible again.

For more information, see ["Resolving Package Conflicts" on page 497](#).


Exporting Packages

- 1 Click the **Packages** tab in the Navigator panel and click to select one or more packages to export.
- 2 Right-click and choose **Export Package to Bundle**.
- 3 Enter a name and folder for the local bundle file. The default extension is **.arb**.

The exported bundle will have reference IDs if that box was checked in the Package Editor, and it will be obfuscated if that box was checked in the editor.

Installing Packages

If you chose not to install a package when its bundle was imported, or if you left the Installed checkbox unchecked when you created a package, it will be uninstalled. Uninstalled packages are not shown in the Normal view of the package tree.

- 1 Click the **Packages** tab in the Navigator panel. If the  icon is not highlighted, click it to switch to the Advanced view.
- 2 Right-click the uninstalled package (shown with a gray icon) that you would like to install and choose **Install Package**.
- 3 Review the dialog for any conflicts. Each conflict will display one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window.



Please do not install older, pre-v4.x system content into ArcSight ESM version 4.x systems. Doing so can cause unpredictable consequences on the ArcSight Manager and associated Console clients. (In this release, the Packages feature does not prevent install of older system content.) You can install any custom content with no problems, including pre-v4.x content, as long as it does not reference pre-v4.x system content. For more information, see ["Managing Pre-v4.x Content" on page 498](#).

For more information, see ["Resolving Package Conflicts" on page 497](#).

Uninstalling Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be uninstalled. Choose **Uninstall Package**. (This command is disabled if the package is already uninstalled or if it is locked.)

Uninstalling a package removes its resources from the system and hides the package in Normal view, but it remains in the system and can easily be installed again.

Dependent resources will be deleted automatically unless they are contained in another package.

For more information, see [“Resolving Package Conflicts” on page 497](#).

Editing Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Change the package name or other properties on the Attributes tab. For more information on package fields, see [“Creating Packages” on page 492](#).
- 4 Click the **Resources** tab to add or remove resources from the package.

Adding Resources to Packages

You can add to a resource to an existing package by using the right-click menu on a selected resource in the Navigator tree.

- 1 Click the **Resources** tab in the Navigator panel.
- 2 Choose the resource type you want to add (for example, Reports).
- 3 Navigate to and right-click the particular resource you want to add (for example, My Report), and choose **Add to Package**. The system displays the Package Selector dialog.
- 4 Select a package to which to add the selected resource and click **OK**.

Removing Resources from Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Click the **Resources** tab in the Package Editor.
- 4 In the upper half of the Resources tab, select the resource you want to remove. (A gray highlight on the entire row indicates the resource is selected.)
- 5 Click **Remove**.

Deleting Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be deleted and choose **Delete Package**.
- 3 Confirm that you want to delete the specified package.
- 4 Choose **Remove Resources in Package** or **Leave Resources**. If you Leave Resources, only the package itself will be deleted. The resource that it contained will remain in the system resource tree. If you Remove Resources, all resources that the package contained will be deleted from the system resource tree.



Deleting a package that contains resources that maintain state--active lists with values, session lists, or trends--will delete the state information as well.

For more information, see ["Resolving Package Conflicts" on page 497](#).

Resolving Package Conflicts

Package conflicts can occur during install, uninstall, delete, or import of packages. Most package conflicts are resolved internally by the ArcSight Manager without the need for user intervention. However, some package conflicts will prompt the administrator for an appropriate course of action from among several options. This section describes two of these scenarios as examples.

If the ArcSight Manager detects package conflicts for a pending package **uninstall**, the Console provides choices for resolving the conflict and proceeding, or aborting the uninstall operation. The options provided depend on the type of conflict detected.

For example, if you attempt to uninstall a package that changed since it was installed, the conflict is indicated and you are asked to choose from the following **Resolution Options**.

Option	Description
Create a new archive for package	Creates a new archive for the modified package (and retains original).
Create new archive for remaining changed packages	Creates new archives for all changed packages before uninstall (retains all originals).
Continue without saving changes	Uninstalls this package without saving changes.
Uninstalls this and remaining packages without saving changes	Uninstalls all selected packages without saving changes.
Abort	Abandons the uninstall process and keeps the package(s) as is.

If the ArcSight Manager detects package conflicts for a pending package import or install, the Console provides choices for resolving the conflict and proceeding, or aborting the import operation. The options provided depend on the type of conflict detected.

For example if you attempt to import a package with content that is older than the currently imported package, the conflict is indicated and you are asked to choose from the following Resolution Options:

Option	Description
Leave newer packages	Leaves the newer packages installed.
Never override newer packages	Completes the import but imports only packages that are newer than those currently installed.

Option	Description
Update packages	Imports the selected packages, and prompts for package conflict resolutions on a per-package basis.
Always update packages	Imports the selected packages, and overwrites newer packages if they exist.
Abort	Abandons the uninstall process and keeps the package(s) as is.

Managing Pre-v4.x Content

Please do not import or install older, pre-v4.x system content into ArcSight ESM version 4.x systems. Doing so can cause unpredictable consequences on the ArcSight Manager and associated Console clients. (In this release, the Packages feature does not prevent import or install of older system content.)

Custom content will be compatible across versions. You can import and install custom content, including pre-v4.x content, as long as it does not reference pre-v4.x system content. You can encounter problems if you import/install custom content that references older system content.

Before importing archive files, edit the files to exclude URIs that reference ArcSight system content.

To determine whether ArcSight system content is included in an archive, we recommend either of the following methods:

- Read through the archive XML
- Use the `arcsight archive` command with the `list` option to show referenced URIs:
`arcsight archive –action list –f <archive file path>`

See the *ArcSight ESM Administrator's Guide* for more information on working with the archive command and other utilities.

Managing SmartConnectors

ArcSight SmartConnectors can be configured to optimize their performance and increase their functionality. You can configure SmartConnectors to enable aggregation, batching, and time filter correction functionality. You can also send control commands, from the ArcSight Console, to SmartConnectors to manage the flow of events.

Selecting and Setting SmartConnector Parameters

From the Console, use the Connector Editor to control SmartConnectors.

Configuring the SmartConnector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to manage and choose **Configure**. This opens the **Inspect/Edit** panel for the **Connector Editor**. On the Connector tab, the Name field is automatically populated with the name assigned during SmartConnector Installation.

- 3 Type in the **Connector Location** and the **Device Location**. All events are tagged with these fields by the ArcSight SmartConnector. Creation date and other information is automatically populated.
- 4 On the Default tab, change any additional Batching, Time Correction or other parameters as desired, using the configuration fields explanations provided below.
- 5 Click **Apply** to add your changes and to keep the Connector Editor open. To apply your changes and close the Connector Editor click **OK**, or, if applicable, click **Add Alternate** to save your changes as an alternate configuration you can select and apply later.

The description entry associated with the setting provides tool tip information. These parameters are not localized since they come directly from the connector and the connector may contain new resources (since it may be a newer version).

The framework for connector commands operates in a similar way. Configuration of the connector command menu is achieved by sending the list of commands that are supported on the connector at registration time.



The ArcSight Console doesn't currently provide support for command parameters.

There are several controls you can adjust in the Connector Editor. The variety of options are best summarized by briefly describing what's available at each of the editor's tabs or subtabs.

Connector Editor Option Tabs

Table 20-6 Connector Editor Option Tabs

Connector Tabs	Options
Connector Tab Configuration Fields	Basic identification, ownership, and date/time parameters.
Networks	The ArcSight network(s) to which the connector is or can be assigned.
Default Content Tab Configuration Fields	Includes options for report batching, aggregation, and time corrections.
Default: Filters	A filter condition editor for constraining what the connector reports. (Please see "Managing SmartConnector Filter Conditions" on page 515 and "Common Conditions Editor" on page 616 for details on how to define filters for connectors.)
Alternate: Content	A set of options identical to those under Default, which you can use to create alternate configurations.
Alternate: Filters	A filter condition editor for constraining what the connector reports, in an alternate configuration.
Notes: Table	A text editor for, and tabular list of, configuration notes.

Connector Tabs	Options
Notes: List	A text editor for, and text presentation of, configuration notes.

Connector Tab Configuration Fields

You do basic configuration through the Connector and Default: Content tabs. Many of these fields correspond to resource editor fields. See also [“Common Resource Attribute Fields” on page 552](#).

Table 20-7 Connector Tab Configuration Fields

Name Field	Value Field
Name	The Name text field is automatically populated with the name assigned during SmartConnector installation.
ID	The identification string assigned during SmartConnector installation.
Status	The SmartConnector's current mode of operation.
Connector Location	A description of the (usually) physical location of the SmartConnector. This appears in all the events issued from the connector.
Device Location	A description of the (usually) physical location of the device the SmartConnector is monitoring. This appears in all the events issued from the connector.
Version	The connector's software version number.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight ESM. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your ArcSight ESM administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight ESM. A given alias will appear in place of the resource's name everywhere it may be seen. Your ESM administrator can advise you on the correct values for this field, if applicable.
Description	A text description of the configuration or other related information. This text appears as a tooltip to any ArcSight user who has Console access to the connector.
Owner	An ArcSight ESM user selected from the Users resource tree who should be notified about this connector.

Name Field	Value Field
Notification Groups	The ArcSight ESM user groups selected from the Users resource tree who should be notified about this connector.
Created By	A user identity provided at SmartConnector installation.
Creation Time	The time of SmartConnector installation.
Time Since Creation	A value calculated from Creation Time.
Last Updated By	The time of the last configuration change.
Last Update Time	The time of the last configuration change.
Time Since Last Update	A value calculated from Last Update Time.

Default Content Tab Configuration Fields



SmartConnector configuration options available may vary depending on which version of SmartConnectors you are using. SmartConnector configuration options come directly from the connector, and newer versions of connectors might contain new or different resources than previous versions.

Table 20-8 Default Content Tab Configuration Fields

Name Field	Value Field
Batching	SmartConnectors can batch events to increase performance and optimize network bandwidth. When activated, SmartConnectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires. You can also prioritize batches by severity, forcing the SmartConnector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, 100 events).
Enable Batching (in seconds)	The SmartConnector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is Time Based if the SmartConnector should send batches as they arrive (the default) or Severity Based if the SmartConnector should send batches based on severity (batches of Highest Severity events sent first).

Name Field	Value Field
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the SmartConnector to automatically correct the time reported by the device.
Use Connector Time as Device Time	(No Yes) Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. The default is No .
Enable Device Time Correction (in seconds)	The SmartConnector can adjust the time reported by the device Detect Time , using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol.
Enable Connector Time Correction (in seconds)	The SmartConnector can also adjust the time reported by the Connector Time SmartConnector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the SmartConnector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and SmartConnectors is the NTP protocol.
Set Device Time Zone To	(Disabled <TimeZone>)(Default is Disabled) Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the SmartConnector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported.
Device Time Auto-correction	
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by Past Threshold seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by Past Threshold seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, (ALL) means all devices.
Time Checking	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking.
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is 1 hour (3,600 seconds).

Name Field	Value Field
Frequency	The SmartConnector checks its future and past thresholds at intervals specified by this number of seconds. Default is 1 minute (60 seconds).
Cache	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Cache Size	SmartConnectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the SmartConnector receives bursts of events. This parameter specifies the disk space to use. The default is 1 GB which, depending on the connector, can hold about 15 million events, but it also can go down to 5 MB . When this disk space is full, the SmartConnector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is 10,000.
Notification Frequency	How often to send notifications once the Notification Threshold is reached. (1 min, 5 min, 10 min, 30 min, 60 min.)
Payload Cache	If the represented SmartConnector supports it, setting this to True causes the connector to automatically create and populate a cache for device payload data. This capability improves upon the previous ability to manually retrieve individual payloads. The payload data is retrieved from the original device or retained from the received event data, depending on how it operates. The default setting is False . Consult the a SmartConnector's Configuration Guide to find out whether it supports this capability. Changes to this setting take effect after you restart the SmartConnector.
Payload Cache Size	If Payload Cache is True , these choices determine the maximum size of the cache. The cache operates on a last-in-first-out (LIFO) basis.
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the ArcSight Manager. The default is 10 seconds , but it can go from 5 seconds to 10 minutes . Note that the heartbeat is also used to communicate with the SmartConnector; therefore, if its frequency is set to 10 minutes , then it could take as much as 10 minutes to send any configuration information or commands back to the SmartConnector.
Enable Name Resolution	(Enabled Disabled) The SmartConnector tries to resolve IP addresses to host names, and host names to IP addresses, if the event rate allows it and if required. This setting controls this functionality. The Source, Target and Device IP addresses and Hostnames may also be affected by this setting. (Default is Enabled)

Name Field	Value Field
Name Resolution Host Name Only	(Yes No) If set to Yes, for reverse resolution (IP Address to Host name), only the host name field is set. If set to No, the host name is split up and put into both the DNS domain and the host name fields. This affects the source, destination, device and SmartConnector name fields. (Default is Yes)
Name Resolution Domain from Email	(Yes No) If set to Yes, the host name and DNS domain fields are empty, and the corresponding user name field appears as an email address, then the domain from the email address is put in the DNS domain field. This only affects the source and destination fields. (Default is Yes)
Clear Host Names Same as IP Address	(Yes No) If set to Yes and the host name field is set to an IP Address that matches the corresponding IP Address field, then the host name field is cleared. This affects the source, destination, and device fields. (Default is Yes)
Don't Resolve Host Names Matching	<p>By default, host names are resolved to their IP addresses. You have the option to specify a regular expression for all or part of a host name <i>for which you do not want the system to attempt host name resolution to an IP address.</i></p> <p>When this option is configured, the system will not attempt to resolve host names matching this expression.</p>
Don't Reverse-Resolve IP Ranges	<p>By default, IP addresses are resolved to their domain names. You have the option to specify IP address ranges <i>for which you do not want the system to attempt reverse-resolution to domain names.</i></p> <p>When this option is configured, the system will not attempt to reverse-resolve IP addresses that fall within any of the specified ranges.</p>
Limit Bandwidth To	A list of bandwidth options you can use to constrain the connector's output over the network. (Disabled , 1 kbit/sec to 10 Mbits/sec.)
Transport Mode	<p>You can configure the SmartConnector to cache to disk all the processed events it receives. This is equivalent to pausing the SmartConnector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (Normal Cache Cache (but send Very High severity events)).</p>
Address-based Zone Population Defaults Enabled	This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 because the system has integral zone mapping.

Name Field	Value Field
Address-based Zone Population	This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 because the system has integral zone mapping.
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's source address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Source Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated source address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Destination Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's destination address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Destination Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated destination address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Connector Zone UR	When populated, this field shows the URI of the zone associated with the SmartConnector's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.

Name Field	Value Field
Connector Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Device Zone URI	When populated, this field shows the URI of the zone associated with the device's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Device Translated Zone URI	When populated, this field shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.

Name Field	Value Field
Field Based Aggregation	<p>This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, the fields of the two events are the same per the fields listed in the description of "Enable Aggregation (in seconds)" on page 510. However, field-based aggregation implements a more flexible aggregation mechanism; two events are aggregated if only the <i>selected</i> fields are the same for both events. (Note: Field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored, unless "Preserve Common Fields" is set to "Yes".)</p> <p>Field-based aggregation offers several advantages over basic aggregation, including:</p> <ul style="list-style-type: none"> • Control over what fields to aggregate on • Start and end time set to the earliest start time and latest end time, respectively (instead of taking the values from the first event in the group, like basic aggregation) • Option to preserve common fields • Option to sum one or more numeric fields <p>SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate "accepts" and "rejects" in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.</p> <p>Note: The legacy, basic aggregation feature is described in the field description for Enable Aggregation (in seconds).</p>
Time Interval	<p>Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled, 1 sec, 5 sec, and so on, up to 1 hour.)</p>
Event Threshold	<p>Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled, 10 events, 50 events, and so on, up to 10,000 events.)</p>

Name Field	Value Field
Field Names	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. Use Ctrl+click to select multiple fields. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-host names. You can use any of the event fields displayed in the event inspector; the name can contain no spaces and the first letter should not be capitalized.
Fields to Sum	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. If specified, this set of numeric fields is summed rather than aggregated, preserved, or discarded. The most common fields to sum are bytesIn and bytesOut . Note that if any of the fields listed here are also in the list of field names to aggregate, they are aggregated and not summed.
Preserve Common Fields	(Yes No) Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing No , the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events). SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you will then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Fields to Sum	(Optional) Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.

Name Field	Value Field
Processing	
Preserve Raw Event	<p>(Yes No) Some devices contain a raw event that can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field in the event inspector. This feature is disabled, by default, since using raw data increases the event size and therefore requires more database storage space.</p> <p>You can enable this by changing the Preserve Raw Event setting. If you choose Yes, the serialized representation of the "Raw Event" is sent to the ArcSight Manager and preserved in the Raw Event field.</p>
Turbo Mode	<p>If your configuration, reporting, and analytic usage permits, you can greatly accelerate the transfer of a sensor's event information through SmartConnectors by choosing one of two "turbo" (narrower data bandwidth) modes. The default transfer mode is called Complete, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).</p> <p>Complete mode does indeed use all the database performance advances of ArcSight v3.x.</p> <p>The first level of Turbo acceleration is called Faster and drops just additional data, while retaining all other information. The Fastest mode eliminates all but a core set of event attributes, in order to achieve the best throughput. Consider the possible effects such a restricted data set might have from a given device (e.g., on reports, rules, threat resolution) before selecting it.</p> <p>The specific event attributes that apply to these modes in your enterprise are defined in the self-documented \$ARCSIGHT_HOME/config/connector/agent.properties file for the ArcSight Manager. Because these properties may have been adjusted for your needs, you should refer to this file for definitive lists.</p> <p>Only scanner SmartConnectors must run in Complete mode, to capture the additional data.</p> <p>Note: SmartConnector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to Faster will not pass all the data possible for a SmartConnector that is set for the default of Complete.</p>

Name Field	Value Field
Enable Aggregation (in seconds)	<p>Note: If you have already used this feature for setting up previous SmartConnectors, you can continue to do so. However, ArcSight recommends that you use the new Field Based Aggregation feature as a more flexible option. (Please see “Field Based Aggregation” on page 507.)</p> <p>Here is the description of the legacy “Enable Aggregation” feature, for those of you who are still using it:</p> <p>When enabled, Enable Aggregation (in seconds) aggregates two or more events on the basis of the selected time value. (Disabled, 1, 2, 3, 4, 5, 10, 30, 60)</p> <p>The aggregation is performed on one or more matches for a fixed subset of fields:</p> <ul style="list-style-type: none"> • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) <p>The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.</p>
Limit Event Processing Rate	<p>You can moderate the SmartConnector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts.</p> <p>The choices range from Disabled (no limitation on CPU demand) to 1 eps (pass just one event per second, making the smallest demand on the CPU).</p> <p>Be sure to note that this option's effect varies with the category of SmartConnector in use, as described in the SmartConnector Processing Categories table below.</p>

Name Field	Value Field
Fields to Obfuscate	Using MD5 hashing, this option allows you to specify a list of fields for obfuscation in a security event.
Store Original Time In	This parameter allows you to move the original device receipt time to a specified field if altered by the time correction.
Enable Port-Service Mapping	<p>(Disabled Enabled)</p> <p>If Enabled and one of the two fields destination port and application protocol is set, and the other is not, the one that is set is used to set the other. For example, if the destination port is 22 and application protocol is not set, then the application protocol is set to ssh.</p> <p>Default is Disabled.</p>
Enable User Name Splitting	<p>(Yes No) If this is set to yes and the destination user name contains commas in the event, this parameter duplicates that event. Each user name in the list is placed in one of the events.</p> <p>For example, if the destination user name in an event is "User 123, User 456", then that event is sent twice, with the destination user name set to "User 123" in the first and "User 456" in the second.</p> <p>Default is No</p>
Split File Name into Path Name	<p>(Yes No) If this is set to yes and an event's file name field is set but its file path field is not, this parameter splits the file name into a path and a name, placing each part into appropriate fields.</p> <p>For example, if the file name field is set to <code>C:\dir\file.ext</code> and the file path is not set, then the file path is set to <code>C:\dir</code> and the file name to <code>file.ext</code>. The separator character can be either \ or / as the system looks to the SmartConnector to determine its platform.</p> <p>Default is No</p>
Event Integrity Algorithm	<p>(Disabled SHA-256 SHA-1 MD5 SHA-512)</p> <p>If this is set to one of the algorithms (such as SHA-256), and the Preserve Raw Event parameter is Enabled, then additional event integrity internal events are generated, normally at a rate of about 1 per 50 normal events.</p> <p>The crypto signature field is <i>also</i> set in each event in the format: "<code>#seq(alg):digest</code>", where <i>seq</i> is a persistent event sequence number, <i>alg</i> is the message digest algorithm, and <i>digest</i> is the hexadecimal message digest.</p> <p>These extra events and the crypto signature field values can be used to verify that no events were tampered with after generation.</p> <p>Supported algorithms are: SHA-256, SHA-1, MD5, and SHA-512.</p> <p>Default is Disabled (i.e., no algorithm is applied)</p>

Name Field	Value Field
Generate Unparsed Events	<p>(Yes No) If set to yes and some incoming event data cannot be parsed (perhaps because a device has been upgraded since the SmartConnector parser was written), then a special event named "Unparsed Event" is generated. The raw event appears in the event message field.</p> <p>If set to No, the SmartConnector log files indicate the unparsed events.</p> <p>Default is No</p>
Preserve System Health Events	<p>(Yes No) If set to yes, internal system health events are preserved.</p> <p>SmartConnectors generate system health events that provide information about the systems on which they are installed (e.g., disk usage, network memory, JVM memory, percentage of processing of CPU memory usage, and so forth). By default, these events are not retained or passed on to ArcSight destinations like ESM and, therefore, not available for viewing. Setting this option to yes makes them available in the Console.</p>

Name Field	Value Field
Enable Device Status Monitoring (in milliseconds)	<p data-bbox="824 258 1279 285">(<NumberOfMilliseconds> -1 (disabled))</p> <p data-bbox="824 296 1377 426">If set to a <NumberOfMilliseconds>, the selected SmartConnector generates internal events periodically 1 minute (60000 milliseconds) or greater with the status of the devices for which the connector is receiving normal events.</p> <p data-bbox="824 436 1377 516">These events have the name "Connector Device Status," and are intended primarily for the use of content in ESM v.4.0 SP3 and newer versions.</p> <p data-bbox="824 527 1377 606">Enabling periodic device status monitoring events helps monitor both the SmartConnector and device uptime.</p> <p data-bbox="824 617 1377 667">Device status monitoring events include this information, if available:</p> <ul data-bbox="824 678 1377 972" style="list-style-type: none"> <li data-bbox="824 678 1279 705">• Event name (Connector Device Status) <li data-bbox="824 716 1203 743">• Vendor and Product information <li data-bbox="824 753 1203 781">• Source Address and Host Name <li data-bbox="824 791 919 819">• Zone <li data-bbox="824 829 1073 856">• Last event received <li data-bbox="824 867 1377 926">• Total number of events for the device since the connector started <li data-bbox="824 936 1143 963">• Event count since last call <p data-bbox="824 974 1377 1087">Device status monitoring events can be set to generate every 1 minute (60000 milliseconds), or less frequently (i.e., a greater number of milliseconds than the minimum).</p> <p data-bbox="824 1098 1377 1211">If you specify a number less than 60000, you will get a warning message in the log indicating that the minimum is 60000 milliseconds (1 minute) and that the system will use the minimum.</p> <p data-bbox="824 1222 1377 1335">If you enter a non-number in the field, this generates an error in the log indicating the value could not be parsed. In this case, the feature will be disabled (and the log message will say that).</p> <p data-bbox="824 1346 1377 1440">In such cases, there is no indication on the Console that anything went wrong because there is no mechanism for the Connector to convey that error.</p>

Name Field	Value Field
Payload Sampling	Payload sampling is used by some SmartConnectors to send a portion of packet payload (as opposed to the complete packet payload) along with the original event. This portion is retrieved using the on-demand payload retrieval in the event inspector.
Maximum Length	<p>This feature allows you to configure the maximum length of the payload sample using the following values:</p> <ul style="list-style-type: none"> • Discard • 128 bytes • 256 bytes • 512 bytes • 1 Kbyte <p>When the Discard option is chosen, no payload sample is sent inside the original event.</p>
Mask Non-printable Characters	This feature allows you to mask the non-printable characters in the payload sample.

SmartConnector Processing Categories

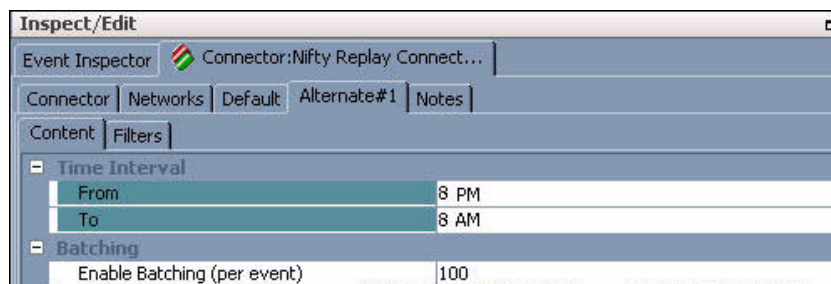
Table 20-9 SmartConnector Processing Categories

SmartConnector Type	Effects of Limited Usage
Syslog connectors	Due to the nature of UDP (the transport protocol used by Syslog), these connectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache may fill and the operating system drop UDP messages. Note that ArcSight does not recommend using the Limit CPU Usage option with these connectors because of this possibility of event loss.
SNMP connectors	Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they potentially lose events. SNMP is also UDP-based and has the same issues as Syslog.
Database connectors	Since connectors "follow" the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. On the other hand, note that no events will be lost, unless the database tables are truncated. After the event burst is over, the connector may eventually catch up with the database if the event rate does not exceed the configured limit.

SmartConnector Type	Effects of Limited Usage
File connectors	Similar to database connectors, file-based connectors "follow" files, so limiting their event rates also causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. Similarly, the connectors may catch up if the event rate does not exceed the configured rate.
Proprietary API connectors	These connectors' behavior depends on the particular API, (e.g., OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. Therefore, these connectors work much like database or file connectors.

SmartConnector Time Interval Options

This time interval applies to the Alternate Settings and it specifies when the alternate settings must be used by the SmartConnector. For example, if you want to cache the events during the day and send everything at night, you can configure the Transport Mode to cache in the default configuration and configure the Transport Mode to normal in the Alternate Settings, then you would set the time interval from 8PM to 8AM (next day).



- **"From:"** Specifies the starting time to apply the Alternate settings.
- **"To:"** Specifies the ending time that the Alternate settings will no longer apply (and revert to the default settings). If this is less than the From setting, the value will be interpreted as "next day". For example, a setting from 8PM to 8AM will be interpreted as starting at 8PM and ending at 8AM the following day.

To save configuration changes to the SmartConnector, click **OK**.

Managing SmartConnector Filter Conditions

SmartConnector can function as a filtering tool between devices and the ArcSight Manager, using filtering conditions. Filtering conditions are set with a combination of AND or OR statements and data field values. Extraneous events are filtered out to minimize the number of events sent to the ArcSight Manager and analyzed in the ArcSight Console.

Creating SmartConnector Filters

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the Default | Filter tab, right-click and choose **Add new condition**.

- 4 In the Filter Condition dialog box, select a data field from the drop-down menu. (See [“Using Field Sets” on page 623](#) under [“Common Conditions Editor” on page 616](#), especially [“Condition Tree Command Buttons” on page 618](#) and [“Condition Tree Context Menu Commands” on page 619](#).)
- 5 Choose logic operators from the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

Adding SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the **Default: Filters** tab, right-click the **if** folder and choose **Add OR** condition to create an OR condition, or right-click the existing filter condition and choose **Add AND condition** to create an AND condition.
- 4 In the Filter Condition dialog box, choose a data field on the drop-down menu.
- 5 Choose logic operators on the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

Deleting SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector and choose **Configure**.
- 3 In the Filtering section on the Advanced tab, right-click a condition and choose **Delete condition**.

Setting Special Severity Levels

You can customize or conditionalize the event-severity levels reported by SmartConnectors. Customizing means pre-setting a given SmartConnector's filter to one specific severity level; conditionalizing is essentially the same, but with the addition of a filter condition to determine when the pre-set severity level is reported.

Setting a Custom Severity Level

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the appropriate SmartConnector and choose **Configure**.
- 3 In the Connector Configuration Editor, select the Connector: **Default: Filters** tab.
- 4 In the Filters tab, right-click the **Right-click to add an action** item and choose **Add severity action**. The filter shows SetSeverity Very-High.
- 5 Right-click the SetSeverity value and choose a different severity level from the **Set severity** to menu, if necessary.
- 6 Click **Apply** or **OK**.

Configuring a Conditional Severity

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the appropriate SmartConnector and choose **Configure**.
- 3 In the Connector Configuration Editor, select the **Connector: Default: Filters** tab.
- 4 In the Filters tab, right-click the **Right-click to add an action** item and choose **Add severity action**. The filter shows SetSeverity Very-High.
- 5 Right-click the **SetSeverity value** and choose a different severity level from the **Set severity** to menu, if necessary.
- 6 Right-click the SetSeverity value and choose **Add new condition**.
- 7 In the Filter Condition dialog box choose a field, a logical operator, and enter a value for the condition.
- 8 Click **OK** in the Filter Condition dialog box and **Apply** or **OK** in the Connector Configuration Editor.

For more information, see [“Managing SmartConnector Filter Conditions” on page 515](#).

Sending Model Mappings to SmartConnectors

Updates to network model mappings are sent automatically from the ArcSight Manager to SmartConnectors within heartbeat messages. The heartbeat messages themselves are sent on an interval which can be anywhere from every 5 seconds to every 10 minutes, but network model mappings are included in the messages only when there are updates to the model.



The interval on which information is exchanged between the Manager and SmartConnectors is determined by the Heartbeat Frequency setting on each Connector. (See information on [“Heartbeat Frequency” on page 503](#) in default content tab configuration fields under [“Selecting and Setting SmartConnector Parameters” on page 498](#).)

If you have made several configuration updates to the network model on the Manager and would like these changes to take effect immediately on the SmartConnectors without waiting for the next automatic refresh, you can use the following command to send the update information to a selected Connector.

Sending Model Mappings to a Connector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to update and choose **Send Model mappings now**.

This sends information about the current network model mappings from the Manager to the selected Connector. It will force a comprehensive refresh of the zone mappings and network model information on the Connector.

Sending Control Commands to SmartConnectors

From the Console you can issue basic event-flow-control commands to SmartConnectors, get the operational status of a SmartConnector, or issue control commands to network devices through their SmartConnectors. This topic discusses the first two points. To author

rule-driven device-command responses to events, please see [“Creating Rule Actions” on page 310](#).

Getting Status Reports

You can see a SmartConnector's current operational state at any time.

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command>Status>Get Status**.
- 3 In the Connector Status window you can see a readout of all the connector's current parameters.

Sending Flow-Control Commands

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command**, and one of the following menu options described below.
- 3 The Console's status bar shows a confirmation message when the flow control option takes effect.



- Commands available on this menu will vary depending on which SmartConnectors you are using. The standard set of commands is described here.
- Because there is no local cache, events that occur while a connector is stopped or paused are not retained.
- If a SmartConnector runs out of disk space, it can lose its ability to track events.
- The **Terminate** command should only be used in very special circumstances as it will **kill all** SmartConnector processes.
- See [“Creating Rule Actions” on page 310](#) for a description of the rule-based automated alternative for giving SmartConnector commands.

Flow Category	Command	Description
Status	Get Status	Provides a full report on the selected SmartConnector's current operational state.
	Get Device Status	Provides the status of the device that reports to the SmartConnector. (Currently only available for the CiscoIDS/IPS SmartConnector.)

Flow Category	Command	Description
Connector Process	Restart	<p>Restarts a running SmartConnector.</p> <p>Caution: Once a connector is terminated, Console commands cannot access it. Therefore, a "restart" works only on a connector that is currently running. Sending a restart command to a running connector will terminate and restart the connector.</p>
	Terminate	<p>Shuts down the SmartConnector and all processes the SmartConnector started.</p> <p>Caution: Once a connector is terminated, Console commands (including Connector Process > Restart) cannot access it. The connector must be restarted manually from the machine on which it is installed.</p>
Event Flow	Pause	<p>Stops the SmartConnector from sending events to the ArcSight Manager.</p> <p>Note: Events received from the target device will be saved in the connector cache (even though the connector is in Pause state).</p>
	Stop	<p>Stops the SmartConnector from sending events to the ArcSight Manager.</p> <p>Caution: A Stop command causes the SmartConnector to drop all events, including events stored in the connector cache.</p>
	Start	<p>Prompts the SmartConnector (previously in Stop or Pause state) to start sending events to the ArcSight Manager.</p>
Network	Flush Name Resolver Cache	<p>Clears cache for Network name resolver.</p>

Flow Category	Command	Description
Upgrade	Upgrade	<p>Launches a Command Parameters dialog for remote upgrade to newer versions of ArcSight SmartConnectors for managed assets.</p> <p>Provide the version number of the connector to which you want to upgrade and a wait time to verify that the upgrade completed successfully. (If the upgrade is not successful, the system performs an automatic rollback to the previous version of the connector.)</p> <p>Click OK to start the upgrade.</p> <p>See "Upgrading SmartConnectors" on page 529 for prerequisites for the upgrade process and detailed information on how to upgrade Connectors.</p>
	Rollback Upgrade	<p>Launches a Command Parameters dialog for remote rollback of connector version to a specified previous version. See "Upgrading SmartConnectors" on page 529 for complete information.</p>



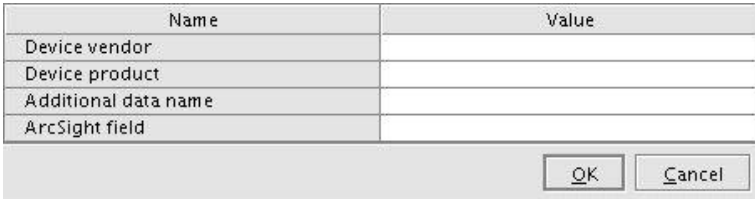
Tech Support commands are provided for use primarily by ArcSight Customer Support. Brief descriptions of these Tech Support commands are provided for informational purposes, but these commands are not intended for use by ArcSight customers except as instructed by ArcSight Customer Support.

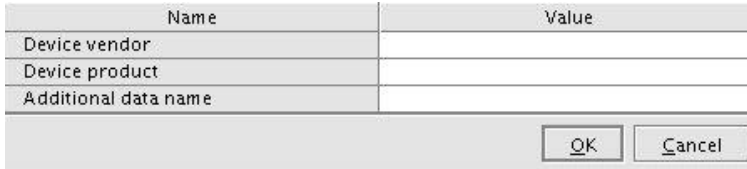
Flow Category	Command	Description
Tech Support	Get support info	Gets logs and other feedback on SmartConnectors.
	Get 'agent.properties'	Shows the list of properties for the selected SmartConnector.
	Get Upgrade Logs	Get upgrade logs on SmartConnectors.
	Get 'agent.wrapper.conf'	Shows the wrapper configuration for the selected SmartConnector.
	Get Configuration XML File	Shows the XML configuration file for the selected SmartConnector.
	Get Thread Dump	Gets one thread dump for the selected SmartConnector.

Flow Category	Command	Description
	Get Two Thread Dumps...	Gets two thread dumps for the selected SmartConnector spaced by the time interval specified. By comparing both thread dumps, ArcSight Customer Support can troubleshoot connectors with threads that are hanging for unknown reasons.
	Get last N lines of 'agent.log'...	Shows an excerpt from the connector log file based on the number of lines you specify. The default is 500 lines.
	Get system properties	Shows system properties for the selected connector, including details on variables such as Java runtime name, Java virtual machine (VM) version, operating system name, paths for various Java components, paths for ArcSight Home, user directories, user home, and so forth.
	Enable Event Flow Tracing...	Allows you to specify a component and fields to log for initiating an event flow trace. Component and field names must be provided per appropriate syntax. The component should be chosen from the components listed in the Get Status results.
	Disable Event Flow Tracing...	Disables event flow tracing on the selected component.
	Get Event Flow Tracing Log	When tracing is enabled on the selected connector, the connector logs data about events it receives.



The following commands provide access to SmartConnector component mapping and event categorization for advanced users.

Flow Category	Command	Description
Mapping	Get Additional Data Names	<p>Returns a list of additional data names seen for each device vendor/product combination since the connector started running. For example:</p> <pre>Additional Data Names Seen: Generic (no vendor/product): test1 [3 times] test11 test13 [2 times] Vendor/product [vend/prod]: test1 test10 [6 times]</pre> <p>By default, the command limits the list to show only the most recent 100 device vendor/product combinations and the most recent 100 names for each.</p> <p>Tip: You can change this limit by editing the SmartConnector property <code>agent.additionaldata.mapper.track.max.names</code> in the file <code>\$ARCSIGHT_HOME/ArcSightSmartAgents/current/user/agent/agent.properties</code> on the machine where the connector is installed. However, in most cases we recommend keeping the defaults. If you do change a property setting such as this, you will need to restart the connector.</p> <p>If a data name is not a string, its data type is displayed in the list. If the connector saw an additional data name more than once, the command output indicates the number of times the name was seen.</p>
	Map Additional Data Name...	Brings up a dialog where you can map an additional data name for the selected connector.
		

Flow Category	Command	Description
		<p>For a generic mapping, you can leave the Device vendor and Device product fields blank. For a specific mapping, fill in these fields with the appropriate vendor and product names.</p> <p>Typically, the Additional data name is one of the names shown in the Get Additional Data Names output (but can be another name not on that list).</p> <p>The ArcSight field must be a valid ArcSight event field.</p> <p>Click OK to create the mapping.</p> <p>Here is an example of the command output for a successful generic mapping:</p> <pre>Successfully mapped additional data name [test11] to event field [message] for vendor/product []</pre> <p>A successful device vendor/product-specific mapping returns output similar to this:</p> <pre>Successfully mapped additional data name [test10] to event field [message] for vendor/product [vend/prod]</pre> <p>If the additional data name has not been seen, the name is still mapped, but with a warning like this:</p> <pre>Successfully mapped additional data name [foo] to event field [deviceCustomString1] for vendor/product [vend/prod] (note that additional data name [foo] has not been seen for vendor/product [vend/prod])</pre> <p>If the ArcSight field is not valid, the error returned is similar to this:</p> <pre>Failed to map additional data name [bar] to event field [messages] for vendor/product [vend/prod] (event field [messages] is unknown)</pre>
	Unmap Additional Data Name...	Brings up a dialog where you can unmap an additional data name for the selected connector.
		

Flow Category	Command	Description
		<p>To remove a generic mapping, you can leave the Device vendor and Device product fields blank. To remove a specific mapping, fill in these fields with the appropriate vendor and product names. The additional data name should be one that was previously mapped for the specified device vendor and product combination.</p> <p>Click OK to unmap the data name.</p> <p>Here is an example of the command output for a successful generic unmapping:</p> <pre>Successfully unmapped additional data name [test11] for vendor/product []</pre> <p>A successful device vendor/product-specific unmapping returns output similar to this:</p> <pre>Successfully unmapped additional data name [foo] for vendor/product [vend/prod]</pre> <p>If the specified additional data name was not previously mapped, the output looks like this:</p> <pre>Failed to unmap additional data name [foo] for vendor/product [vend/prod] (not previously mapped)</pre> <p>Notes:</p> <ul style="list-style-type: none"> • One additional data name can be mapped to more than one ArcSight field for the same device vendor/product combination, and in this case unmapping it unmaps it from all ArcSight fields for that device vendor/product. This is an unlikely scenario, however. • The converse case, where multiple additional data names are mapped to the same ArcSight field for the same device vendor/product combination, results in the last mapping taking precedence over any previous mappings to that ArcSight field for that device vendor/product. No warning is generated in this case.

Flow Category	Command	Description
Categorizer/ mapper	Reload custom categorizations	<p>There are several ways to set event category information for events. The least common of these is to store custom categorization files (organized by vendor and product) on the connector machine in the <code>user/agent/aup/acp/categorizer/current</code> directory (or the <code>user/agent/acp/categorizer/current</code> directory).</p> <p>If such categorization files exist and have been changed, this command reloads them without restarting the connector.</p>
	Reload custom map files	<p>Rescans and reloads map files in <code>user/agent/map</code> directory on the machine where the connector is installed.</p> <p>The map files are named in the form <code>map.n.properties</code>, where <code>n</code> is a number starting with 0. Changes to these files will be seen periodically in any case, but you can use this command to immediately apply the latest changes. Not all connector setups include custom map files.</p> <p>Caution: Map files are created on some connector machines to fulfill specific needs. If you are not familiar with the categorizer/mapping setup of an environment, we recommend that you do not use these commands.</p>



This menu also provides options to test commands.

Managing SmartConnector Groups

You can best manage ArcSight SmartConnectors when you organize them into groups. You'll find all uncategorized SmartConnectors in the Unassigned group.

You can move or copy groups and SmartConnectors into other groups in the Connectors resource tree by using drag-and-drop. If a group is deleted, the SmartConnectors within that group are also deleted.

You should not delete a Connector resource at the ArcSight Console, unless the corresponding SmartConnector is first stopped. If the SmartConnector on the device is running and its Connector resource is deleted, the SmartConnector will no longer be able to send events to the ArcSight Manager, causing the SmartConnector to start caching events and eventually dropping these events.

Creating SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

Renaming SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Rename**.
- 3 In the "name" text field, rename the group.
- 4 Press **Enter**.

Editing SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Edit Group**.
- 3 In the Group Editor, edit the **Name** and **Description** text field.
- 4 Click **OK**.

Moving or Copying SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

Managing SmartConnector Resources

This topic describes how to do basic resource management for SmartConnectors.

Moving or Copying a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.

- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

Importing and Exporting SmartConnector Configurations

As a part of Managing SmartConnectors, you may want to share configurations among several instances of the same or a similar connector.

You can import and export SmartConnector configurations as a means of sharing custom configurations among several connectors on the same or multiple Managers. Rather than redefining a complex configuration on each connector, you can export the configuration as an XML file and then import it into connectors that share some or all of its configuration settings. An override feature allows you to make changes to any of the parameter values upon import.

Importing a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector into which you want to import a new configuration and choose **Import Connector Configuration...**

This brings up a file browser where you can select the file to import.

- 3 In the file browser, navigate to and select the [.xml](#) file that contains the connector configuration, and click **Open**.



SmartConnector configurations must be saved and imported as XML files.

This brings up a dialog showing original and proposed new configuration settings for the selected connector, with an option to override any of the proposed new values. (Click **Show** to show the details of the import or **Hide** to hide them.)

- On the Import Connector Configuration dialog, review the import information and override any values that you do not want to import.

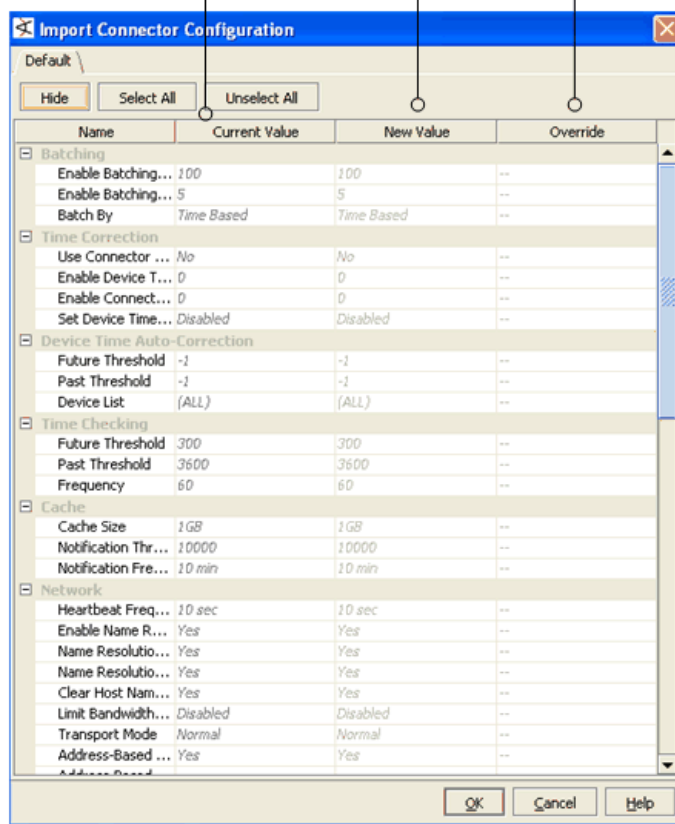
This dialog shows original values for the selected connector configuration and new values that will be applied upon import. You can override any of the settings you do

not want to import by either keeping the parameter value in the original configuration or defining a new value.

For example, you even can limit the import to only filters by keeping all values in the original configuration and choosing to override only the filter values with the imported values as is detailed in SmartConnector Filters. (Scroll down to the Filters section at the end of the Import dialog to see the filters.)

Before import, the Import Connector Configuration dialog shows current value, new value, and override option for each aspect of SmartConnector configuration.

You can accept all new values or override the import by keeping some of the original values.



- When you are satisfied with the settings to import and overrides (if any), click **OK** to import the configuration.

Exporting a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to export, and choose **Export Connector Configuration As...**

This brings up a file browser where you can navigate to the location where you want to save the configuration as an XML file.

- 3 In the file browser, navigate to and select the location where you want to save the configuration, provide a name for the file, and click **Save**.



SmartConnector configurations must be saved as XML files.

SmartConnector Filters

You can import and export only the filters associated with SmartConnectors as a part of an import or export on a SmartConnector.

- To export a SmartConnector filter, export the connector that uses the filter (as described in the previous topic on exporting a SmartConnector configuration).
- To import a SmartConnector filter into another connector, start by selecting in the Navigator the SmartConnector to which you want to add a new filter. Follow the steps to import the connector that includes the filter you want to import (as described in the topic on importing a SmartConnector configuration). On the Import Connector Configuration dialog, limit the import to only the filter(s) you want by keeping all values in the original configuration and choosing to override only the filter values with the import. (Scroll down to the Filters section at the end of the Import dialog to see the SmartConnector Filters.) When you have the new, imported filter values selected to override those in the original connector, complete the import by clicking **OK** on the Import Connector Configuration dialog. This adds the imported filter(s) to the original SmartConnector.

Upgrading SmartConnectors

ArcSight Enterprise Security Management (ESM) now provides the ability to not only centrally manage and configure SmartConnectors, but also to update them remotely. You can use the Upgrade command on the Console to upgrade to newer versions of ArcSight SmartConnector software for managed devices. (And you can use the Rollback command to revert to a previous version on an upgraded connector.)

The Upgrade command lets you launch, manage, and review the status of upgrades for all SmartConnectors. A fail-over mechanism launches SmartConnectors with previous versions if upgrades fail. All communication and upgrade processes between components (Console, Manager, connectors) take place over secure connections.

The ArcSight Console reflects current version information for all of your SmartConnectors.



For this release, SmartConnector remote upgrade is supported for connectors installed on Linux, Solaris, and Windows platforms only.

Overview of the Upgrade Process

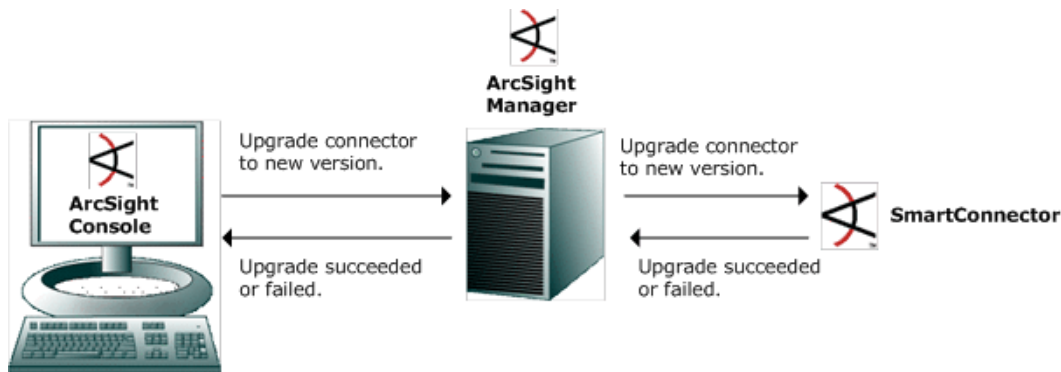
- 1 As an ArcSight customer, you will receive an e-mail notification about new connector releases from ArcSight support.
- 2 ArcSight administrators download the latest releases to the ArcSight Manager where they are available for SmartConnector upgrades.



SmartConnector "upgrade" version files are delivered as ArcSight Update packs (**.aup**) files. (ArcSight update packs are compressed file sets, similar to **.zips**.) The administrator copies the **.aup** file to ARCSIGHT_HOME/updates/ onto a running Arcsight Manager. The Manager automatically unzips the **.aup** file and copies its contents to ARCSIGHT_HOME/repository/.

- 3 From the ArcSight Console, administrators select connectors to be upgraded (one at a time) and launch the upgrade command for each of them.

- 4 Upon receipt of the upgrade command, the selected connectors upgrade themselves, restart, and send upgrade results (success or failure) back to the ArcSight Console through the ArcSight Manager.
 - ◆ If the upgrade is successful, the new connector starts and reports on successful upgrade status. (The upgraded connector runs in the same home directory as the old connector.)
 - ◆ If the upgraded connector fails to start, the original connector restarts automatically as a fail-over measure. (This is essentially an automatic rollback, and re-start).



Tips on Monitoring SmartConnector Upgrade Status

SmartConnectors automatically determine their upgrade status when they start.

- When a connector starts up, it determines whether it is upgraded.
- If so, it waits for a configurable time interval for events from the monitored device to be processed.
- If, after that time interval, events have been processed, the SmartConnector is deemed up and running. The Console indicates that the upgrade for that connector is a success and the newer connector version is reflected.



Notes on SmartConnector Upgrade Procedure

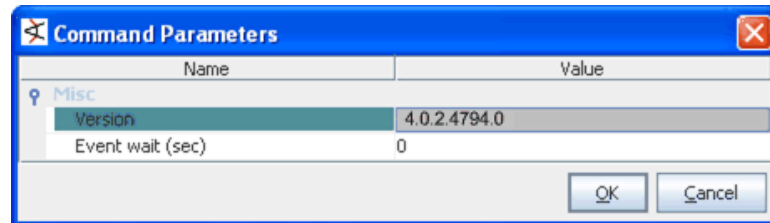
- When upgrading SmartConnectors, be sure to download current versions of the connector Configuration Guides from the ArcSight Customer Support Web site. New or revised information is provided in these guides as appropriate per each release of SmartConnectors. (To check version numbers on your current connectors, see [“Getting Status and Versions on Installed SmartConnectors”](#) on page 532.)
- You need administrative permissions to upgrade connectors.
- Newer versions of the connectors you want must be available on the Manager to which you are connected.
- The option for remote upgrade is available only in ArcSight ESM v.4.0 Console and only on SmartConnectors of version 4.0.2.xxxx.0 or newer. Earlier versions of Connectors (or Agents) must be upgraded manually as per the original process by installing a newer version of the connector.
- As a prerequisite to upgrading connectors, both the ArcSight Manager and the connector you want to upgrade must be running.

The **Upgrade** SmartConnectors command is available as one of several SmartConnector control commands.

Upgrading SmartConnectors

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Upgrade**.

This launches a Command Parameters dialog.



- 3 Provide the following information in the dialog.
 - **Version** - The Version field provides a drop-down menu showing the connector versions available on this Manager. Choose the Version number of the connector to which you want to upgrade.
 - **Event wait (sec)** - Number of seconds the upgrade process will wait for the first event from the device after the new, upgraded connector is started. If no events are received from the device within the specified time frame, the upgrade is considered "failed" and the old connector is launched.

This optional check is an additional safeguard against upgrade failures. For example, the connector binaries may have been upgraded successfully, but the new version may have problems communicating with the device. In that case, this check will assume that the upgrade failed and bring back the old connector.

If the **Event wait (sec)** value is **0** (the default), then the upgrade does not perform this check.

- 4 Click **OK** to close the dialog and start the upgrade.

As the upgrade proceeds, the connector will show as "down" and then "running" again in the resource tree. Status messages on the Console will indicate whether the upgrade succeeds or fails. You can check the logs for the connector to determine if the upgrade succeeded. (**Send Command > Tech Support > Get 'agent.properties' and Get Upgrade Logs.**)

Rolling back to a Previous Version



Notes on SmartConnector Rollback Procedure

- You need administrative permissions to roll back Connectors.
- The option for SmartConnector rollback is available only in ArcSight ESM v.4.0 Console and only on SmartConnectors of version 4.0.2.xxxx.0 or newer that have been previously upgraded.
- Rollback automatically reinstates the most recent version prior to the currently installed version. You cannot do a remote rollback on a connector to other than the previously installed version. (For example, if you start with a connector of version 4.0.2.4793, upgrade to 4.0.2.4794, then upgrade again to 4.0.2.4795, a remote rollback at this point will re-install/start connector version 4.0.2.4794. If you wanted to roll back to an earlier version, you would need to do this manually.)

You can roll back an upgraded connector to the previous version with the Rollback command.

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Rollback**.

As the rollback proceeds, the connector shows as "down" and then "running" again in the resource tree. You can check the logs for the connector to determine if the rollback succeeded. (**Send Command > Tech Support > Get 'agent.properties'** and **Get Upgrade Logs**.)

Troubleshooting

If an upgrade or rollback fails, you can review the related logs. Choose **Send Command > Tech Support > Get Upgrade Logs** from the ArcSight Console menus.

You can also use the Send Logs wizard to collect and send logs, including upgrade logs, to ArcSight for support help.

Getting Status and Versions on Installed SmartConnectors

Before or after you upgrade a SmartConnectors, you may want to check version numbers of currently installed connectors or get other status information. There are several ways to get information on currently installed connectors (including various control commands, channels, dashboards). Two of these are highlighted here as easy ways to get connector version information.

Getting Status on a SmartConnector

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Status > Get Status**.

The Status information on a connector includes "Agent Version" near the top of the message window. Here is an example snip-it of the Get Status command results for a Test Alert connector, Version 4.0.2.4793.0:

```
Status Generated: Wed Mar 07 13:20:09 PST 2007
Memory Usage: 65Mb out of 253Mb

Agent Content Version.....2007-03-01-09-02-05_4793
Agent Type.....testalertng
```



```

Agent Version.....4.0.2.4793.0
CommandResponses Processed.....1097
Current Max Rate.....22
Event rate LTC.....Wed Mar 07 13:18:42 PST 2007
Events Processed.....24003

```

SmartConnector Dashboards

Choose **Dashboards** from the Navigator panel, and expand the folders to find various dashboards. To view a dashboard, right-click it and choose **Show Dashboard**.

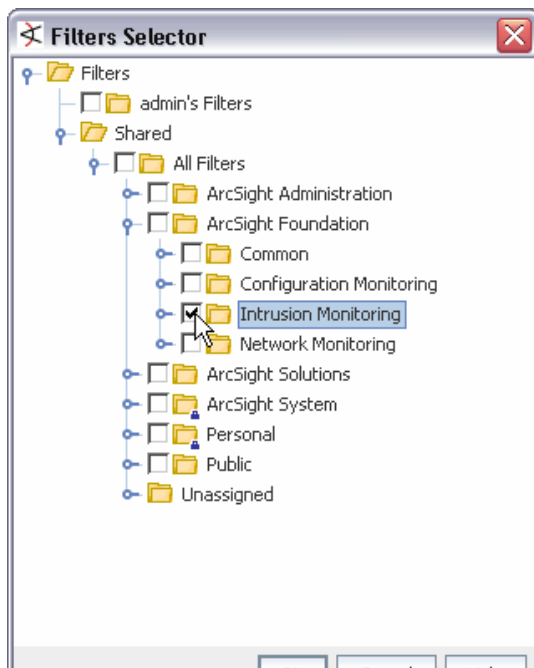
You can find some these SmartConnector dashboards in /Dashboards/Shared/All Dashboards/ArcSight Administration/Connector/:

- Connector and Device - Heads Up Display
- Connector Status

Selecting Resources

You often need to select resources to act on or use while authoring or configuring analysis tools. Selecting is often the first step in managing, authoring, or analyzing resources.

While the Navigator panel is your usual means of selecting resources, you can also encounter the Select Resources dialog box any time selection is a necessary part of some task, such as adding a case group to a rule action or adding user groups to access control lists (ACLs).



For resource groups, click to highlight and select the group you want to choose, then click **OK**. For options that allow multiple selections, select the check boxes next to individual entries in the list under a group, then click **OK**.

This dialog is also displayed for setting user permissions on resources and operations.

For information about setting permissions on resources, see [“Managing Permissions and Resources” on page 443](#).

For information about setting action permissions on who can deploy data monitors, see also [Step 4 on page 453](#) in “Controlling Who Has Permissions to Deploy Data Monitors” on page 452.



Finding Resources

Apart from visually navigating the resources in the Navigator panel, you can also find items in busy resource trees by searching or by locating them.

Searching for System Resources

The search capability uses conventional query elements to search the entire set of system resources, returning a ranked list of qualifying items. Each user sees only those resources for which they have permission, regardless of the query. You can search for a string in All Resources or within a particular resource with both of the following methods.

Search Field on Console Tool Bar

In the Search field  on the Console toolbar type a name or phrase and click the Find Resource button (). The Search hits are displayed in the Viewer. Single-click an item to display a preview of its definition in the Details pane on the Viewer, or double-click it to open its definition in an Editor in the Inspect/Edit panel.

To limit a search to a particular resource type, click the **drop-down menu** tab on the Search field and choose a resource type from the menus. Notice that some resource types have sub-types from which you can choose. If you limit the Search to a resource type, an icon representing the resource type you are searching on is displayed in the Search field (instead of the standard looking glass Search icon).

For example, to search for a name or phrase only in Trends, choose **Reports > Trends** from the Search drop-down, enter the search string, and click the **Find Resource** button.

The Search field in the toolbar accepts all the Query Options described below.

The screenshot shows the ArcSight Console 4.0.0.2190.0 interface. The top toolbar contains a search field with the text 'VPN Logins' and a magnifying glass icon. A callout bubble points to this field, stating: 'Type the name or phrase associated with the item you are searching for (you can include spaces in the Search string; e.g., VPN Logins) and click the Find Resource button.' Another callout bubble points to the search results in the 'Viewer' panel, stating: 'Search results are shown in the Viewer panel on a Find Resource tab. Single-click a found resource to get a Details preview of it. Double-click the item to open it in an Editor.' A third callout bubble points to the 'Reports' menu, stating: 'To limit the Search to items of a particular resources, click the Search drop-down button and select a resource type, then enter the Search string and click the Find Resource button. Note that some resource types have sub-types you can select; e.g., Reports > Trends.' The 'Viewer' panel shows a list of search results for 'VPN Logins', with the top result being 'VPN Logins' (Trend). The 'Details' panel shows the 'VPN Logins Outcome - Hourly' report.

As an alternative to using the quick Search field option, you can get a full Search panel in the Viewer:

- 1 Choose **Edit > Find Resource** in the Console's menus, or press **Ctrl+F**.
- 2 In the Viewer panel's Resource Search tab, enter a query string in the **Search query** line, set the number of results to allow, and click **Find**. See ["Query Options" on page 535](#).
- 3 When the search returns its results, click any item to see its details or click a result column heading to change the order.

When you click a resource listing in the **Details** panel, it shows you the various pieces of related system information that justified that item's ranking.

Query Options

Pose your queries using these conventions.

Query Elements	Descriptions	Examples
Full or partial strings	Phrases, words, or partial words.	"Attack Notification" notification notif

Query Elements	Descriptions	Examples
Wildcards	Question marks (?) for single-character substitutions and asterisks (*) for multi-character substitutions.	<code>attack??</code> (attacker, attacked) <code>notif*</code> (notify, notifier, notification)
Boolean Operators	Use AND and OR to join strings.	<code>attack AND suspicious AND high</code>
Fields	Resource field labels (grid view columns) followed by a colon, with the data expressed as plain strings, Boolean strings, quoted strings, or parenthetical expressions.	<code>type:datamonitor AND name:"event counts"</code> <code>name:"address space"</code> <code>name:(address+space)</code> <code>name:(+address space)</code>
Exclusion	Use NOT, the minus sign (-), and the exclamation point (!) to exclude strings.	<code>at???? - attack at???? NOT attack at???? AND !attack at???? AND !attack AND !type:zone</code>
Proximity	Extend data-field queries' scope with a proximity factor expressed as a numeral following a tilde (~). The numeral sets the maximum number of words allowed between the specified words in the resources found.	<code>name:("top events"~1)</code> (top attack events) <code>name:("top events"~2)</code> (top serious attack events)
Fuzzy	Broaden query results with a relative letter-substitution factor expressed as a decimal fraction following a tilde (~). The values 0.0 to 0.9 apply, with the higher values increasing the substitutions made in the string.	<code>name:mssp~0.2</code>

Result Columns

Click any column heading to toggle between descending and ascending order.

Column	Description
Score	Ranking of resources a query returns, based how frequently the search term appears in each resource.
Type	Top-level categorization of the resource, as shown on the Navigator panel.
Name	The full name of the individual resource.
URI	Full uniform resource identifier for the individual resource.

Locating Specific Resources

The resource trees in the Navigator panel are handy for finding and using the security assets available in your organization and provided by ArcSight. However, when you are working with a particular resource in an editor or grid view, locating that item's position in a heavily populated resource tree can be inconvenient.

You can use two right-click commands to instantly spot resource entries in the Navigator panel, from applicable grid view resource listings or resource editors.

- 1 In an entry in a resources grid view, or in the top tab of a resource editor, right-click and choose **Find <asset type> in Navigator**.
- 2 Look for the highlighted item in the Navigator panel's resource tree.

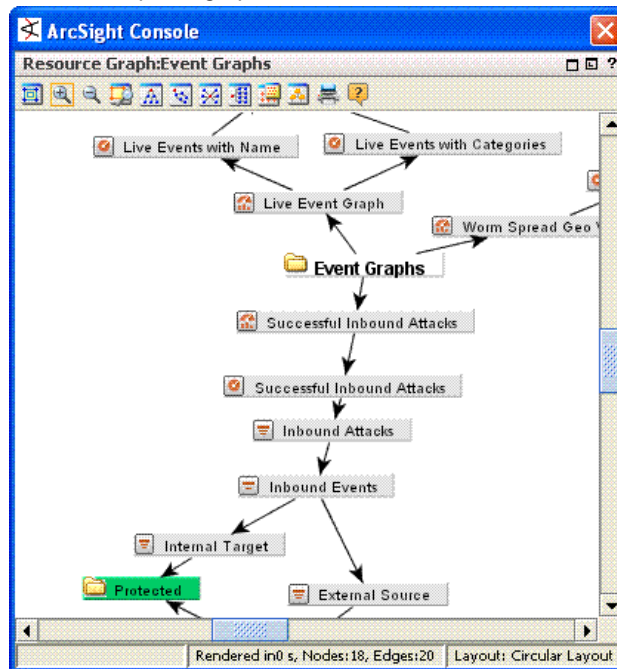
Visualizing Resources

The resources presented in the Navigator panel or graphically in the Viewer panel are organized into hierarchical groups for easy browsing. Among similar types of resources, there can be logical relationships. Graphs can make these relationships readily visible.

Graphing Resources

- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.











The Viewer panel graphs the resources in a new channel.





Using Graphs

Once generated, you can manipulate graphs further. There is a set of command buttons at the top of the view and a parallel set of commands available by right-clicking the graph itself.

Table 20-10 Resource Graph Buttons and Right-click Commands

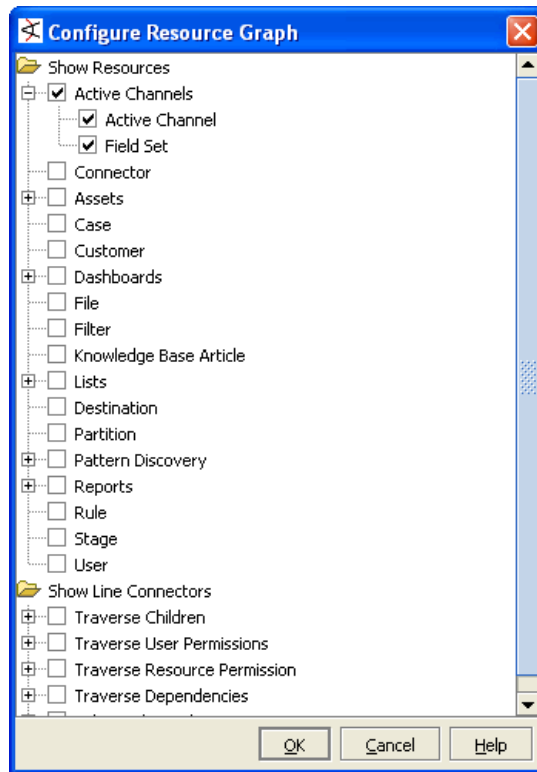
Command	Button	Description
Inspect		Opens a new event-monitoring channel, using the visualization's current timeframe, event and node filters.
Refresh		Updates the graph.
Fit Content		Sizes the graphic to the available display space.
Zoom In / Zoom Out		Increases or decreases the size of the displayed graphic.
Zoom Selected		Zooms in on a selected portion of a graphic.
Hierarchic Layout		Presents nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing event relationships that have a common root.
Organic Layout		Displays nodes in an arrangement based on minimum edge length, which tends to cluster nodes that relate to a common node. Likewise, node clusters with nodes in common will also tend to group together.
Circular Layout		Positions nodes in hub-and-spoke arrangements with each node radiating edges to, or receiving edges from, the nodes with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout instead.
Orthogonal Layout		Arranges nodes on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are very useful for clearly tracing connections and identifying node clusters.
Overview		Opens a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.
Hierarchy Tree		Opens a complete list of the nodes plotted in graphic layouts. Click a node in the list to scroll to that node in the main view.
Print		Prints the displayed graphic.
Export to JPEG		Create and save a JPEG-format copy of the current image.

Command	Button	Description
Add Graph View to Case		Adds the current graph view to a case you select. Choosing this option opens the Case Selector dialog, where you can browse cases. Select a case to which to add the current graph view and click OK on the Case Selector dialog. The graph view is added to the selected case as an attachment, accessible on the Attachments tab in the case editor for that case.
Help		Display the relevant ArcSight Console online Help topic.
Snapshot		Creates a new copy of the visualization itself. This graphic is not associated with a dashboard, even when starting from a dashboard viewer.
Snapshot Selection		Opens a new visualization that contains only the selected nodes and their connecting edges.

Configuring Resource Graphs

- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.
- 4 Hover cursor or click anywhere in the Viewer panel, and right-click **Configure Resource Graph** option on the context menu.

This brings up the Configure Resource Graph dialog where you can specify which resources to display in graph views.



- 5 Select resources to show or hide. (Click checkboxes to toggle show/hide options on resources. Resources with check marks are configured to show for the selected graph view.)
- 6 Click **OK** to save your changes.

For more information, see [“Selecting Resources” on page 533](#).

Viewing Resources in Grids

While the grids you see in the Viewer panel are most often views of events, these grids can also display organized sets of information about resources in the Navigator panel.

In the Navigator panel, certain resource groups include **Grid View** in their right-click context menus. This command causes the items in the group to display in a grid view, where you can review them using the sorting and column customization features that grid views offer. You can also right-click resource items in grid views and use the same context commands that those resources have in the Navigator panel.



Validating Resources

Resources can break or become invalid because they are improperly built or cannot find other resources they depend on. The following topics describe how to identify valid and invalid resources, show how to troubleshoot and fix broken resources, list requirements for valid resources, and provide tips for manual and automatic resource validation.

Valid and Invalid Resources

Valid resources show up in the Navigator with their associated icons as described in [“Navigating” on page 58](#).

A resource can “break” or become “invalid” either because it is constructed improperly (for example, when an active list schema does not match the underlying table) or because another resource it depends on is missing from the database (for example, when a rule references an unavailable filter). The latter can happen when a resource used in other resources is deleted from the Manager, or not retained during an upgrade, import, or export.

Invalid resources show up in the Navigator as broken or torn. For example, the Navigator displays a valid filter like this: , and an invalid filter like this: . An invalid resource also includes an “Invalid Reason” field under on the Attributes tab of its editor, as described in [Common Resource Attribute Fields under “Invalid Reason” on page 553](#).



A valid resource is fully available to other resources that reference it, and can participate in the event flow, trends, reports, data monitors, channels, filters, rules, and so forth.

An invalid resource cannot participate in the event flow or other resources in real time. For example, an invalid asset cannot participate in event asset resolution. Correlated events in which the source or target address points to the invalid asset are not generated. Similarly, an invalid rule does not trigger and generate correlation events.

Fixing and Validating Resources

When a resource becomes invalid, its Editor includes a **Validate** button that you can use to test and validate the resource after you fix it. Clicking the **Validate** button on a resource that was previously broken results in a check of the resource logic and dependencies. If the system determines the resource is now valid, the resource icon in the Navigator is updated to reflect a working resource. If the system determines the resource is still broken, it displays an error message describing the problem.

The general flow of steps to fix and validate a resource are:

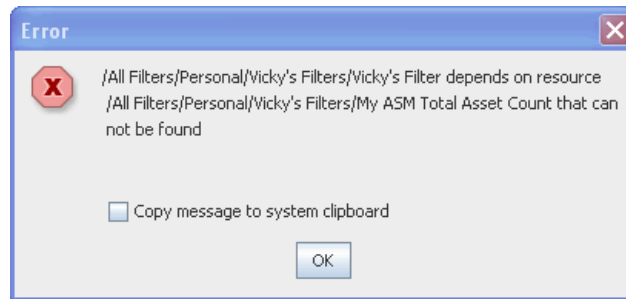
- 1 Identify an invalid resource. Sometimes problems with filters or rules (which are used in many other resources) are a result of broken resources. (A valid resource looks like this: , and an invalid resource looks like this: )

For example, if “My Top Threats” filter depends on “My Hotlist” filter, removing “My Hotlist” filter breaks “MY Top Threats” filter.

A scheduled job (like a scheduled rule group or archived report) can also break if one of the resources it depends on is missing. The broken icon for a scheduled job shows up on the Current Jobs list.

- 2 If you do not already know why a resource is broken, open its editor (double-click the resource in the Navigator panel) and click the **Validate** button in the resource editor.

This will give you an error message that describes the problem. The error dialog includes a Copy button for copying longer messages to an external editor.



- 3 Fix the problems with the resource. This may involve adding back in missing resources or rebuilding the resource to fit various other requirements as described in Troubleshooting Invalid Resources below.

To continue with our example, adding back in the filter "My Hotlist" would fix the problem we mentioned in step 1.

- 4 In the resource editor(s), click **Apply** to save changes to the resources you modified.



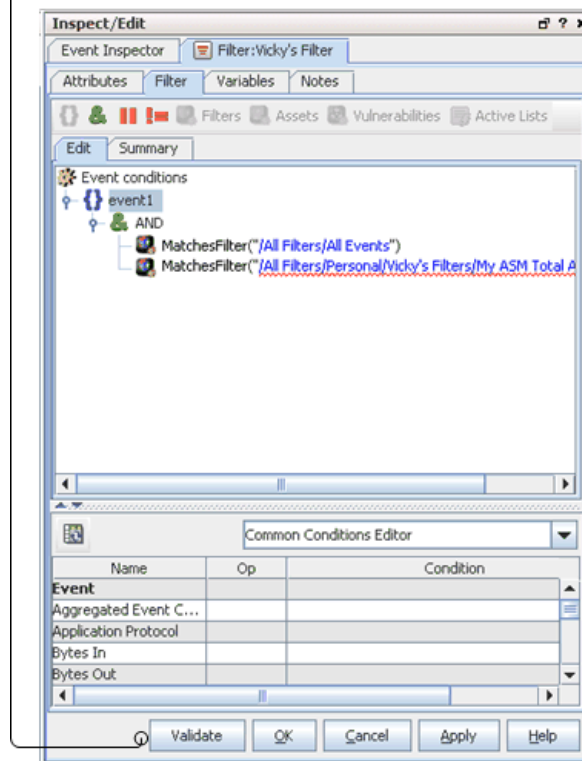
For problems that can be validated on the local client, you can click **Validate** before clicking **Apply** and if the resource is fixed its "working" icon is immediately reflected in the Navigator. However, for other types of problems; you need to **Apply** the changes to the resource before you **Validate** the resource. This is because some types changes must be processed on the Manager to determine dependencies and relationships to other data not available on the local client.

If you think you have fixed a resource but it is still not showing as fixed in the Navigator, make sure you **Apply** all the changes you made to it and then click **Validate** again.

- 5 In the resource editor for the resource that was broken, click **Validate**. If the resource passes validation, its icon in the Navigator updates to reflect a working resource.

In the resource Editor for the resource that was broken, click Validate button. If the resource passes validation, its icon in the Navigator updates to reflect a working resource. Otherwise, the broken icon remains and an error message describes the problems.

Some problems require saving fixes to the Manager, so be sure to click **Apply** and save changes to resources you fix before you click **Validate**.



To validate a scheduled job, click the **Open scheduled jobs list** tool button (🕒) to display scheduled jobs in the Viewer, right-click the job you want to validate, and choose **Validate** from the context menu. If the job passes validation, its icon in the Current Jobs list updates to reflect a valid task.

Troubleshooting (Requirements for Valid Resources)

The most common cause of an invalid resource is a dependency issue; another resource that the broken resource depends on is missing from the database. Some resources have additional requirements or limits that can also affect validity. Following is a summary of requirements for creating valid resources.

If any of these requirements are not met, the resource will break. To fix the resource, edit its definition to be in line with these requirements.

- All Resources - If the definition for a resource references another resource, the referenced resource must be available in the Manager database. This requirement is true for all types of resources.
- Devices and Assets - Each asset address must be unique within a zone, an asset can belong to one zone only, and the asset IP address must fall within the address range of its network zone.

- Device and Asset Ranges - Start addresses must be less than end addresses, asset ranges must be within the address range of the associated network zone, and asset ranges should not overlap another asset range in the same zone.
- Zones - Start addresses must be less than end addresses and network zones should not overlap other zones in the same network.
- Reports - Report templates cannot contain more than 20 charts or more than 15 tables.
- Active Lists - Active List schema must match the underlying table and must not include programming errors.

Resources become invalid when they violate one or more of their constraints. The following table lists the resources that can become invalid:

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Device/Asset	<ul style="list-style-type: none"> • Asset address must be unique within a zone • An asset only belongs to one zone • Asset IP address must fall in the address range of its network zone 	The invalid device/asset can not participate in the event asset resolution. Therefore, if an event has source/target address pointing to the invalid device it will not be resolved.
Device/Asset Range	<ul style="list-style-type: none"> • Start address must be less than end address • Asset range must be within the address range of its network zone • Asset range should not overlap another asset range in the same zone 	The invalid device/asset range can not participate in the event asset resolution. Therefore, if an event has its source/target address fall in an invalid device range its asset resolution will not be resolved.
Zone	<ul style="list-style-type: none"> • Start address must be less than end address • Network zone should not overlap other zones in the same network 	The assets falling within this invalid zone will get invalidated and can not participate in the event asset resolution.
Filter	Dependency constraint. For example, a filter may depend on other resources, like asset, active list, vulnerability etc.	The invalid filter will cause the resources that depend on it to get invalidated.
Rule	Dependency constraint. For example, a rule may depend on other resources, like filter, asset, vulnerability, active list, session list etc.	The invalid rule can not be triggered, so the corresponding correlation events will be missed.

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Data Monitor	Dependency constraint. For example, a data monitor may depend on other resources such as a filter	The invalid data monitor will stop fetching live data to feed the dash board.
Active Channel	Dependency constraint. For example, an active channel may depend on other resources such as a filter, or asset vulnerability	You will not be able to attach or open an invalid active channel
Report	Dependency constraint. For example, a report may depend on other resources, such as filter or asset, vulnerability and active list	The invalid report can not be run either manually from console or as a scheduled task.
Trend	Dependency constraint. For example, a trend that depends on a query will be invalid as soon as a query is changed	The invalid trend will stop generating any trend data.
Scheduled Task	Dependency constraint. For example, a scheduled task may depend on other resources, such as filter	The invalid scheduled task will not run.
Report Template	The report template cannot contain more than 20 charts or more than 15 tables	The invalid template will cause the reports that depend on it to become invalid.
Profile	Dependency constraint. The Profile depends on resources such as the filter it uses to determine which events to run discovery on. It also depends on the group where snapshots and patterns are saved. All these resource must exist and the creator should have appropriate permissions for them.	This resource will get invalidated and the scheduled runs may be skipped.
Active List	If the Active List schema does not match the underlying table etc, or due to some programming error.	The resources (Rules, reports etc.) that are dependent on the Active List get invalidated
Focused Report	Dependency constraint. For example, a focused report may depend on other resources, such as a report, filter or asset.	The invalid focused report can not be run either manually from the Console or as a scheduled task.

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Query	Dependency constraint. For example, a query may depend on other resources, such as a filter, asset, or active list.	The invalid query will cause the resources that depend on it, such as report and trend, to become invalid.

Automatic and Manual Validation

You can validate individual resource manually through the Console with the **Validate** button as described above.

Resource validation takes place automatically during an upgrade, package import or export, or when you insert or update a resource. (Administrators can use a stand-alone, command-line utility on the Manager machine for validating resources and generating validation reports on an off-line Manager. This is often useful after an upgrade.)

You can validate resources manually either through the Console (as described in [“Fixing and Validating Resources” on page 541](#)) or by running the following command from the `<ARCSIGHT_HOME>/bin` directory on the machine where your ArcSight Manager is installed:

```
arcsight resvalidate -persist [true|false] -excludeTypes <list of comma-delimited resource types>
```



The `resvalidate` is a standalone utility and runs as a batch process. We recommend that you run it only if need be (when there are many database updates that happen offline) after doing a product upgrade only. This utility should not be run while the Manager is running.

After you run this utility, you can find the `validationReport.html` report in the `<ARCSIGHT_HOME>` directory, which will list all the invalid resources.

Resource Validation During Upgrade

If the Manager detects a conflict during an upgrade or import process, it invalidates the conflicting resource, and continues with the upgrade or import process. The dependent resources for the conflicting resource will be automatically re-validated and disabled after the resource validation process completes.

After an upgrade process, a report called `validationReport.html` is generated in the `<ARCSIGHT_HOME>/upgrade/out/<time-stamp>` directory. After an import process, you can check the Console to make sure that you do not have any invalid resources. You are expected to fix the invalid resources manually. After you resolve the conflict, the dependent resources for the conflicting resource will be automatically re-validated again.

An invalid resource cannot participate in the event flow, trends, reports, data monitors, or channels in real time. For example, if an asset is marked invalid, it cannot participate in the event asset resolution. As a result, correlated events in which the source or target address points to the invalid asset are not generated. Similarly, when a rule is marked invalid, it does not trigger, therefore, the corresponding correlation events will not be generated.

Extending Audit Event Logging

Starting with ESM v.4.5, updates to existing resources are logged as audit events, as described in [“Resources \(Configuration Events Common to All Resources\)”](#) on page 594.

If you want to get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property on the ESM Manager to specify which resources should show extended audit event information.

To configure resources for more detailed update auditing, add a URI to the `resource.audit.update.uris` property in the `server.defaults.properties` file. For example:

```
resource.audit.update.uris=/All Users/
```

will turn on extended audit logging for all resources under the `/All Users/` subtree.

Leaving this property blank would turn this feature off (and show only default audit information).

To show detailed audit information for multiple resource types, list resource URIs separated by commas (no spaces). For example, to show extended update audit logging for users and system assets, set the property like this:

```
resource.audit.update.uris=/All Users/,/All Assets/ArcSight System Administration/
```

Extended information on the resource update is logged in two places.

- In the internal audit event generated for the resource update, `Device Custom String5` is set with the update information. The audit event information is shown in the `Device Custom String5` field in this format:

```
<UUID generated for this change>:<name of attribute>:<old value>:<new value>]+
```

- The update information is also written to a log file, `<ARCSIGHT_HOME>/logs/default/resource_update_audit.log` file. The audit event information is shown in the log in this format::

```
<UUID generated for this change>:<URI of resource>:<ID of resource>:<name of attribute>:<old value>:<new value>]+
```



- The “+” in the message format examples above is regular expression notation used to indicate that there can be one or more of `<name of attribute>:<old value>:<new value>` triplets shown in the audit event.
- Any “:” character in any attribute name or value is escaped with a backslash to “\:”.
- Any “\” character in any attribute name or value is escaped with a backslash to “\\”.

Managing Partitions

While the Partition Manager operates automatically, and follows the parameters set for it through the ArcSight Database Configuration Wizard during installation, you can use the Partition features of the Console to review activity and to change partitions’ active, inactive, or reactivated status.

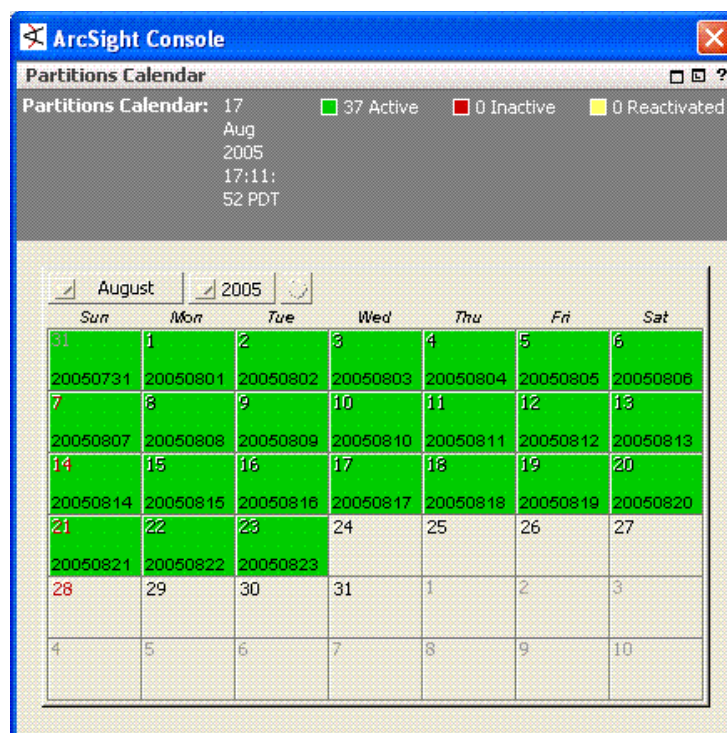
Getting Partition Information

- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a particular partition.
- 2 Choose **Partition Information**.
- 3 Review the partition's properties as displayed in the Partitions Editor, which are described below.

Seeing a Partition Schedule

Partition scheduling applies only to the **System Partitions>Active Partitions** branch of the resource tree. The Partitions Calendar graphically shows the partitioning schedule for a group in the Partitions resource tree. This view can help clarify relationships not readily visible in a resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a partition group.
- 2 Choose **Partitions Calendar**.
- 3 View the current schedule or click the **Month** or **Year** selectors to change the time period.



Archiving Partitions

Archiving a partition removes it from the database and compresses it for long-term storage. Although it may still be stored online, it is offline relative to the database until you reactivate it. Archiving applies only to the System Partitions>Active Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Archive Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to archive and click **OK**.

Reactivating Archived Partitions

Reactivating a partition restores it to the database, making it available to ArcSight features such as active channels and reports. Reactivation applies only to the System Partitions>Archived Partitions>Inactive Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Reactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

Reactivating Zipped or Large Archived Partitions

Although you can reactivate most partitions from the Console, follow the process below to reactivate these partitions if

- **Archive Type** was configured as **ZIP** when the partition was archived.
- the partition's **Data Size** field in the Partition Information section of the Partition Editor shows a value of **4000** or greater.

If these conditions are true, do the following:

- 1 Manually unzip the partition with an unzipping tool.
- 2 Ensure that the `arc_event_PartitionName` directory contains the files:
 - ◆ `arc_event_data_PartitionName.dmp`
 - ◆ `arc_event_data_PartitionName_01.dbf`

If either of these files is missing, the partition archive is invalid and cannot be reactivated. Contact ArcSight Customer Support for assistance.

- 3 On the database machine, enter this in `ARCSIGHT_HOME/bin` to get an SQL interface:

```
arcdbutil sql <username/password>@tnsname
```

- 4 At the SQL prompt, run this script to update the partition's status:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType
<partition_name>
```

Example:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType 20060101
```

- 5 Check the log `SetPartitionArchiveType.partition_name.log` to ensure that the script ran successfully. The log shows the before and after values for the row corresponding to the partition in the `ARC_PARTITION_SHADOW` table.
- 6 Reactivate the partition from the Console as described above.

Deactivating Archived Partitions

Deactivating takes a formerly reactivated partition back out of the database. Deactivation applies only to the **System Partitions>Archived Partitions>Reactivated Partitions** branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Deactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

Running Scheduled Tasks Right Away

You can manually start certain scheduled tasks to cause them to run immediately, rather than wait for the scheduled occurrence. Currently this option covers partition and archive maintenance tasks the system performs automatically.

- 1 Choose the **Partitions** resource tree in the Navigator panel.
- 2 Right-click in the panel and choose **Run scheduled task now**, then **Partition maintenance** or **Archive maintenance**.
- 3 Depending on the task, timing, and context, the system reports the degree of success or result of the command.

Partition Properties

Partition Property	Description
Name	The partition's name, usually by date.
Description	A description of the partition.
Lower Bound	The beginning timestamp for the partition.
Upper Bound	The ending timestamp for the partition.
Fully Valid	Indicates whether or not the partitions for all five tables that make up this logical partition checked as valid. These tables are individually validated in the Table Status section below.
Usable	Indicates whether the most important table, Events, is valid.
Active	Indicates whether the partition is accessible to the database (in contrast to "archived").
Archived	Indicates whether the partition has been removed from the database (in contrast to "active").
Event Count	The number of events recorded in the partition.
Data Size (MB)	The number of megabytes of disk space occupied by event data (not indexes).
Index Size (MB)	The number of megabytes of disk space occupied by indexes (not event data).
Index Type	Either default or custom.

Partition Property	Description
Table Status	These five items show the validity status of the partitions for the tables that make up the logical partition. This is summarized in the Fully Valid field above.

Managing Customers

The Customers resource tree, when populated, maps out the various external or internal customer accounts your enterprise tracks for cost, security analysis, or administrative reasons. These accounts, if present, are usually set up as part of the ArcSight deployment process. If the Customers resource tree is abbreviated or empty, your organization is probably not using this feature.

When the Customers resource tree is populated, you primarily use its branches as references in analysis filters that exclude or include certain customers.

Apart from analysis, the activities necessary to maintain the Customers resource tree include creating new customer references, editing existing references, and occasionally deleting references.

Creating Customers

When you create a customer, remember that the branch you add to the resource tree has to **match** the Customer URI attribute configured for that branch in the relevant SmartConnectors. In other words, you create customer-tracking resources only for those customers that have parallel URI values set in the SmartConnectors that monitor their devices.

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer group and choose **New Customer**.
- 3 In the Customer Editor, enter values for the properties that identify the customer. Note that the **Name** value has to complete the correct Customer URI for this account as found in its related SmartConnectors.
- 4 Click **Apply** to update the customer and leave the editor open, or OK to complete editing and close the editor.

Editing Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Edit Customer**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the customer and leave the editor open, or **OK** to complete editing and close the editor.

Deleting Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Delete Customer**.
- 3 Click **Yes** to confirm the deletion.

Saving Copies of Read-Only Resources

Although you may be limited to read-only access to certain resources in the Navigator panel, you do have the option to save a copy of such a resource to your own group where you do have write access.

Click the **Save As** button to make a copy of the resource and save it in a specified group.

In the resource group selector dialog, displayed when you click **Save As** in the editor for a read-only resource:

- 1 Select the group in which you want to save a copy of the resource.
- 2 Specify the name you want to assign to your copy of the resource.
- 3 Click **OK**.

The resource copy appears in the resource tree. You have write permission with this copy of the resource.

The Connectors, Users, and Notification editors do not support **Save As** functionality. In these editors, you will see the **OK/Cancel/Apply** buttons, but the fields for those resources are read-only.

Using the Image Editor

Please contact ArcSight Professional Services for assistance with using this feature.


Common Resource Attribute Fields

The following fields are common to several types of resources. You can find these fields in the resource editor Attributes tabs for the resources in Common, Assign, Parent Groups, Creation Information, and Last Update Information sections. (See also, [“Resource Attributes” on page 749.](#))

Common

Entering data in the **Common** section is optional, depending your environment setup.

Field	Description
Resource ID	Read-only field that shows the ArcSight ESM system resource ID.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight ESM. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your ArcSight ESM administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight ESM. A given alias will appear in place of the resource's name everywhere it may be seen. Your ESM administrator can advise you on the correct values for this field, if applicable. If you use an alternate event naming scheme in your environment, enter an alias for this resource here.

Field	Description
Invalid Reason	<p>If a resource is broken or invalid, an "Invalid Reason" field is included in its Attributes table. An abbreviated explanation is shown in this field. (See also, "Validating Resources" on page 540.)</p> <p>Click the browse button  at the end of this field to get a popup dialog that shows the full text of the explanation.</p>
Description	<p>Description of the resource.</p> <p>You can use this field to communicate the purpose of this resource to other users. For example, if this is a resource that leverages or depends on another resource (e.g., a query viewer or trend that uses an SQL query), this is a good place to make note of that relationship.</p>
Version ID	The globally unique version ID for this resource.
Deprecated	Toggle to indicate whether the resource is current or deprecated (obsolete).

Assign

Field	Description
Owner	A user selected from the Users resource tree who should be notified about this resource.
Notification Groups	The user groups selected from the Users resource tree who should be notified about this resource.

Parent Groups

Field	Description
Parent Group	Read-only field that shows the name and path to parent group of this resource.

Creation Information

Field	Description
Created By	Read-only field that shows the user who created this resource.
Creation Time	Read-only field that shows the date/time when this resource was created.
Time Since Creation	Read-only field that shows the time elapsed since this resource was created. This value is calculated from Creation Time.

Last Update Information

Field	Description
Last Updated By	Read-only field that shows the user who last updated the resource.
Last Update Time	Read-only field that shows the date/time when this resource was last updated.
Time Since Last Update	Read-only field that shows time elapsed since last update. This value is calculated from Last Update Time.

Personalizing the Console

The ArcSight Console has displays and settings that you use to monitor an enterprise using various windows, panels, views, controls, and tool bars. You can change these displays and settings based on your monitoring needs.

[“Changing the Console Display” on page 555](#)

[“Changing User Preferences” on page 556](#)

[“Saving and Sending Settings” on page 569](#)

Changing the Console Display

You can change the look and feel of the Console to better display information, focus on particular panels, or hide information not of interest. You can resize the Console, float or dock Console panels, apply translucency to a floating panel, and show or hide the menu bars, tool bars, and various displays.

Resizing the Console


To expand the Console to the whole screen, click the **Maximize** icon at the top-right corner of the window. To collapse the Console, click the **Minimize** button or drag the corners of the Console to resize it.

You can also drag and drop any dividers between panels to resize them.


Showing or Hiding Menu Bars and Tools

You can show or hide the Console menu bar, and all the other individual components of the Console interface (apart from the main panels). Right-click the **Menu bar** area of the Console and use the context menu to enable (check) or disable (clear) each component.


Showing or Hiding the Status Bar

Click the **Status Bar** button () on the toolbar, or on the Window menu, choose **Status Bar**.


Showing or Hiding the Navigator Panel

Click the **Navigator** button () on the toolbar, or on the Window menu, choose **Navigator Panel**.


Showing or Hiding the Viewer Panel

Click the **Viewer** button () on the toolbar, or on the Window menu, choose **Viewer Panel**.

Showing or Hiding the Inspect/Edit Panel

Click the **Inspector** button () on the toolbar, or on the Window menu, choose **Inspect/Edit Panel**.

Floating a Console Panel

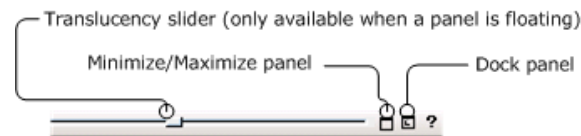
Click the **Float/Dock** button () on the panel header, or right-click the panel header and choose **Float Panel**.

Applying Translucency to a Console Panel


Move the **Translucency** slider on the panel header.




A panel must be floating before you can apply translucency to it. You cannot apply translucency to docked panels.



Docking a Console Panel

Click the **Float/Dock** button () on the panel header, or right-click the panel header and choose **Dock Panel**.

Closing a Console Panel

Click the **Close** button () on the panel header, or right-click the panel header and choose **Close Panel**.

Changing User Preferences

You can change several ArcSight Console characteristics to suit your security needs, working style, or personal preferences. You reach the Preferences dialog box through the **Edit>Preferences** menu command.

The display on the Preferences dialog changes depending on which Preference button you select.

Changing Your Password

A temporary password is created for you during your first ArcSight session. When you first log in, you should change to a permanent or more personal password. After changing it, be sure to keep it confidential.



You can change your password only if your ArcSight installation is configured to use built-in password authentication. Contact your system administrator for instructions on how to change passwords on ArcSight systems that use RADIUS SecurID or SSL authentication.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Password**.
- 3 Enter your old password, new password, and confirm the new password.
- 4 Click **OK**.

By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. Ask your system administrator about any special requirements for your site.

Changing Other Users' Passwords

Administrators may also reset user passwords; for example, if a user's original password has been compromised or you want to make users update their passwords. For information on how to do this, see [Resetting User Passwords](#) in “Managing Resources (for Administrators)” on page 437.

Setting Program Preferences

You can set the default editors and viewers to use for text, HTML, and packet payloads. For example, you'll use the HTML editor when editing the Knowledge Base and the Web browser for reports.



Program Preference	Value
Preferred Text/HTML Editor	Type the complete path to your preferred text or HTML editor or click the Browse button to locate one.
Preferred Web Browser	You can choose to use your preferred external web browser for all HTML display functions (e.g., reports, documentation indexes) or to use the Console's built-in web viewer, which is Microsoft Internet Explorer by default, for all but exceptionally large, numerous, or insecure HTML files. To use the internal viewer as your primary display, select Use the web browser embedded in ArcSight Console . The external web browser always needs to be specified. Type the complete path or click Browse to locate one. Note that you can use Internet Explorer or Netscape 6.0 or later, or Firefox 1.0.
Preferred Payload Viewer	Type the complete path to your preferred packet-payload viewer or click the Browse button to locate one.
Text to PCAP Converter	Type the complete path to your preferred packet-payload PCAP converter or click the Browse button to locate one.

Changing Global Options Like Panel and Editor Characteristics

You can make the Inspect/Edit panel open as a docked window inside, or as a floating window outside, the Console. You can do the same with all child windows as a class. You can also choose how informational and error messages are displayed from the Console.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Global Options**.
- 3 Select the check boxes next to options you want to enable.
- 4 Click **OK**.

Table 21-1 Global Options

Option	Description
Font	<p>Set global preference for font face, size, and style used throughout the Console, except on windows or views where you can set fonts specific to those Console elements. (For example, you can set fonts specific to Grid views as detailed in the next topic.)</p> <p>Click into the Font field to get the drop-down menu arrow.</p>  <p>Click the arrow to bring up the Fonts dialog. Set the Font, Size and Style.</p>
Launch editors in a floating window	Open all editors in a floating window. If deselected, all editors appear in the Inspect/Edit panel. If you select this option, you can still float or dock the windows.
Allow multiple editors of the same type	Permit more than one resource editor to be opened simultaneously for a given resource type (e.g., opening three instances of the Filter Editor at once). Enabling this option is very useful for analysts and persons implementing security solutions, but may inappropriate for operators or other persons who should have less-extensive editing access.
Show error messages in a pop-up dialog	Display all errors in a pop-up dialog.
Show informational messages in a pop-up dialog	Display all information messages in a pop-up dialog.
Create independent floating windows	<p>Independently float new windows that are children of another window such as the Viewer panel. This is the default. When enabled, you can choose a window's name from the list at the</p> <p>Window>Floating command, or toolbar button (), to bring it forward.</p>
Auto Relogin	Automatically log in again after logging out of the Console.
Use system defaults for dashboard background	When this option is selected, your system defaults are used for all Dashboard backgrounds.


Option	Description
Launch Help in external Web browser	<p>When this option is de-selected, the ESM Console Online Help is displayed in an embedded Web browser. This is the default.</p> <p>Launch Help in external web browser <input type="checkbox"/></p> <p>When this option is de-selected, the Online Help is displayed in your default Web browser (not embedded).</p> <p>You can access ESM Console Online Help from the Help menu on the Console, right-click Help options on the Navigator and Grid displays, Help buttons on dialogs, and so on. For more about the Help, see "About this Guide" on page xxxv.</p> <p>Note: The ArcSight Console uses Web browsers to display various charts, graphs, reports, and data monitor output (not just Online Help). On Windows systems, the Console defaults to using Internet Explorer Web browser even if you have a different browser set as your personal default browser. So if you enable "Launch Help on web browser" and want the Help to launch in a browser other than IE, also re-set the Console preference for its "External Browser". On Preferences dialog, click Programs for "External Browser" preference setting. (See also "Setting Program Preferences" on page 557.)</p>
Set Help dialog size (Width,Height)	<p>The Help display window defaults to width of 910 x length of 650 pixels.</p> <p>Set Help dialog size (Width,Height) <input type="text" value="910,650"/></p> <p>You can specify a different default Help window display size here. To do this, enter a new window size (for example: 750,900) and hit keyboard Enter or Return.</p> <p>Note: You need to hit keyboard Enter or Return after entering the new display size, and then <i>also</i> click Apply or OK to save all preference settings. If you do not hit Enter or Return, the new window size setting will not be saved even if you click Apply or OK.</p>

Setting Grid View Options

You can change several characteristics of the Viewer panel's grid views.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Grid View Options**.
- 3 Select the check boxes of the options you want to enable.
- 4 Click **Apply** to put your changes into effect and leave the Preferences dialog box open, or **OK** to save your changes and close the dialog box.

Table 21-2 Grid View Options

Option	Description
Font	<p>Set global preference for font face, size, and style used in Grid views.</p> <p>Click into the Font field to get the drop-down menu arrow.</p>  <p>Click the arrow to bring up the Fonts dialog. Set the Font, Size and Style.</p>
Color text by priority in grid	<p>Apply distinguishing colors to the event rows in Viewer panel grid displays, based on their threat-priority levels. Note that this option can be overridden by the Color text by filter in grid option if conflicts occur. When these options are not selected, the text in grid rows defaults to black.</p>
Color text by filter in grid	<p>Apply distinguishing colors to the event rows in Viewer panel grid displays, based on the filters that selected them. You set these colors through the Configure button, described below. Note that this option, when selected, overrides the Color text by priority in grid option if conflicts occur. When these options are not selected, the text in grid rows defaults to black.</p>
Pause the current channel on event selection	<p>By default, selecting an event pauses the event flow to avoid scrolling. Clear this check box to allow the flow to continue regardless of a selection.</p>
Do not prompt on verifying rule channel's timestamp change	<p>Toggles on or off the option to have the system generate a prompt when the timestamp changes on an active channel populated by correlation events.</p>
Do not prompt on channel restart	<p>Toggles on or off the option to have the system generate a prompt when an active channel is restarted.</p>
Check available database partitions on Active Channel start	<p>When selected, this option causes the ArcSight Manager to recheck the status of available database partitions before starting an active channel. This does have a performance effect and is used only for certain forensic purposes.</p>
Filter Coloring Preferences	<p>Click Configure to assign identifying colors to as many as five filters in the Configure Filter Colors dialog box.</p>
Print Column Flip Limit	<p>Determines the print format for Grid Views (channels, lists, and so forth). Grid views with the same or fewer columns than the Column Flip Limit print as a table, the same as is shown in the UI on the Console grid view. Grid views with the more columns than the Column Flip Limit print details per row rather in a normal table like that shown on the Console grid view.</p> <p>The default setting for Column Flip Limit is "10" columns. (Tables with more than 10 columns will print details per row.)</p> <p>See also "Printing from the Console" on page 83.</p>

Setting Date and Time Formats

Use the Date/Time option to choose a formatting style for the date and time strings displayed throughout the Console. You can also customize the details of any style you pick.

- 1 On the Edit menu, choose **Preferences**.

- 2 In the Preferences dialog, click **Date & Time**.
- 3 Click the **Formats** buttons and choose a date/time style from the lists for **Date & Time** Format and **Short Date & Time** Format options. Select **Express all times as GMT** to universally show time values in GMT rather than local times.
- 4 Click **Apply** to put your changes into effect and leave the Preferences dialog box open, or **OK** to save your changes and close the dialog box.

If you wish, you can customize the selected format. Edit the **Format** string using the Java-style date options described in the **Format Help** window, and the information in Timestamp Variables.

Configuring Event Graphs

You can modify the way graphs plot events, choosing to keep the source-event-target visual relationships compact, or to emphasize unique sources, targets, or both in order to more easily clarify the nature of attacks or situations.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Event Graph**.
- 3 Click the **Value** fields of the graph attributes to choose appropriate options, as described below.
- 4 Click **OK**.

Latitude and Longitude Options

Set the Latitude and Longitude preferences here . . .

Latitude & Longitude Entry Format

☒ DMS: Degree Minute Second (-49°30'00")

☐ DM: Degree Minute (-49°30.0')

☐ DD: Decimal Degree (-49.5000°)

☒ Show compass direction (49.5000° S).

. . . to control which measurement entry format is used for **Asset Locations** descriptions in the Assets Location Editor. (Choose **Assets** in the Navigator, click **Locations**, and edit or create new location to bring up the **Location Editor**.)

Inspect/Edit

Location Editor

Attributes Notes

Location

* Name

Latitude 0° 0' 0" N

Longitude 0° 0' 0" W

City

Region Code

Postal Code

Country N/A

(See "Location Editor" on page 471. This is a part of [Working with Locations, Zones, Networks, Vulnerabilities, and Categories](#) in [Modeling Your Network and Managing Assets](#).)

The options for latitude and longitude format vary from more exact to less so. Latitude and longitude can be shown in degrees, minutes, and seconds; degrees and minutes; or decimal degrees only. Additionally, an indicator of compass direction for the specified location can be shown or hidden in the editor.

Event Graph Options

- **Show Event Nodes:** Choose a basis for visually expanding or aggregating event nodes, relative to their source and target node instances.

Choice	Description
Once per common event	Graph only one instance of a given event node, regardless of the number of unique sources and targets that have it in common. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there may be visual instances for each source and target, but only one of the event node.
Once per unique source	Graph one instance of a given event node per unique source, regardless of the commonality of associated targets. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there will be two visual instances of the event in support of the two distinct sources.
Once per unique target	Graph one instance of a given event node per unique target, regardless of the commonality of associated sources. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there will be three visual instances of the event in support of the three distinct targets.
Once per unique source-target pair	Graph one instance of a given event node per unique source-target pair, regardless of the commonality of the events involved. For example, if sources 1 and 2 are directing a given event at targets 1, 2, and 3; and as a chain, targets 1, 2, and 3 are sourcing the same events on to targets 4, 5, and 6; then there are six visual instances of the event in support of six distinct targets.

- **Show Source/Target IP Addresses as:** In cases where one source-event-target chains to another, you can choose to graph a source/target IP address as a single node, or to graph both the source and target instances of such an IP address.

Choice	Description
Distinct nodes	Visually plot both the source and target instances of a chained IP address.
Simple nodes	Visually plot a single node for an IP address that represents both source and target.

- **Source Node Identifier:** Choose a different event attribute to use as the identifier for source nodes. The default attribute is Source Address. Note that while all attributes are available, not all are appropriate choices for this purpose.
- **Event Node Identifier:** Choose a different event attribute to use as the identifier for event nodes. The default attribute is **ArcSight Category**. Note that while all attributes are available, not all are appropriate choices for this purpose.

- **Target Node Identifier:** Choose a different event attribute to use as the identifier for target nodes. The default attribute is **Target Address**. Note that while all attributes are available, not all are appropriate choices for this purpose.

Setting Notification Popups

You can manage received notifications from within the Console. In the Preferences dialog box, you can set a severity threshold for notification popups and optionally play a sound when notifications arrive.

For **Severity threshold for notification popup**, raise or lower the integer value to a priority value that is appropriate for the level at which you want to be alerted.

Select **Play a sound when a notification message is received** to also emit a sound when the alert threshold is met.

Managing Hot Keys

The ESM Console provides schemas for configuring keyboard shortcuts to common actions. These schemas come with the Console:

- \$default
- Schemas for users (such as **admin** and other users)



- Schemas for users other than admin are listed only for users who have set up custom shortcuts on this Console under their login.
 - Custom shortcuts are available locally only. (See [“Sharing Custom Shortcut Schemas” on page 569](#) for more information.)
-

Schemas for users are all based on the \$default schema. That is, user schemas inherit all \$default schema shortcuts. The \$default schema.

On the Edit > Preferences > Manage Hot Keys dialog, under “Available shortcut schemas”, the schema currently in use shows as “**(active)**” next to its name.

You can define a keyboard shortcut for each command listed. Each command can have a different (or the same) keyboard shortcut depending on which schema is selected.

Keyboard shortcuts are pre-defined for common commands. For example, the pre-defined keyboard shortcut for the Select All command (`edit.selectAll`) is Ctrl+A.

Commands shown in red on Preferences dialog are not editable (e.g., `edit.delete`, `edit.redo`, `edit.cut`, `edit.copy`, `edit.paste`, and so forth). The flyover tooltips on these commands also indicates they are not editable.

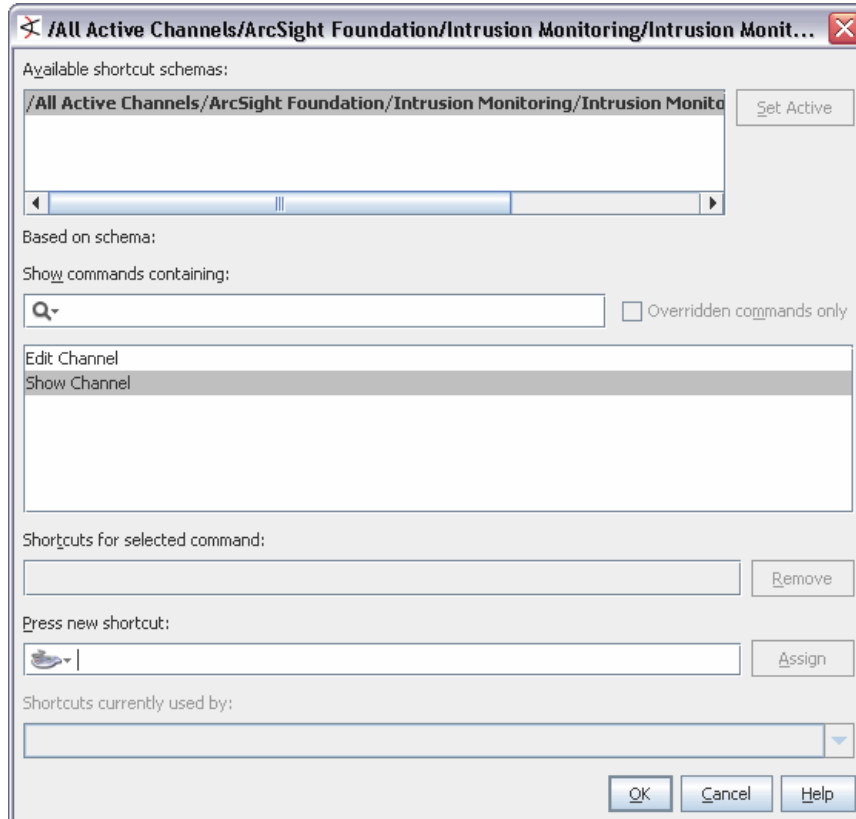
There are many commands listed for which no shortcut is provided (e.g., `file.new.Report`, `file.new.Rule`, `navigator.reports`, `navigator.queryViewers`, etc.)

Adding Shortcuts for Frequently Used Resources


This first task is not initiated on the Edit > Preferences dialog, but rather from various resource contexts in the ESM Console. But the results of setting up Hot Keys on selected resources are shown on the Edit > Preferences > Managing Hot Keys dialog, as described below.

To add a shortcut to a resource:

- 1 Navigate to and select the resource for which you want to add a shortcut.
(For example, choose **Active Channels** in the Navigator, and select an active channel such as [/All Active Channels/ArcSight Foundation/Intrusion Monitoring/Intrusion Monitoring - Significant Events](#).)
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.



- 3 Select the action you want to take with regard to the resource (e.g., Edit or Show).
- 4 In the **Press new shortcut** field:

- ◆ Optionally, press the button () to get a drop-down menu where you can set the type of shortcut to add (mouse, tab, etc.) and limits on keystrokes. (For example, if you want to set the shortcut on this channel to Ctrl+C+H, this requires first changing the keystroke limit from the default of 1, to 2 keystrokes.)
- ◆ Type the keyboard sequence you want to associate with the command.

If there the keyboard sequence you typed is not in use, a light gray “no conflicts” message is shown in the “Shortcuts currently used by” field. (For example, if you select [navigator.rules](#), place the cursor in the “Press new shortcut field”, and type Ctrl+Alt+X, you will get the “no conflicts” message.)

If you type a sequence that is already used by another shortcut, you get a message in the “Shortcuts currently used by” field telling you which resource is currently using the shortcut. (For example, the default shortcut for [navigator.rules](#) is Ctrl+Alt+L. If you type Ctrl+Alt+R in the “Press new

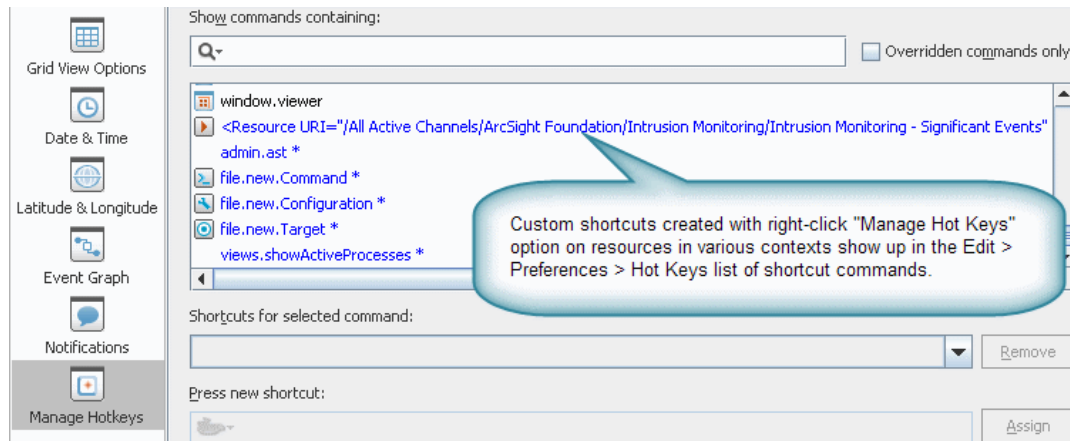
shortcut" field, you get a message noting that this sequence is already in use for `navigator.reports`.)

If you continue with the assignment, you get a prompt asking whether you want to remove the shortcut from the other resource and add it to this new one.

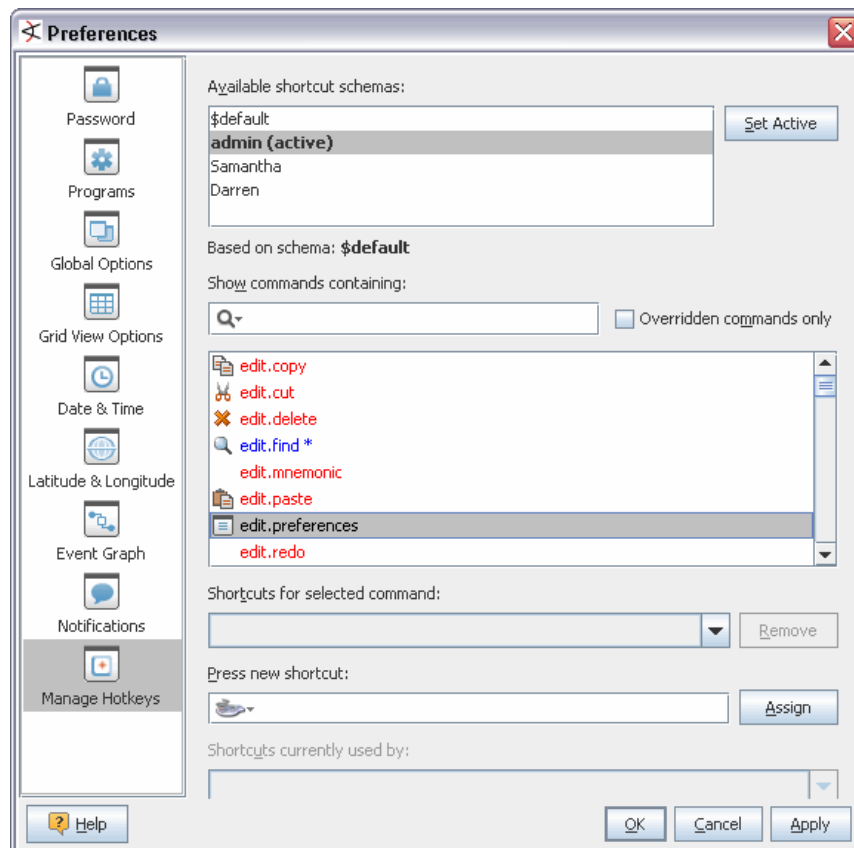
5 Click **Assign** to associate the shortcut with the resource.

6 Click **OK** to save your changes and close the dialog.

Custom shortcuts added to resources are listed on the **Edit > Preferences > Managing Hot Keys** dialog.



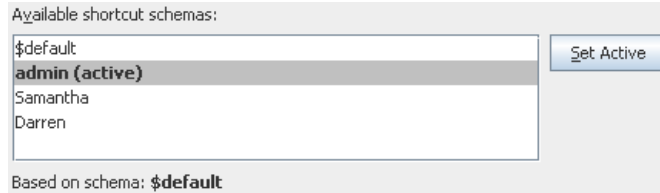
Modifying a Custom Shortcut



To modify a custom shortcut:

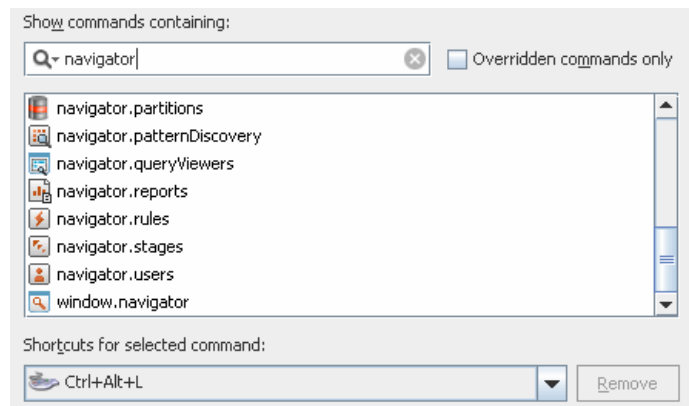
- 1 Select the schema in which you want to modify shortcuts for commands.

In this example, the **admin** schema is selected. Note, however, that the schema selected for modifying a hot key need not be the “active” schema; as it happens to be in this example.




- 2 Select the command for which you want to modify the hot key(s).

You can filter for commands containing a given string (e.g., “navigator” to find all navigator commands).



- 3 In the **Press new shortcut** field:

- ◆ Optionally, press the button () to get a drop-down menu where you can set the type of shortcut to add (mouse, tab, etc.) and limits on keystrokes. (The default keystroke limit is one. If you set it to 2 or 3, you have more combinations of keystrokes available to use for custom settings.)

- ◆ Type the keyboard sequence you want to associate with the command.

If there the keyboard sequence you typed is not in use, a light gray “no conflicts” message is shown in the “Shortcuts currently used by” field. (For example, if you select `navigator.rules`, place the cursor in the “Press new shortcut field”, and type `Ctrl+Alt+X`, you will get the “no conflicts” message.)

If you type a sequence that is already used by another shortcut, you get a message in the “Shortcuts currently used by” field telling you which resource is currently using the shortcut. (For example, the default shortcut for `navigator.rules` is `Ctrl+Alt+L`. If you type `Ctrl+Alt+R` in the “Press new shortcut” field, you get a message noting that this sequence is already in use for `navigator.reports`.)

If you continue with the assignment, you get a prompt asking whether you want to remove the shortcut from the other resource and add it to this new one.

- 4 Click **Assign** to apply the new shortcut to the command.



An asterisk is displayed next to commands for which the pre-defined shortcuts have been modified or overwritten. These customized commands are also displayed in blue text, rather than the usual black.

```
navigator.queryViewers
navigator.reports
navigator.rules *
navigator.stages
```

- 5 Click **Apply** to save/apply the new shortcut, or click **OK** to save/apply the new shortcut and close the Preferences dialog.

Modifying Custom Shortcuts for Resources

You can modify a custom shortcut for a resource in either of these ways:

- Directly from the right-click Manage Hot Keys dialog on that resource
- From the Edit > Preferences > Manage Hot Keys dialog as described above in [“Modifying a Custom Shortcut” on page 565](#).

To remove a custom shortcut directly from the resource:

- 1 Navigate to and select the resource from which you want to remove the shortcut.
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.

- 3 Select the action (e.g., Show or Edit) associated with the shortcut.

The shortcut is shown in the “Press new shortcut” field.

- 4 Modify it as needed. (See [“Modifying a Custom Shortcut” on page 565](#).)
- 5 Click **OK** to save your changes and close the dialog.

Removing a Custom Shortcut

To remove a custom shortcut (key sequence) for any command:

- 1 Select the schema in which you want to modify the command.
- 2 Select the command for which you want to modify the hot key(s).
- 3 Select one of the customized commands (blue, with an asterisk).

```
navigator.queryViewers
navigator.reports
navigator.rules *
navigator.stages
```

The current key sequence associated with this command is shown in the **Shortcuts for selected command** field.

- 4 Click the **Remove** button next to the “Shortcuts for selected command field”.

The custom shortcut (key sequence) is removed, and replaced by the default key sequence (if there was one).



As soon as you remove the shortcut by clicking **Remove**, the changes are saved. Even if you click Cancel to close the Preferences dialog at this point, *the shortcut is not saved* for when you return.

For example, if `navigator.rules` was modified to be associated with Ctrl+Alt+X, then when you remove this shortcut `navigator.rules` would again be associated with its default shortcut of Ctrl+Alt+L.



Only custom shortcuts can be removed. Default shortcuts cannot be deleted.

Removing Custom Shortcuts for Resources

You can remove a custom shortcut for a resource in either of these ways:

- Directly from the right-click Manage Hot Keys dialog on that resource
- From the Edit > Preferences > Manage Hot Keys dialog as described above in [“Removing a Custom Shortcut” on page 567](#).

To remove a custom shortcut directly from the resource:

- 1 Navigate to and select the resource from which you want to remove the shortcut.
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.
- 3 Select the action (e.g., Show or Edit) associated with the shortcut.

The shortcut, if any, is shown in the “Press new shortcut” field.

- 4 Click **Remove**.
- 5 Click **OK** or **Cancel** to close the dialog.



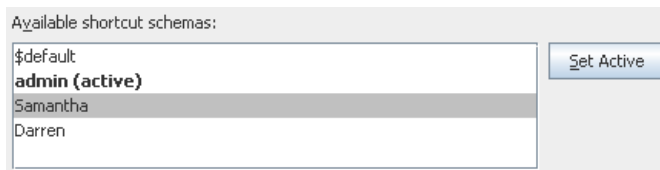
As soon as you remove the shortcut by clicking **Remove**, the changes are saved. Even if you click Cancel to close the dialog at this point, *the shortcut is not saved* for when you return.

Activating a New Shortcut Schema

For more information on schemas, see the introduction to the hot key management at [“Managing Hot Keys” on page 563](#).

To activate a new schema:

- 1 Select the schema you want to activate.

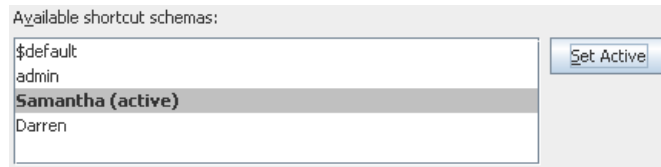


- 2 Click **Set Active**.



To get an enabled Set Active button, select a schema that is not currently applied. If you select a schema that is already active, the Set Active button is disabled.

- 3 Click **Apply** to apply the new schema, or click **OK** to apply the new schema and close the Preferences dialog.



Sharing Custom Shortcut Schemas

As of ESM v.4.5, *shortcut schemas are made available local to the ESM Console only*. That is, if schemas for several different users are configured on a Console running on a particular machine, those shortcut setups (i.e., schemas) will not be available from the same user logins on other machines.

For example, suppose you customize shortcuts for **admin** user, and two other users (e.g., Samantha a Darren) on laptop A. All three of those users can log in and use their shortcuts on the Console running on laptop A. But if the same users log in on another machine (laptop B) and log in as admin, Samantha, Darren, none of the custom shortcuts will be available on laptop B (unless the same shortcuts were set up manually here also).

Saving and Sending Settings

The **File Save** and **Save As** options allow you to save ArcSight Console settings (.ast files) locally. You can also save and load your own personal settings from the ArcSight Manager by using the **File Save to Manager** and **File Load from Manager** options. That way, for example, you can quickly restore Console settings when you move to a Console running on a different computer.

Saving a File

- 1 On the File menu, choose **Save** or **Save As**.
- 2 In the Save dialog box, navigate to a directory and enter a file name.
- 3 Click **Save**.

The ArcSight Console saves your settings in the file you specified, on the local computer. Later, you can restore those settings to return the Console to that configuration, using the **File>Open** command.

Saving a File to the ArcSight Manager

On the File menu, choose **Save to Manager**.

Your Console settings (based on your login user name) are saved to a file and maintained by the ArcSight Manager. To restore your Console to those settings, choose **File>Load from Manager**.

Loading a File From the ArcSight Manager

On the **File** menu, choose **Load from Manager**. The ArcSight Console loads the saved settings (.ast) file and asks whether you want to apply them to your current session. If you say **Yes**, the Console restarts and refreshes the display.

Sending a File by E-mail

- 1 Choose **File>Send To**.
- 2 In the Send To dialog box, enter the **E-mail Address** and click **OK**.

Chapter 22

Reference Guide

The topics that follow provide information on ESM resources, components, and terms in a “reference” format. Topics are organized alphabetically, and introduced and defined in a style meant to help you get more drill-down information about a term quickly and easily. Unlike a standard “glossary”, however, many of these topics present quite a bit of in-depth information including conceptual and reference material. These topics are cross-referenced (linked) extensively with the rest of the Help topics and vice versa.

Access Control Lists

ArcSight ESM uses Access Control Lists (ACLs) to manage user group permissions. ACLs define which user groups have permissions to which resources, and to which ESM components such as rules, reports, and filters. (See also [“Editing Access Control Lists \(ACLs\)” on page 443.](#))

User groups can have inspect (read) permissions, edit (write) permissions, or both. If a group has inspect permissions, it can read the resource. For example, the users in the group can see the resource and related information through the ESM Console. If the group has edit permissions, it can write to or change the resource, such as writing or editing a rule or report resource.

Resources can be read with inspect access or changed with edit access. Resources, like user groups, are managed as groups and not as individual resources. Therefore, a resource can only be accessed if a user group has access to the resource's group. Resources are login-based and only appear in the ESM Console if the logged in user has inspect permissions.



Always remember to have both ESM Console and ArcSight Web users log out and back in after changing user or resource access permissions, so they can see those changes.

Resource ACLs

Resources have ACLs to help you manage user permissions based on the resource. You can use the resource ACL to determine which user group will be able to access it. You can control which user group has access to inspect or to edit any resource, such as rules, cases, and reports. (See also [“Editing Access Control Lists \(ACLs\)” on page 443.](#))

Events are also available to user groups based on resource ACLs. For example, you can control which user group has access to a filter by adding the group to the filter's ACL and giving them inspect or edit permissions. If you no longer want the group to have permissions to that filter, you can edit the group's permissions or remove the group from the filter ACL. In this example, the user group listed on the filter ACL with inspect

permissions will be able to see events from that filter in the ESM Console. Those without permissions will not see any events from that filter.

Events are also extracted from the ArcSight Database based on ACLs. For example, when users generate reports, events extracted from the database are based on ACLs. Therefore, only data that users have access to is retrieved and all data may not be included in the report. Report ACLs will only provide events if the user generating the event has the permissions to view those events. For example, if user group A has permissions to view events from filter A and user group B does not, user group B will not be able to extract event values from filter A when running a report; the report will come back empty. However, since user group A does have permissions to filter A, user group A's report will come back with the values from filter A.



The Resource ACL display shows relationships between users and groups, and how permissions are acquired for each of the user groups. Child groups inherit permissions from parent groups.

For example, consider the following set of ACLs for assets.

Resource	1	R	W
/All Users/Administrators		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Users/Default User Groups		<input checked="" type="checkbox"/>	<input type="checkbox"/>
/All Users/Default User Groups/Analyzer Administrators		<input type="checkbox"/>	<input checked="" type="checkbox"/>

In this scenario, the following permissions apply:

- A user logged in as Administrator (belonging to the group /All Users/Administrators) has read and write permissions by virtue of being in the Administrators group.
- All users have read permissions because they belong to the group /All Users/Default User Groups by default.
- A user logged in as an Analyzer Administrator has both read and write permissions because they inherit read permissions from the parent group (/All Users/Default User Groups) and get write permissions per the Analyzer Administrators child group

Actions

Actions are automatic procedures that occur when all rule conditions and threshold settings have been met. You can choose to be notified of a triggered rule at the ESM Console or through the Notifier, have information about the events that triggered the rule sent to a case or an active list, or automatically execute a command line function. You can also assign more than one rule action to any rule. See also ["Rule Actions" on page 751](#).

Active Channels

Active channel event-viewing, introduced in ArcSight ESM v3.0, replaces the prior "real time" and "replay" styles of gathering events for analysis. Almost all event-related views are now **active channels**. Additionally, starting with ArcSight ESM v4.0, views for several types of resources related to assets and cases are also shown as active channels.

Rather than simply flowing events through as received, or capturing a fixed set of events for replay, a channel is in effect a live, on-going event query. Because it is continually re-evaluated, the set of events collected in a channel can continue to change (due to reporting latency), even when defined with a fixed time-bracket.

In other words, active channels are definitions for collections of events; definitions that are always freshly re-evaluated so the resulting sets are as valid as the data received up to that moment.

The queries that define active channels are composed, at a minimum, of time parameters; other filter conditions of the usual sorts can also apply. You find and use these queries in the Navigator panel's Active Channels resource tree. You create these definitions through the **File>New>Active Channel** command and can refine them using inline filters and the Active Channel Editor. Once defined and displayed, you can manipulate the order, format, and content of these views with all the familiar features of the ESM Console.

Starting with ArcSight ESM v.4.5, query viewers are provided as a quick alternative to active channels, better suited to some scenarios. See [“Query Viewers” on page 161](#) for more information.

Active Channel Views

Each individual view is one **rendering** of an active channel, whether it is a grid view or chart view. Individual views are represented by the tabs you see at the bottom edge of the Viewer panel. Channels are represented by the tabs at the top of the Viewer panel, that group together individual views.

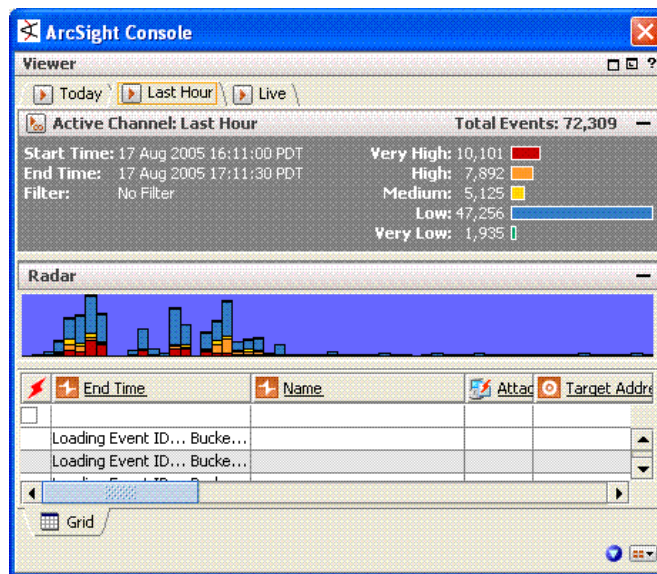


Figure 22-1 Channel tabs at the top of a view

Active Channel Headers

The channel name and statistics line appears at the top of active channel views. These statistics are event-severity indicators for the view. The indicators show the current number of events in the view for each of the priority categories. You can click these indicators to instantly filter the channel to show only the selected priority.

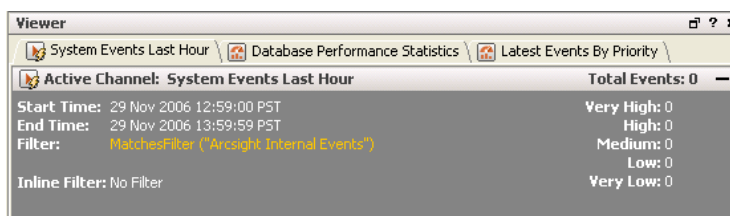
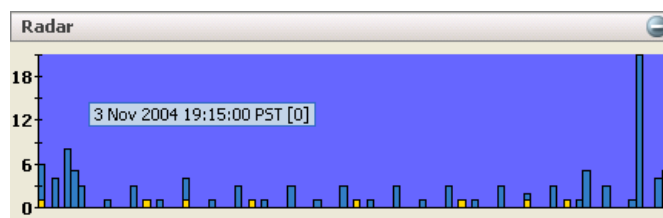


Figure 22-2 An Active channel header

The **Filter** status line describes the filter conditions the channel is currently using.

The Radar display in active channel headers indicates the activity taking place in the channel, in graphics that represent units of time horizontally, and numbers of events in vertical bars segmented by Priority attribute-value counts. The time and quantity scales in the graphic automatically adjust to accommodate the scope of the channel. The broader the scope, the smaller the graphical units become.

**Figure 22-3 A radar display in an active channel header**

You can open and close the Radar display with the **Plus (+)** and **Minus (-)** button at the right end of the Filter line.

With simple gestures, you can control the contents of a grid view using its Radar display.

Click, **Shift+click**, **Ctrl+click**, or drag to select one or more contiguous or non-contiguous bars in the display. You can also drag selection borders left or right to adjust a span further. The grid then shows just the events the selection represents.

Comparisons

You may want to note that the ArcSight ESM Manager handles active channel traffic through its database. This means that the content is persisted, but may involve processing delays that cause an active channel to show information later than a more direct method such as the data monitors in dashboards. Conversely, data monitor traffic resides only in memory and is subject to loss or abbreviation by server restarts.

See the topic [“Viewing and Using Channels” on page 92](#) to learn more about active channel tasks. You may also want to compare active channels to active lists as analysis tools.

Active Channel Views for Assets and Cases

The Console shows assets, vulnerabilities, asset categories, scanner reports, and cases in **active channels** (rather than static grid views, as in previous releases). Now you can leverage the power of channels for asset management, including use of filters, field sets, better sorting capabilities, and dynamic display of an unlimited number of items (continually updated).

Active Lists

You can use **active lists** to create a configurable data store that can hold information derived from events, or other sources.

No longer limited to IP addresses, active lists can now monitor activity based on any rule-driven combination of event attributes or set of custom fields. For example, active lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised.

You can populate active lists "manually" when necessary (adding entries from grid views or the Active List Editor), or use active lists in conjunction with rules specifically tailored to work with them. Rules can dynamically add and remove entries on active lists, thereby making them a flexible information-gathering tool.

You can now open and edit active lists in grid views.

Active lists function differently than active channels. Active lists are not continuously re-evaluated and are not time-window constrained. Active lists draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them.

You can use active lists as filters in other resources that are not based on active channels, such as reports.

In addition to their integral definitions, you can apply temporary (not saved) filters to active list grid views. Click the status description in the **Filter** line in the view header to use the Common Condition Editor.

ESM includes a set of default items in the Active Lists resource tree that you can use for templates or for operational monitoring with minor modifications. For example, use the Trusted List to watch activity from known-to-be-safe IP sources and the Untrusted List to do the same for known unsafe sources.

If you have Administrator access you will have another group named All Active Lists that contains all active list groups and lists.

Uses of Active Lists

The main uses of active lists are:

- Maintain information, such as in the system content provided "Hostile List" or "Trusted List" which maintain information on hostile and trusted IP addresses (and corresponding zones)
- Check for the existence of particular information in lists using the InActiveList condition (see ["Condition Tree Command Buttons" on page 618](#) under ["Common Conditions Editor" on page 616](#)).

For example, when a system is compromised (such as in a security breach), it can be added to the compromise list using rule actions. The information in the active list can then be used to collect all the events that occur on the asset while it is compromised. This can be used for tracking and further investigation on other systems that have come into contact with the compromised system

Active Lists for Long-term State Retention

Active lists can store data over a longer period of time than rules or data monitors are capable of retaining. For example, rules can hold a state that describes the very recent past, normally few minutes. Data monitors may contain up to a day's worth of data, but data monitors usually contain aggregated data.

For example, Active Lists can answer the following question, which cannot be addressed directly by rules or data monitors: "Has the source IP of the current event attacked one of my systems in the last 30 days?"

Optimize Data with Hash-Based Active Lists

A **hash-based active list** uses a hash function to map a set of data to a single number (a hash value).

To create a hash-based active list, enable the Optimize Data option on the Active Lists **Attributes** tab. (See [“Managing Active Lists” on page 385](#).)

The main advantage of using the hash-based active list (via the “Optimize Data” option) is to reduce memory usage. Instead of storing the complete active list entry in memory, only the hash code (a number), count, and last modified time are stored. The complete entry is available in the database. Therefore, the size of each entry in memory is constant, regardless of the number of fields and corresponding data types in the active list schema.

In terms of performance, there is little or no difference between hash-based and regular active lists.

The “Optimize Data” option is useful for active lists that will contain a large number of entries (for example, more than 100,000 entries) or a large amount of information per entry.



There is a possibility of getting an inaccurate result from an active list that uses the “Optimize Data” option due to hash collisions. When two active list entries map to the same hash code, the result of the “InActiveList” condition can be inaccurate in some cases. However, the chances of two entries evaluating to same hash code are quite rare. In the current scheme, for an active list with 1 million entries, the chances of hash code contention are about 1 in 4,000,000.

Active Lists can be switched between optimized (hashing) and non-optimized (non-hashing) after they are created.

Active List Audit Events

Audit events are sent on the following Active List Activity.

- Adding an entry (DEC: /ActiveList/Add)
- Removing an entry (DEC: /ActiveList/Delete)
- Updating an entry (DEC: /ActiveList/Update)
- Expiration of an entry (DEC: /ActiveList/Expire)
- Eviction of an entry (DEC: /ActiveList/Evict)



DEC stands for *device event class*, an event field. For example, when an active list entry is added, an audit event is generated with a DEC string of ActiveList/Add.

You can use audit events in rules, filters, and other analytical or administrative resources. For more information, see [“Audit Events” on page 583](#).

Active List Monitor Events

The following monitor events include Active List Usage statistics. (See [“Status Monitor Events” on page 766](#) for more information.)

- Open Active Lists count (DEC: /Monitor/ActiveLists/ListCount)

- Active List entry count (DEC: /Monitor/ActiveLists/EntryCount)
- Active List entry capacity (DEC: /Monitor/ActiveLists/EntryCapacity)
- Active List entry usage (% of capacity used) (DEC: /Monitor/ActiveLists/EntryPercentUsed)
- Active List entry look-ups per second (DEC: /Monitor/ActiveLists/QueriesPerSecond)
- Active List entry updates per second (DEC: /Monitor/ActiveLists/ChangesPerSecond)
- Temporary Active Lists count (DEC: /Monitor/ActiveLists/TemporaryListCount)
- Temporary List entry count (DEC: /Monitor/ActiveLists/TemporaryEntryCount)
- Temporary Active List entry capacity (DEC: /Monitor/ActiveLists/TemporaryCapacity)
- Temporary Active List entry usage (% of capacity used) (DEC: /Monitor/ActiveLists/TemporaryPercentUsed)

Active Lists with Values

An active list with values divides the set of fields into key fields and value fields. Active lists with values provide the following functionality:

- Use an "InActiveList" condition to check the existence of an entry (using only keys, or keys along with values). See ["Condition Tree Command Buttons" on page 618](#) in ["Common Conditions Editor" on page 616](#) for more about applying an "InActiveList" condition.
- Look up value fields, for given key field values

Variables are used to retrieve the value portion of the active list entry

To create an active list with values, select the **Fields-based** data option on the Active List editor "Attributes" tab, check **Key Fields** to enable a per-field Key option, and then select one or more data fields that must be unique. (For the complete procedure, see the topic on ["Creating an Active List" on page 385](#).)

Variables

You can define variables to retrieve value information from active lists with values. Be sure to specify these attributes for the variable:

- Name of the variable
- The active list to be used to retrieve values for the key
- Field mappings (mapping of the event fields to key fields in the active list)

Example: Active List with Values to Store Directory Information

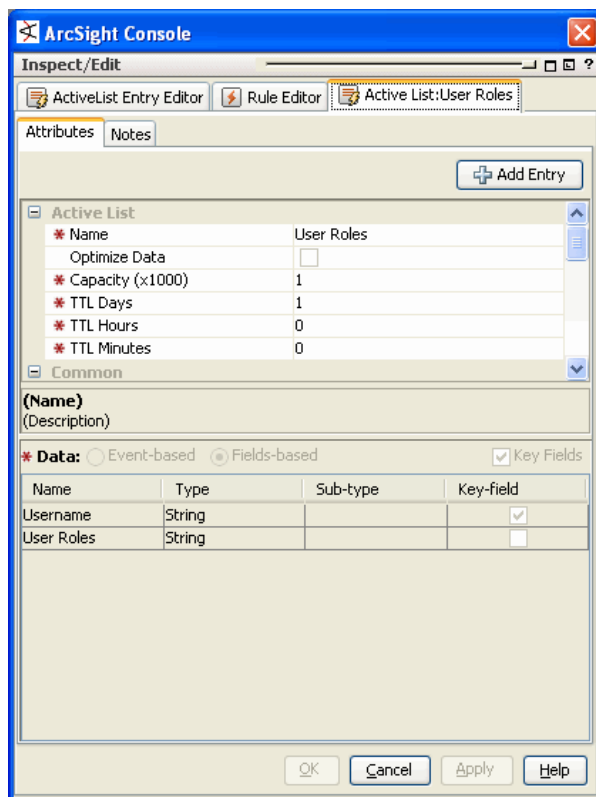
As an example, suppose we want to create an active list with values to store directory information.

Create an Active List

We follow the basic procedure to create a new active list shown in ["Managing Active Lists" on page 385](#). For the example, we create the active list with these options.

- Specify **Fields-based** data using **Key** fields
- The **Key** will be the "Username".

- The values will contain various information corresponding to the given user name. For simplicity, you can store only User "role" information. (The user role usually determines the type of actions a user can take, and on what type of resources.) If desired, you can store additional information such as the user's First Name, Last Name, Phone Number, Email Address, and so on.



Populate the Active List

We can populate the list in any of various ways:

- Manual data entry
- Export required information from Active Directory into a CSV file, and then import entries to the active list from the CSV file
- Use Active Directory User Group Puller tool
- Use event-based integration or other tools

Correlate Information Stored in UserRoles List

Once the Active Directory information is populated to an active list with values, we can access and correlate the user information using reports, rules, active channels, data monitors, and so on. The details of the correlation logic are as follows.

Create a Rule

For this example, we choose a rule that does the following:

- Looks for events that update some critical database information
- Checks if the target user had privilege to perform the operation using the Active Directory User Role information, maintained in the active list

(For more information on creating rules, see [“Creating Rules” on page 302](#) and [Chapter 13, Rules Authoring, on page 301](#).)

Use Variable to Get Role Information

For the database update events, we can get the corresponding Active Directory role information using the **GetActiveListValue** variable.

The 'Edit Variable' dialog box is shown with the following details:

- Name:** userRole
- Function:** GetActiveListValue
- Retrieve ActiveList value:** (checked)
- Arguments:**
 - List:** User Roles
 - Field Mapping:**

Name	Field	Key
Username	Target User Name	<input checked="" type="checkbox"/>
- Preview:**

Set a value for each key field.

Name	Value
Key Fields	
Username	

Buttons at the bottom: Calculate, OK, Cancel, Help.

Set Conditions to Check Role Permissions

Once the role information is retrieved, we can check if the user has the role required to perform this operation. If the user does not have the required role, then the rule will be triggered to alert the administrator to the unauthorized access.

The ArcSight Console Rule Editor is shown with the following details:

- Inspect/Edit** tab is active.
- ActiveList Entry Editor** and **Rule Editor** tabs are visible.
- Attributes** tab is selected.
- Event conditions:**
 - event1
 - AND
 - Name = Database Update
 - userRole.UserRoles NOT Contains |dba|
- Common Conditions Editor:**

Name	Op	Condition
Model Confidence		
Priority		
Relevance		
Severity	=	
Variables		
userRole.UserRoles	Contains	dba
userRole.UserRoles		
userRole.Username		

Buttons at the bottom: Test, OK, Cancel, Apply, Help.

Take Action Based on Results of Permissions Check

If the user does not have required role, then rule can trigger and alarm the administrator regarding this unauthorized access. (This is configured via the Actions tab.)

Working with Active Lists

For procedural information on working with active lists (including how to create, edit, delete, import, and export them), see [“Managing Active Lists” on page 385](#).

Administrator

An ESM administrator is a person who has the rights to administer ArcSight ESM and manage users, groups, and their permissions.

See also [“Users” on page 783](#), [“User Types” on page 783](#), [“Managing Users” on page 438](#), and [“Managing Permissions and Resources” on page 443](#).

Aggregation

Aggregation is a composition technique for building a new event from one or more existing events that support some or all of the new event's conditions.

You use aggregation to group occurrences of matching conditions based on incoming event field data values, and optionally count only distinct occurrences of those events. To support that, the Console provides Group By aggregation, in which you can group (aggregate) correlated events by field values. You can also optionally include distinct-value event processing combined with either join conditions and/or event grouping, to provide further constraints on when rules should fire.

Rules always run subject to their associated aggregation parameters, even if only the defaults.

ArcSight Web

ArcSight Web is ArcSight's next-generation web server product. ArcSight Web supersedes myArcSight as the web-based solution for access to the ArcSight [Manager](#).

- In ArcSight ESM, ArcSight Web offers a subset of the features found in the ArcSight ESM [Console](#), including full event monitoring and drill-down capabilities.
- For ArcSight Express users, the streamlined ArcSight Web client fitted with ArcSight Express specific content is the primary user interface for monitoring and analysis.

ArcSight Web features include monitoring [Events](#), managing [Cases](#), acknowledging and resolving [Notifications](#), running [Reports](#), and reading [Knowledge Base](#) articles. You can open ArcSight Web with the **File > Launch ArcSight Web** command in the Console, or use a bookmark that points to a URL similar to:

<https://<ArcSightWebHost>:9443/>

Because it can be installed at a location remote from the ESM Manager, ArcSight Web can operate outside a firewall that protects the Manager. Because of its new design, it also offers opportunities for custom branding and styling.

To learn more about ArcSight Web, please use its online Help system.



You can set the starting view of the home display for new ArcSight Web users through the ESM Console.

ArcSight Web uses the Macromedia Flash player, version 6.0 or later. While most browsers for most operating systems include Flash, some do not. If not, you will need to download it from <http://www.macromedia.com>.

See the instructions in the **ArcSight Installation and Configuration Guide** to install, set up, and begin using ArcSight Web.



When installing ArcSight Web, it is important to ensure that its version number matches the ESM Manager. Because a mismatch could cause unpredictable results, the web server prevents users from logging in. During setup, you will specify the ArcSight Web server. There is an option not to setup this server, but doing so will de-activate ArcSight Web.

Assets

Assets are network devices, installed throughout your enterprise, that you monitor for vulnerability or attack. Once asset information is stored in its database, ESM tracks your assets and notifies you if they are exposed to a threat or vulnerability, or if they are attacked.

Within the Navigator panel's Assets resource tree there are a number of views of associated information. The Assets, Networks, Zones, Locations, Categories, and Vulnerabilities tabs each show different aspects of the devices in question.

When, how, and why you might need to modify the resources in the Assets tabs is described in Managing Assets and Associated Resources, and particularly in Changing Assets. Help for managing hundreds of thousands of assets is described in ["Asset Scalability" on page 475](#). What the Assets tabs contain is described below.

Assets Tab

This view shows the population of your network as discreet entities with specific IP addresses and unique MAC and host names. You often use this view to pinpoint a particular asset, then double-click it to change its characteristics and associations in the Asset Editor. The presentation is hierarchical and shows only the assets to which you have access through the Asset Editor. Note that you can also identify mobile assets by MAC address.

Because the usage (Zones) and descriptive (Categories) views are separate, the Assets view is free to accurately describe the access restrictions that apply to a given user.

The Internet Address Range asset category has its own Asset Range Editor. The address range groups are standard spans of IP addresses provided as a convenience for your use in rules. You can also collectively reference these ranges using the named networks on the Zones tab. For example, a rule could reference the Dark Address Space item under System Zones to identify a category of source IP addresses from which traffic should not legitimately originate.

The Asset, Zone, and Asset Range Editors all include Categories and Zones tabs for editing these attributes.

The Asset Editor has an Alternate Interfaces tab. When a single device has multiple network interfaces, you can define each interface as an independent asset. Common examples of multiple interface devices are network connection points such as routers and bridges. To use this editor from an appropriate asset in the tree, right click it and choose **View Asset Alternate Interfaces**.

An asset or asset range (or its group) can belong to only one zone or location.

Zones Tab

The **Zones** tab shows the hierarchy of network-related logical (usage) groups into which assets are collected, and on which you can act through the Zone Editor.

You can also think of zones as aliases for portions of your network that are dedicated to certain organizational groups or functions. The Zones view can help disambiguate multiple private networks that might have overlapping address spaces.

When the zones in your enterprise are referencing multiple global or local zones, ArcSight networks can help disambiguate erroneous address space overlaps or gaps, especially for SmartConnectors. A zone or zone group can belong to only one network or location, and expresses a single contiguous address range.

Networks Tab

Here you can view the hierarchical collection of network entities recognized within your system. In this context a "network" is an enterprise-level registry of ArcSight zones. "Networks" are used to reconcile overlapping or missing asset ranges among zones (if they should erroneously occur). When networks are present, SmartConnectors use them to find their correct zone assignments. Note that networks apply only in enterprises that have networks broad enough to require multiple local or global maps. If your enterprise maps only its own address space (meaning that overlaps and gaps aren't likely) the Networks tab won't be populated.

Each Network resource can relate to only one Customer resource, but to multiple Zones, provided address ranges do not overlap.

Categories Tab

The hierarchy of asset categories provides a way to reference assets by means of their application or context. A given asset can be associated with multiple categories.

Asset categories are a cross-referencing capability that supports numerous business objectives. By making it possible to track network activity with certain assets on the basis of their business significance, data collection becomes possible; but just as importantly, other ArcSight ESM analytical tools can also be brought to bear to derive many kinds of information. Finally, ESM reporting capabilities can further analyze and permanently record the results.

The categories for a given enterprise are often quite specialized, but certain categories are usually present, even if customized.

Typical high-level asset categories often include:

- **ArcSight System Administration:** These are the assets that make up the ESM world, meaning its Console, Databases, SmartConnectors, and Managers. ESM automatically detects its own administrative assets and creates these entries in their respective groups.

- **Site Asset Categories:** These can be general monitoring categories such as Address Spaces, Applications, or Open Ports, but will likely include asset-tracking categories that are specific to issues such as business impacts and regulatory compliance. Business impacts might analyze the activity of a server that supports a particular product line. Regulatory compliance could monitor groups of workstations for HIPAA conformity.
- **System Asset Categories:** These can be any of a number of categorizations of assets such as Criticality (low, medium, high, very high), which would monitor by a classification of how crucial assets are to the enterprise.



SmartConnector configuration also affects the ability of ESM to automatically create the assets that represent network devices. Each SmartConnector needs to report an IP address or hostname for its sensor so its events can be identified on the network. See the configuration guides for your SmartConnectors to ensure they are reporting this information.

Vulnerabilities Tab

The **Vulnerabilities** tab presents known vulnerabilities associated with the devices identified through the Assets tab.

Device vulnerabilities are presented as closely as possible with device descriptions to facilitate useful comparisons and easy reference

Locations Tab

The **Locations** tab shows the hierarchy of names your enterprise uses for its physical or geographical domains.

Similar to zones, you can think of locations as another type of alias. You use this alias for portions of your network that are referenced by where they are rather than by organizational group or function. A given asset or asset range can be associated with only one location, but a given location can be associated with any number of appropriate assets, zones, or their groups

Attack

An exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit Events

Audit events are ones generated within ESM to mark a wide variety of routine actions that can occur manually or automatically, such as adding an event to a case or when a Moving Average data monitor detects a rapidly rising moving average. Audit events have many applications, which can include notifications, task validation, compliance tracking, automated housekeeping, and system administration.

This topic lists the ArcSight audit events you can use in your rules, filters, and other analytical or administrative resources. Observe the way these events are used in the default system-related resources for examples of how to apply them.

In the table below, use the **Audit Event Category** to locate events. You use the Device Event Class (DEC) ID string in rules and filters. The **Audit Event Description** reflects the

resource name you see in active channel grids. Additional details, when necessary, appear in the **Notes** column.

Compare audit events, which report on *system activity*, with [Status Monitor Events](#) events, which provide information about a wide variety of *system states*.



Starting with ESM 4.5, updates to existing resources are logged as audit events “[Resources \(Configuration Events Common to All Resources\)](#)” on page 594.

To get *additional* details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property called `resource.audit.update.uris` in the file `server.defaults.properties` on the ESM Manager to specify which resources should show extended audit event information.

For more information, see “[Extending Audit Event Logging](#)” on page 547.

Active Channel

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Active Channel	<code>activechannel:100</code>	An active channel was opened	
Active Channel	<code>activechannel:101</code>	An empty active channel was opened	

Active List

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Active List	activelist:101	An entry was added to an active list	
Active List	activelist:102	An entry was removed from an active list	
Active List	activelist:103	An entry was changed in an active list	

Authentication

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Authentication	authentication:100	A client authenticated with the Manager	
Authentication	authentication:101	A client authentication login failed	
Authentication	authentication:102	An authenticated client logged out of the Manager	
Authentication	authentication:103	Authentication logout time	
Authentication	authentication:104	A client made several unsuccessful attempts to log in to the Manager, resulting in an excessive number of failed logins	
Authentication	authentication:105	A non-FIPS client authenticated with the Manager via login. (A valid login by a non-FIPS Arcsight ESM Console authenticating itself to the ESM Manager will trigger this audit event.)	For information on how to configure a non-FIPS client (such as ESM Console) to log in to a FIPS-enabled Manager, see the ArcSight ESM Administrator's Guide.
Connector Login	authentication:200	Successful connector authentication	
Connector Login	authentication:201	Connector authentication failed	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Authentication	authentication:202	A non-FIPS connector authenticated with the Manager via login. (A valid login by a non-FIPS Arcsight ESM SmartConnector authenticating itself to the ESM Manager will trigger this audit event.)	For information on how to configure a non-FIPS SmartConnector to connect to a FIPS-enabled Manager, see the ArcSight ESM Administrator's Guide.



Looking for User Login and User Management audit events? See [“User Login” on page 599](#), [“Group Management” on page 590](#), and [“User Management” on page 600](#).

Authorization

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Authorization	authorization:100	Manager refused to authorize client	



Looking for User Login and User Management audit events? See [“User Login” on page 599](#), [“Group Management” on page 590](#), and [“User Management” on page 600](#).

Connectors

Audit events related to SmartConnectors are described in the following tables.

Connector Connection

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Connection	agent:009	Manager rejected a connection attempt from a connector for reasons other than authentication failure	
Connector Connection	agent:30	Connector started	
Connector Connection	agent:31	Connector shutdown	
Connector Connection	agent:101	Connector has just connected to Manager	
Connector Connection	agent:102	Connector is sending events but no heartbeats	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Connection	agent:103	Connector is sending neither events nor heartbeats	
Connector Connection	agent:104	An unknown connector attempted to connect to the Manager	
Connector Connection	agent:105	A connector presented an incorrect shared secret when authenticating	

Connector Exceptions

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Exceptions	agent:012	Connector detected source events from a sensor device containing incorrect time stamps	
Connector Exceptions	agent:013	Connector noted that a new sensor device is sending events	
Connector Exceptions	agent:014	Connector could not find a base event referenced in a syslog aggregate event	
Connector Exceptions	agent:016	Connector successfully connected to the sensor device's log	
Connector Exceptions	agent:017	Connector successfully executed a command	
Connector Exceptions	agent:018	Connector could not execute a command	
Connector Exceptions	agent:019	Connector is caching events because they could not be immediately transmitted to the Manager	
Connector Exceptions	agent:020	Connector has emptied its cache of events	
Connector Exceptions	agent:021	Connector could not communicate with an NT collector sensor	
Connector Exceptions	agent:023	Connector could not communicate with a CheckPoint sensor	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Exceptions	agent:024	Connector is having difficulty communicating with CheckPoint	
Connector Exceptions	agent:028	Connector experienced an unexpected problem	
Connector Exceptions	agent:029	Connector was forced to drop its cached data	
Connector Exceptions	agent:030	Connector cache filled and part of the cached data was deleted	

Connector Login

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Login	authentication:200	Successful connector authentication	
Connector Login	authentication:201	Connector authentication failed	

Connector Registration and Configuration

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Registration and Configuration	agent:007	Connector successfully registered with Manager	
Connector Registration and Configuration	agent:008	Connector did not successfully register with Manager	
Connector Registration and Configuration	agent:029	Connector configuration was successfully change	
Connector Registration and Configuration	agent:022	Connector could not process a reconfiguration request	
Connector Registration and Configuration	agent:032	Connector configuration was successfully changed	
Connector Registration and Configuration	agent:025	Connector content was successfully updated	
Connector Registration and Configuration	agent:026	Connector content update failed	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Connector Registration and Configuration	agent:010	Connector upgrade succeeded	This is currently in the context of an installer upgrade.
Connector Registration and Configuration	agent:011	Connector upgrade failed	This event is not currently being generated.

Dashboard

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Dashboard	dashboard:100	Dashboard has opened	

Data Monitors

Audit events related to data monitors are described in the following tables, categorized by data monitor type.

Moving Average Data Monitor

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Moving Average Data Monitor	datamonitor:102	Moving Average data monitor detected a rapidly falling moving average	
Moving Average Data Monitor	datamonitor:103	Moving Average data monitor detected a rapidly rising moving average	
Moving Average Data Monitor	datamonitor:104	Moving Average data monitor reporting the current moving average	

Reconciliation Data Monitor

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Reconciliation Data Monitor	datamonitor:300	Correlation data monitor reporting a correlated or non-correlated event	

Statistical Data Monitor

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Statistical Data Monitor	datamonitor:200	Statistical Data Monitor reporting a change in status	

Top Value Counts Data Monitor

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Moving Average Data Monitor	datamonitor:500	For a Top Value Counts DataMonitor, the top N counts (N events)	
Moving Average Data Monitor	datamonitor:501	Counts that were most recently added to the data monitor (from 0 ... N events)	
Moving Average Data Monitor	datamonitor:502	Counts that were most recently removed removed from the data monitor (from 0 ... N events)	

Group Management

The following audit events are generated for any group add, update, or delete, including user groups. The details of the which type of resource was configured or modified are provided in the event name. (For more information on user management audit events, see ["User Management" on page 600.](#))

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Group Delete	group:100	A group was deleted	
Group Update	group:101	A group was updated	This audit event is generated (1) when an existing group is modified, and (2) in conjunction with a "group add" audit event when a new group is added (see also Group Add).
Group Add	group:102	A group was added (inserted)	When a new group is added, two audit events are generated: this Group Add event (group:102), and a Group Update audit event (group:101).

Manager Activation

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Manager Activation	manager:100	Manager has started	
Manager Activation	manager:101	A clean Manager shutdown has been requested	

Manager Database Error Conditions

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Manager Database Error Conditions	database:100	Database tablespace is low and will be deactivated	
Manager Database Error Conditions	database:101	Database has generated a fatal error and will be deactivated	
Manager Database Error Conditions	database:102	Database has been reactivated	
Manager Database Error Conditions	database:103	Database has more tablespace available after detecting a low tablespace condition	

Manager External Event Flow Interruption

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Manager External Event Flow Interruption	manager:200	Manager has stopped the event flow	
Manager External Event Flow Interruption	manager:201	Manager has allowed the event flow to resume	

Notifications

Audit events related to notifications are described in the following tables.

Notification

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Notification	notification:100	Notification has been disabled	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Notification	notification:101	Notification has been disabled because the queue of notifications to be sent is too large	
Notification	notification:102	Notification has been enabled	
Notification	notification:103	Notification has been enabled because the queue of notifications is back under control	
Notification	notification:104	A particular notification destination has been disabled	
Notification	notification:105	A particular notification destination has been disabled because too much traffic was directed at it	
Notification	notification:106	A particular notification destination has been enabled	
Notification	notification:107	A notification expired without being acknowledged	
Notification	notification:108	A functioning destination could not be located for this notification	
Notification	notification:109	Old notification has been purges	

Notification Acknowledgement, Escalation, and Resolution

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Notification Escalated	notification:110	Notification has been escalated	
Notification Sent Requires Acknowledgement	notification:111	Notification sent requires acknowledgement	
Notification Sent (Informational)	notification:112	An informational notification was sent	
Notification Acknowledgement	notification:300	This notification has been acknowledged	
Notification Resolve	notification:301	This notification has been resolved	

Notification Testing

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Notification Testing	notification:20	Sent a test notification to this destination group	

Partition Archiver

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Partition Archiver	partitionarchiver:100	The partition was successfully archived	
Partition Archiver	partitionarchiver:200	There was a problem while archiving the partition	
Partition Archiver	partitionarchiver:300	Partition archiving is disabled	
Partition Archiver	partitionarchiver:400	Partition archiving did not complete in the allotted time	
Partition Archiver	partitionarchiver:500	Partition archiving failed	
Partition Archiver	partitionarchiver:600	There was an unexpected error while archiving partitions	

Partition Manager

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Partition Manager	partitionmanager:100	Partitions have been successfully rotated	
Partition Manager	partitionmanager:200	There was a problem rotating partitions	
Partition Manager	partitionmanager:300	The partition manager has been disabled	
Partition Manager	partitionmanager:500	Partitions could not be rotated	
Partition Manager	partitionmanager:600	There was an unexpected error while rotating partitions	

Query Viewers

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Query Viewer	<code>queryviewer:100</code>	Base query used by the query viewer succeeded	
Query Viewer	<code>queryviewer:101</code>	Base query used by the query viewer failed	

Reports

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Report	<code>report:100</code>	Generated a new archived-report configuration resource	
Report	<code>report:101</code>	Failed to generate a new archived-report configuration resource	
Report	<code>report:102</code>	Generated a new delta archived-report configuration resource	

Resources (Configuration Events Common to All Resources)

These audit events are generated in response to configuration updates to any resource, regardless of type. As shown below, the Device Event Class ID (DEC ID) for these events is generic in terms of resource type. However, the resource type is given in the event name.



To get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property called `resource.audit.update.uris` in the file `server.defaults.properties` on the ESM Manager to specify which resources should show extended audit event information.

For more information, see “[Extending Audit Event Logging](#)” on page 547.

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Resource (Delete)	<code>resource:100</code>	Resource deleted	The Event Name describes the action and resource type (<code><ResourceName> deleted</code>); e.g., deleting a filter results in an event named <code>Filter deleted</code> .

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Resource (Update)	resource:101	Resource updated	This audit event is generated (1) when an existing resource is modified, and (2) sometimes in conjunction with an add audit event when a resource is added. See also Resource (Add) . The Event Name describes the action (update) and resource type ((<ResourceName> updated)); e.g., modifying a report, results in an event name of Report updated .
Resource (Add)	resource:102	Resource added (inserted)	The Event Name describes the action (insert) and resource type ((<ResourceName> inserted)); e.g., adding a case, results in an event name of Case inserted . Adding a Case group results in an event name of Group [Case] inserted .
Resource	resourcereference:100	Could not locate a resource	Through the supplied universal resource identifier (URI).

Resource Quota

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Resource Quota	quota:100	Resource usage has fallen below the fixed-quota level	
Resource Quota	quota:101	Resource usage has exceeded the fixed-quota level	
Resource Quota	quota:102	Asset autocreation has exceeded a fixed quota	
Resource Quota	quota:103	Asset autocreation is proceeding too rapidly	

Rules

Audit events for rules are described in the following tables.

Rule Actions

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Actions	rule:301	Set Severity action	This event has been deprecated.
Rule Actions	rule:302	Set Event Attribute action	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Actions	rule:303	Send to Notifier action	
Rule Actions	rule:304	Execute Command action	
Rule Actions	rule:305	Export... action	
Rule Actions	rule:306	Create New Case action	
Rule Actions	rule:307	Add to Case action	
Rule Actions	rule:308	Create New Case action failed	
Rule Actions	rule:309	Add to Case action failed	
Rule Actions	rule:310	Add to Active List action	
Rule Actions	rule:311	Move between Active Lists action	This event has been deprecated.
Rule Actions	rule:312	Remove from Active List action	

Rule Activations

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Activations	rule:700	Rule has been deactivated	
Rule Activations	rule:701	Rule has been deactivated because it is unsafe	There was excessive recursion or event matching.
Rule Activations	rule:702	Rule has been activated	

Rule Firings

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Firing	rule:100	Any rule fired	
Rule Firings	rule:101	Rule fired OnEveryEvent	
Rule Firings	rule:102	Rule fired OnFirstEvent	
Rule Firings	rule:103	Rule fired OnSubsequentEvents	
Rule Firings	rule:104	Rule fired OnEveryThreshold	
Rule Firings	rule:105	Rule fired OnFirstThreshold	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Firings	rule:106	Rule fired OnSubsequentThresholds	
Rule Firings	rule:107	Rule fired OnTimeUnitExpiration	

Rule Warnings

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Rule Warnings	rule:501	Rule is firing on events generated by itself	

Scheduler

Audit events related to the job scheduler are described in the following tables.

Scheduler Execution

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Scheduler Execution	scheduler:200	A task has been executed	
Scheduler Execution	scheduler:201	A task failed to execute	

Scheduler Scheduling Tasks

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Scheduler Scheduling Tasks	scheduler:300	A new task has been scheduled	
Scheduler Scheduling Tasks	scheduler:301	A new task could not be scheduled	
Scheduler Scheduling Tasks	scheduler:302	Enabled a task	
Scheduler Scheduling Tasks	scheduler:303	Could not enable a task	
Scheduler Scheduling Tasks	scheduler:304	Deleted a task	
Scheduler Scheduling Tasks	scheduler:305	Failed to delete a task	
Scheduler Scheduling Tasks	scheduler:306	Disable a task	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Scheduler Scheduling Tasks	scheduler:307	Could not disable a task	

Scheduler Skip

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Scheduler Skip	scheduler:100	The task scheduler skipped a scheduled task execution because the scheduler was not allowed to run	
Scheduler Skip	scheduler:101	The task scheduler skipped a scheduled task invocation because the last invocation of the task is still executing	

Stress

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Stress	test:100	A stress test event	This event is generated only by ArcSight Quality Assurance.

Trends

Audit events for trends are described in the following tables.

Trends (Starting)

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend	trend:100	Trend run started	
Trend	trend:101	Trend run success	
Trend	trend:102	Trend run failure	

Trend Partitions

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend Partitions	trend:301	Trend partition added	
Trend Partitions	trend:302	Trend partition dropped	

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend Partitions	trend:303	Trend partition add failed	
Trend Partitions	trend:304	Trend partition drop failed	

Trends Enabled or Disabled

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend	trend:401	Trend enabled	
Trend	trend:402	Trend disabled	

Trend Tasks

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend	trend:501	Trend task started	
Trend	trend:502	Trend task ended	

Trend Deactivated by System

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
Trend	trend:601	Trend was automatically deactivated because of too many failures	

User Login

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
User Login	authentication:100	Successful client login	
User Login	authentication:101	Failed client login	
User Login	authentication:102	Client logout	
User Login	authentication:103	Client timed out due to inactivity	
User Login	authentication:104	Too many client login failures occurred within a time period	

See also, [“Group Management” on page 590](#), which reflects adds, deletes, and updates of groups, including user groups.

User Management

Audit Event Category	Device Event Class ID	Audit Event Description	Notes
User Delete	user:100	A user account was deleted	
User Update	user:101	A user account was updated	This audit event is generated (1) when an existing user account is modified, and (2) in conjunction with a "user add" audit event when a new user account is added (see User Add below).
User Add	user:102	A user account was added (inserted)	When a new user account is added, two audit events are generated: this User Add event (user:102), and a User Update update event (user:101).

See also, "[Group Management](#)" on page 590, which reflects adds, deletes, and updates of groups, including user groups.

Batching

Batching is a mode in which ArcSight SmartConnectors receive or send collections of events at one time rather than immediately after each occurrence.

Case Editor Tab Fields

This topic is a directory to reference information about the fields on the Case Editor tabs.

The ESM Case Editor displays case information organized in five major tabs:

Case Editor Tab	Description
Initial	Basic case information: case ticket attributes, description and security classification.
Follow-Up	Description of actions taken, planned, or recommended.
Final	Ticket resolution and reporting including attack mechanism, attack agent, incident information, and vulnerability information.
Events	List of events included in case.
Attachments	List of attachments in the case. Provides option to attach or detach items to the case.
Notes	Miscellaneous case information.



To edit a saved case, you first need to select the **Lock Case** check box, so other users can't modify it while you're editing.

This organization lets you separate information based on the workflow and handling or resolution of individual cases.

Initial Tab

[Case Editor Initial - Attributes Tab](#)

[Case Editor Initial - Description Tab](#)

[Case Editor Initial - Security Classification Tab](#)

Follow-up

[Case Editor Follow-Up Tab](#)

Final

[Case Editor Final - Attack Mechanism Tab](#)

[Case Editor Final - Attack Agent Tab](#)

[Case Editor Final - Incident Information Tab](#)

[Case Editor Final - Vulnerability Tab](#)

[Case Editor Final - Other Tab](#)

Events

[Case Editor Events Tab](#)

Attachments

[Case Editor Attachments Tab](#)

Notes

[Case Editor Notes Tab](#)

Case Editor Events Tab

The fields on this tab provide a list of the events included in a case.

Field	Description
Description	Events auto-populated from events included in a case.
Event Info and Payload fields	For selected events, displays event field values and payload fields, if available.

Case Editor Attachments Tab

This tab lists attachments (if any) for the case, and provides options to attach new items via a file browser or detach items.

Case Editor Final - Attack Agent Tab

Fields on this tab provide ticket resolution and reporting information related to the attack agent associated with a case.

Field	Description
Attack Agent	Auto-populated from Security Classification tab. Possible values are I (Insider), C (Collaborative), O (Outsider), and U (Unknown).
Attack Location Id	Text field allowing entry of up to 255 characters.
Attack Node	Text field allowing entry of up to 255 characters.
Attack Address	Text field allowing entry of up to 255 characters.

Case Editor Final - Attack Mechanism Tab

The fields on this tab provide final ticket resolution and reporting information for the attack mechanism associated with a case.

Field	Description
Attack Mechanism	Auto-populated from Security Classification tab. Possible values are P (Physical), O (Operational), I (Informational), and U (Unknown).
Attack Protocol	Text field allowing entry of up to 64 characters.
Attack OS	Text field allowing entry of up to 64 characters.
Attack Program	Text field allowing entry of up to 255 characters.
Attack Time	Date field.
Actions Target	Text field allowing entry of up to 4000 characters.
Attack Service	Text field allowing entry of up to 4000 characters.
Attack Impact	Text field allowing entry of up to 4000 characters.
Final Report Action	Text field allowing entry of up to 4000 characters.

Case Editor Final - Incident Information Tab

The fields on this tab provide final incident information associated with a case.

Field	Description
Incident Source 1	Auto-populated from Security Classification tab.
Incident Source 2	Auto-populated from Security Classification tab.
Incident Source Address	Text field allowing entry of up to 200 characters.

Case Editor Final - Other Tab

The fields on this tab provide miscellaneous ticket resolution and final reporting information.

Field	Description
History	Selections include: Known Occurrence and Unknown
No Occurrences	Numeric value
Last Occurrence Time	Enterable time or selector.
Resistance	Selections include: High, Low, Unknown
Consequence Severity	Auto-populated from Initial Attributes tab
Sensitivity	Auto-populated from Initial Attributes tab
Recorded Data	Text field allowing entry of up to 4000 characters.
Inspection Results	Text field allowing entry of up to 4000 characters.
Conclusions	Text field allowing entry of up to 4000 characters.

Case Editor Final - Vulnerability Tab

The fields on this tab provide final ticket resolution and reporting information related to the vulnerabilities associated with a case.

Field	Description
Vulnerability	Auto-populated from Security Classification tab. Possible values are D (Design), O (Operational), E (Operational Environment), and U (Unknown).
Vulnerability Type 1	Selections include: Accidental or Intentional
Vulnerability Type 2	Selections include: EMI/RFI, Insertion of Data, Theft of Service, Unauthorized, Probes, Root Compromise, DoS Attack, User Account
Vulnerability Evidence	Text field allowing entry of up to 4000 characters.
Vulnerability Source	Text field allowing entry of up to 4000 characters.
Vulnerability Data	Text field allowing entry of up to 4000 characters.

Case Editor Follow-Up Tab

The fields on this tab describe follow-up entries for a case.

Field	Description
Actions Taken	Text field allowing entry of up to 4000 characters.
Planned Actions	Text field allowing entry of up to 4000 characters.
Recommended Actions	Text field allowing entry of up to 4000 characters.

Field	Description
Followup Contact	Text field allowing entry of up to 4000 characters.

Case Editor Initial - Attributes Tab

The fields on this tab provide basic case information.

Field	Description
Case:	
Name	Required field specifying name of case.
Display ID	An identification provided by an external tracking system.
Ticket:	
Ticket Type	Drop-down list includes Internal, Client, and Incident types.
Stage	Indicate workflow stage of ticket; default selections include Queued, Initial, Follow-Up, Final, and Closed.
Frequency	Indicates how often reported issue occurs. Values assigned are 0 (never or once), 1 (less than 10 times), 2 (10 to 15 times), 3 (15 times), 4 (more than 15)
Operational Impact	Impact of reported issue. Values assigned are 0 (no impact), 1 (no immediate impact), 2 (low priority impact), 3 (high priority impact), 4 (immediate impact)
Security Classification	Values assigned are 1 (Unclassified), 2 (Confidential), 3 (Secret), 4 (Top Secret)
Consequence Severity	Values assigned are 0 (None), 1 (Insignificant), 2 (Marginal), 3 (Critical), 4 (Catastrophic)
Reporting level	Number calculated based on Ticket info values entered.
Incident Information:	
Detection Time	Automatically assigned from event info.
Estimated Start Time	Automatically assigned from event info.
Estimated Restore Time	Automatically assigned from event info.



You can also use entries in all Case Ticket fields to generate reports so you can categorize cases based on specific case information.

Case Editor Initial - Description Tab

The fields on this tab further describe a case.

Field	Description
Affected Services	Text field allowing entry of up to 4000 characters.

Field	Description
Affected Elements	Text field allowing entry of up to 4000 characters.
Estimated Impact	Text field allowing entry of up to 4000 characters.
Affected Sites	Text field allowing entry of up to 4000 characters.

Case Editor Initial - Security Classification Tab

The fields on this tab describe the security classification for a case.

Field	Description
Security Classification:	
Attach Mechanism	Selections include: P (Physical), O (Operational), I (Informational), and U (Unknown)
Attack Agent	Selections include: I (Insider), C (Collaborative), O (Outsider), and U (Unknown)
Incident Source 1	Editable text.
Incident Source 2	Editable text.
Vulnerability	Selections include: D (Design), O (Operational), E (Operational Environment), and U (Unknown)
Sensitivity	Selections include: U (Unclassified), C (Confidential), S (Secret), and T (Top Secret)
Associated Impact	Selections include: A (Availability), C (Confidentiality), I (Integrity), and U (Unknown)
Action	Selections include: B (Block/Shutdown), M (Monitoring), and O (Other)
Security Classification Code:	
Code	Value automatically calculated from other Security Classification field entries.

Case Editor Notes Tab

The fields on this tab provide a place to enter miscellaneous case information and notes.

Field	Description
Notes	Text field allowing entry of up to 4000 characters that you can save per note.
Table and List Tabs	Table lists saved notes that you can select to display contents; List provides a combined listing of the all saved notes, in chronological order.

Cases

Cases are entries in an event-tracking system used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases

are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.

ArcSight ESM has two ways to create and handle cases. First, it has its own complete case-management system. You can use this system to create new cases and assign them to specific groups and users who will be notified and receive the cases and relevant data and information associated with the case. Those users can then act on the assigned cases, specifying resolution or other actions taken on the case, which gets reported back and recorded in the ongoing or final resolution of a case.

In addition to using the built-in case management system that ArcSight provides, you can also integrate ESM with other external case management systems such as Remedy. In that situation, adding new cases in ESM will export event information and bring up forms of the external case management system for you to create and assign new cases. The integration with external case management system can also be customized so that case resolution is reported back and recorded within ESM.

Case attachments enable you to attach files to any case you are able to edit, for example log files. You are also able to delete cases and attachments; if you delete a case, it will delete the attachment. You can add a file to a case, making it public or private. Private means that the attachment is never shared with other cases; Public means that everyone has access to the latest edited version of that file. Sharing attachments makes it possible to share files that are common among many cases, for example as with a non-disclosure agreement.

For complete information on working with cases, see [“Managing Cases” on page 397](#).

Case Groups

Cases are organized into these groups:

Case Group	Description
<User Name>'s Cases	Those assigned to the user ID.
Shared Cases	Cases that the logged-in user has permission to access.
Public Cases	Cases to which all users have read permission.
Unassigned	Cases that are not assigned to any user.

If you have Administrator access you will also have a group named All Cases that contains all user case groups and their cases.

Categories

ArcSight ESM uses six primary categories and a flexible set of supporting attributes to more precisely distinguish the events reported by SmartConnectors or generated internally by ESM Managers. You see these under the Category heading in tools such as the [Common Conditions Editor](#), [Rules Editor](#), or [Event Inspector](#). This ability to recognize more detailed and specific event conditions greatly increases your analytic and reactive options.

These categories and attributes are designated by ArcSight, based on the information offered to SmartConnectors by sensors. Keep in mind that the applicability of a category always depends on the actual configuration of the environment.

If you create a new SmartConnector, remember that you are responsible for establishing the ArcSight categories it should report.

The category groups are:

Category	Description
Object Category	Events are always about a certain object. An object can, for example, be an application, the operating system, a database, a file or the memory of a server. It is important to realize that we are referring to the targeted object. It is not about who is doing something, but what is the object being accessed, altered, etc. (See "Object Category" on page 607.)
Behavior Category	Events not only refer to certain objects, but there is generally an action or a behavior associated with an event. What is being done to an object? Behaviors include access, execution, or modification, and so on. (See "Behavior Category" on page 609.)
Outcome Category	With the first two dimensions, we know what object is being referred to and what action targeted the object. However, we do not know whether the behavior was successful or not. Therefore, the outcome is a success, a failure or an attempt. An attempt really indicates that something was neither a success nor a failure and the outcome is not clear or there is no statement that could be made about the outcome. (See "Outcome Category" on page 610.)
Device Group Category	Many security devices serve a multitude of purposes in one product. Intrusion Prevention Systems for example, generate events associated with their firewalling capabilities, as well as their intrusion detection capabilities. To be able to distinguish between these types of events, we introduced a dimension called deviceGroup . This dimension allows us to query, for example, for all of the firewall-type events as opposed to all of the events generated by a firewall. The distinction being that the former query also returns all the firewall messages, for example, in the operating system logs (e.g., iptables). (See "Device Group Category" on page 611.)
Technique Category	Frequently in a security context, we would like to obtain information about the type of events with respect to a security domain. Is an event talking about a denial of service, a brute force attack, IDS evasions, exploits of vulnerabilities, etc. (See "Technique Category" on page 611.)
Significance Category	We need to know the significance of an event. We need the capability, for example, to separate normal events from hostile events. We also need to know whether certain activity reported by the device impacts the availability, confidentiality, or integrity of our systems. All this information is captured in significance. (See "Significance Category" on page 613.)

Object Category

Host	Any end-system on the network, such as a PDA, a Windows computer, or a Linux computer.
Operating System	The system software that controls execution of computer programs and access to resources on a host.

Application		A software program that is not an integral part of the operating system.
	Service	An application that normally executes at operating system startup. A service often accepts network connections.
	Database	A database application.
	Backdoor	An application, visible on a host, that listens for network connections and can give a non-authorized user control over that host.
	DoS Client	A host that is displaying an application that can participate in a (possibly distributed) denial-of-service attack.
	Peer to Peer	An application that listens for, and establishes network connections to, other installations of the same application (e.g., Kazaa, Morpheus, Napster).
	Virus	A host that is displaying a replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A host that is displaying a self-replicating program that spreads itself automatically over the network from one computer to the next.
	Resource	An operating system resource that is characteristically limited in its supply.
Resource	File	A long-term storage mechanism (e.g., files, directories, hard disks, etc.).
	Process	A single executable module that runs concurrently with other executable modules.
	Interface	An interface to the network.
	Interface Tunnel	Packaging a lower network protocol layer within a higher layer (e.g., IPSec Tunnel, HTTP tunneling).
	Registry	The central configuration repository for the operating system and the applications. Application-specific information is not stored here.
	CPU	Events directed at this object relate to consumption or use of the overall processing power of the host.
	Memory	Events directed at this object relate to consumption or use of the overall memory of the host.
Network		Events that cannot be clearly associated with a host's subitem. Events that involve transport, or many hosts on the same subnet.
Routing		Routing related events such as BGP.

	Switching	Switching related events such as VLANs.
Actor	User	A single human identity.
	Group	A named collection of users, such as an employee division or social group.
Vector		The replication path for a section of malicious code.
	Virus	A replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A self-replicating program that automatically spreads itself across the network, from one computer to the next.
	Backdoor	An application that listens for network connections and can give a non-authorized user control over that host.
	DoS Client	An application that will participate in a (possibly distributed) denial-of-service attack.

Behavior Category

Access		Refers to accessing objects, as in reading.
	Start	The start of an ongoing access, such as login.
	Stop	The end of an ongoing access, such as logging out.
Authentication		Actions that support authentication.
	Add	Adding new authentication credentials.
	Delete	Deleting authentication credentials.
	Modify	Modifying authentication credentials.
	Verify	Credential verification, such as when logins occur.
Authorization		Authorization-related actions.
	Add	Adding a privilege for the associated object (e.g., a user).
	Delete	Removing a privilege for the associated object (e.g., a user).
	Modify	Modifying the existing privileges for the associated user or entity.
	Verify	An authorization check, such as a privilege check.
Communicate		Transactions that occur over the wire.
	Query	Communicating a request to a service.
	Response	Communicating a response to a request, from a service.

Create		Seeks to create resources, install applications or services, or otherwise cause a new instance of an object.
Delete		The reverse of creation events. Includes uninstalling applications, services, or similar activity.
Execute		Involves loading or executing code, booting or shutting systems down, and similar activity.
	Start	The beginning of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.
	Stop	The termination of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.
	Query	A query sent to a specific entity - but not over the network (e.g., as when generating a report).
	Response	The answer returned by an Execute/Query. For example, a report delivered back from an application, or status messages from applications.
Modify		Involves changing some aspect of an object.
	Content	Changing the object's content, such as writing to or deleting from a file or database.
	Attribute	Changing some attribute of an object, such as a file name, modification date, or create date.
	Configuration	Changing an object's configuration. For example, application, operating system, or registry changes.
Substitute		Replacing files, upgrading software, or service or host failovers.
Found		Noticing an object or its state.
	Vulnerable	An exploitable state that is characteristic of a particular hardware or software release.
	Misconfigured	An exploitable state caused by a weak configuration or similar mishandling.
	Insecure	An exploitable state that arises from poor management or implementation. For example, weak authentication, weak passwords, passwords passed in the clear, default passwords, or simplistically named accounts.
	Exhausted	The targeted object was found to be exhausted (e.g., not enough file descriptors available).

Outcome Category

These attributes indicate the probable success or failure of the specified event, within an overall context. For example, the outcome of an event such as an "operation failed" error message can be reported as a "/Success" given that the operation can be presumed to have actually caused a failure. Another example would be an event that identifies a Code Red infection: on a host running Linux the outcome would be "/Failure" (Code Red is

Windows-only) while the same event directed at a host with an unknown OS would be reported as an "/Attempt".

Attempt	The event occurred but its success or failure cannot be determined.
Failure	The event can be reasonable presumed to have failed.
Success	The event can be reasonable presumed to have succeeded.

Device Group Category

Application		An application program.
Assessment Tool		A network- or host-based scanner that monitors issues such as vulnerability, configurations, and ports.
Security Information Manager		A security-event processing correlation engine (e.g. the ESM Manager). This "device" deals only in correlated events.
Firewall		A firewall.
IDS		An intrusion-detection system.
	Network	A network-based intrusion-detection system.
	Host	A host-based intrusion-detection system.
	Antivirus	An anti-virus scanner.
	File Integrity	A file-integrity scanner.
Identity Management		Identity management.
Operating System		An operating system.
Network Equipment		Network equipment.
	Router	A network device with routing (layer 3) capabilities.
	Switches	A network device with switching (layer 2) capabilities.
VPN		A virtual private network.

Technique Category

Traffic		An anomaly in the network traffic, such as non-RFC compliance.
	Network Layer	Anomalies related to IP, ICMP, and other network-layer protocols.
	IP Fragments	Fragmented IP packets.
	Man in the Middle	A man-in-the-middle attack.

Exploit	Transport Layer	Spoof	Spoofing a source or destination IP address.
		Flow	A problem in network-layer communication logic, such as an out-of-order IP fragment.
			Anomalies related to TCP, UDP, SSL, and other transport-layer protocols.
		Hijack	Hijacking a connection.
		Spoof	Spoofing a transport layer property (e.g., a TCP port number, or an SSL entity).
		Flow	A problem in TCP connections or flows, such as a SYNACK without SYN, a sequence number mismatch, or time exceeded.
	Application Layer		Application-layer anomalies.
		Flow	A peer does not follow the order of commands.
		Syntax Error	A syntax error in an application-layer command.
		Unsupported Command	A command which does not exist or is not supported.
	Vulnerability	Man in the Middle	A man-in-the-middle attack on the application layer.
			Exploiting a vulnerability (e.g., a buffer overflow, code injection, or format string).
		Weak Configuration	Exploitation of a weak configuration. This is something that could be remedied easily by changing the configuration of the service (e.g., weak passwords, default passwords, insecure software versions, or open SMTP relays).
		Privilege Escalation	A user identity has received an increase in its user privileges.
Brute Force	Directory Transversal		A user identity is attempting to browse or methodically review directories for which it may not have appropriate privileges.
			Brute-force attacks.
			Continued trials for logins.
Redirection	URL Guessing		Continued trials for URLs to access information or scripts.
			Redirecting an entity.
	Routing Protocols	ICMP	ICMP redirects.
		DNS	Unauthorized DNS changes.
			Attacks aimed at routing protocols (e.g., BGP, RIP, OSPF).

Code Execution	IP	Redirection using the IP protocol (e.g., source routing).
	Application	Redirection attacks on the application layer (e.g., cross-site scripting, mail routing, or JavaScript spoofing).
	Trojan	Either the execution or transmission of executable code, or the transmission of a distinctive response from executed code.
	Application Command	The code in question is concealed within other code that serves as a Trojan Horse. In other words, it appears to be one thing (that is safe) but is really another (which is unsafe).
	Shell Command	The code in question is intended to invoke an application command.
	Worm	The code in question is intended to be executed in a shell.
	Virus	Code associated with a worm.
Scan	Port	Code associated with a virus.
	Service	Any type of scanning. A network, host, application, or operating system scan can be identified through the specified object.
	Host	Multiple ports are scanned.
	IP Protocol	A service is scanned (e.g., DDoS client discovery, backdoors, RPC services, or scans for a specific application such as NMB).
	Vulnerability	Scanning for hosts on a network.
	DoS	A search for responding protocols. Note that TCP and UDP are not the only transport protocols available.
	Information Leak	A scan for vulnerabilities.
Policy	Covert Channel	A DoS attack is in progress.
	Breach	Information leaking out of its intended environment (e.g., mail messages leaking out, system file access, FTP data access, or web document access).
	Compliant	Leakage was detected from a covert channel, such as Loki.
		Policy-related violations such as pornographic web site access.
		A policy-related security breach occurred.
		A policy-compliant event occurred.

Significance Category

Compromise	A potentially compromising event occurred.
------------	--

Hostile	A malicious event has happened or is happening.
Informational	Events considered worthy of inspection; for example, those produced by polling.
Error	An execution problem.
Warning	A possible problem.
Alert	A situational problem that requires immediate attention.
Normal	Ordinary or expected activity that is significant only for forensic purposes.
Recon	Relates to scans and other reconnaissance activity.
Suspicious	A potentially malicious event occurred.

Custom Event Categorization


Events received from ArcSight ESM supported devices are automatically **categorized** (appended with classification information) by ArcSight SmartConnectors per the ArcSight event categorization taxonomy. Event [Categories](#) are used to classify events based on criteria such as object type, behavior, outcome, technique, device group, and significance. This additional information about an event (together with normalization and other filtering) helps to identify the significance events from different devices and vendors based on a consistent model.

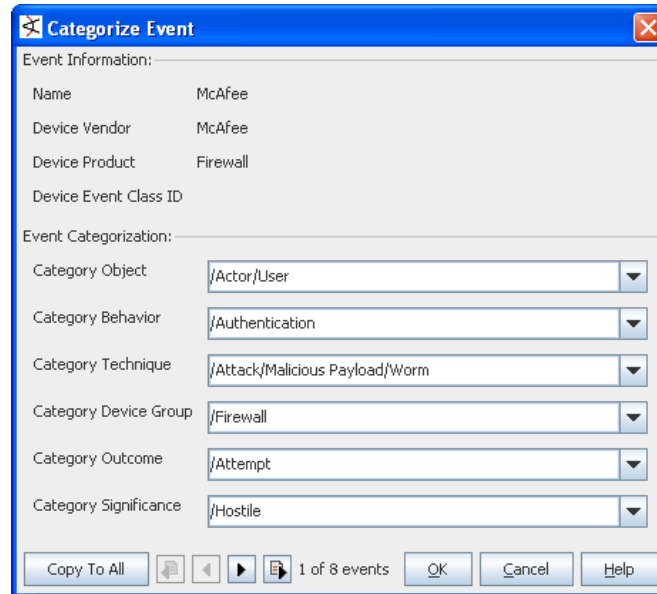
However, events from unsupported or custom devices can generate events that the provided connectors do not know how to categorize. For example, if your organization has developed and deployed ArcSight FlexConnectors to collect and process events specific to customized network nodes, these "custom" events will not be categorized per the usual method.

From the ArcSight ESM Console, you can manually apply categorization to one or more custom events from a FlexConnector (or other custom or unsupported device). Once you apply categorization to events from a particular device (and its associated connector), the categorization is automatically applied to other events of the same type.

To apply event categorization to one or more events:

- 1 Select one or more of the same type of events that you want to categorize.

- 2 Choose Select one or more events and choose the **Categorize Event** command from the System menu (or click the  toolbar button).



- 3 Select values from the given categories from the drop-down menus.
- 4 Click **OK** to apply the categorization information to events of this type.

This generates a SmartConnector update file (**.aup**) containing the new categorization files on the ArcSight ESM Manager. The Manager polls for new SmartConnector update files every 5 minutes, and updates the SmartConnectors when it finds new **.aups**. So, within 5 to 20 minutes after you apply event categorization, new events of the same type will be categorized in the same way.

Note that if a certain type of event is already categorized, this custom categorization will have no effect. If not, the custom categorizations will take effect on all events of the same type going forward.

Collaboration

The ESM Console collaboration capability is a collection of features that make it possible for analyst teams to select certain security events for further on-going investigation. Investigation involves a workflow-style process of information collection that leads through a series of analysis stages to a final disposition.

In the Console, you locate events for analysis through the active channels in the Viewer panel. You use the Annotate Events dialog box or the Event Inspector to annotate an event, or collection of events, and set it up for follow-on analysis. Once you have placed the event or collection in the collaboration "pipeline" by assigning it a disposition stage (such as **Initial**), you or other analysts manage it through to resolution using the assigned stages as filter arguments.

ArcSight provides a set of default collaboration stages, but your enterprise may well use others created specifically for your workflow needs. Owners, disposition stages, comments, and other factors change as an event's handling progresses. The collaboration cycle usually ends when someone marks the event's **Stage** field as **Closed** (or the equivalent).

Compare collaborative annotation to cases, which are a more formal way to track sets of events that are under investigation.

Default Collaboration Stages

Stage	Meaning
Queued	The event has not yet been inspected.
Initial	The event has been inspected.
Follow-up	The event is under investigation.
Final	The investigation has concluded.
Closed	The investigation is closed.
Monitoring	The event is being watched, especially in regard to a reoccurrence in support of a pattern.
Rule Created	The event has been used to create a rule that assists in monitoring for a reoccurrence, especially in regard to patterns, and potentially to respond in some way such as with a notification.
Flagged as Similar	The event is similar to one already under investigation.

Please see [“Collaborating on Events” on page 141](#) for descriptions of the tasks involved.

Common Conditions Editor

The ArcSight ESM [Console](#) has a Boolean logic editor, which is also referred to as the Common Conditions Editor (CCE). If the criteria are met, the evaluation returns a Boolean true/false. All conditions constructed by the CCE are expressions that consist of a value or variable on the left, an operator (not, and, or), and a value on the right, for defining the conditions you use to help analyze resources such as filters, rules, and reports. This topic is your reference for using the CCE, wherever it appears.

See also [“Filtering Events” on page 147](#), especially subtopics on [“Creating Filters” on page 147](#) and [“Debugging Filters to Match Events” on page 151](#).

Editor Features

The CCE has two tabs; **Edit** and **Summary**. In the **Edit** tab, logical operators are represented in a tree form.

In the **Summary** tab, conditions are presented in an easily readable, summary view. Resource references in the **Summary** tab are hyperlinked. (From the Summary tab, click a resource link to open its definition in a resource editor in the Inspect/Edit panel.)

Conditions are editable only on the **Edit** tab. Wherever the CCE appears, you use these features to build or change conditional expressions.

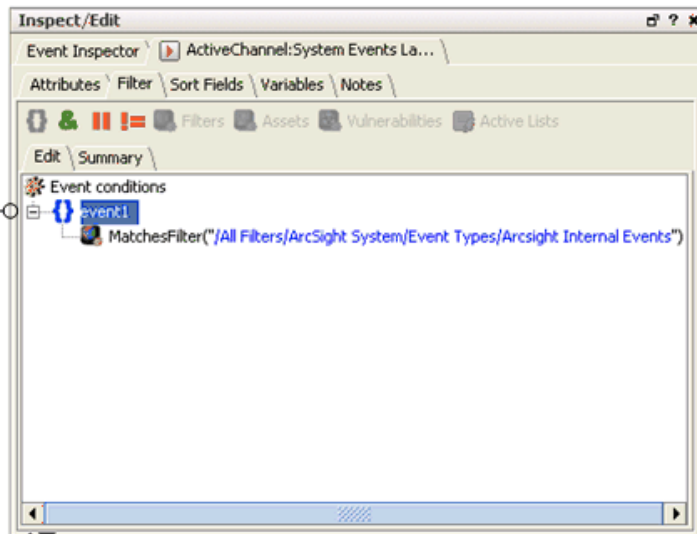
- The condition tree shows the complete set of expressions you are building or changing.
- The root of the tree indicates whether the expression concerns [Filters \(Filter By\)](#), [Correlation \(Correlate\)](#), or [Reports \(Report On\)](#), as you see in the Filters Editor, Rules Editor, or Report Editor, respectively.

- From the root, there are branches for one or more [Events](#). For each event branch, there are sub-branches for one or more condition statements.
- To add an event for a rule, select the root and click the **New Event Definition** button (see below) or right-click the root and choose the same command. Note that only rules can add events because filters and reports do not need additional events for correlation.
- To act on a specific event or [Conditional Statements](#), select it in the tree. Once selected, you can use several features to modify it, as described here and below.
- Use the new event, [Logical Operators](#), and resource selector buttons above the tree to add events, operators, or resource-based constraints to condition statements, if applicable.
- Use the right-click menus that are available for any selected branch of the condition tree to choose commands that are applicable to that statement in that context.
- When you use the right-click **Edit** command to edit a selected statement directly in the tree (rather than through the event fields table), you can use the Enter key to update the condition without having to click **Apply** or **OK**.
- Do use single- or multiple-selection copying and pasting of statements for efficiency. You can use the right-click menu commands or **Ctrl+C** for copy, **Ctrl+X** for cut, and **Ctrl+V** for paste.
- Use the [Field Sets](#) selector to choose an appropriate group of event fields when an event-related statement is selected in the condition tree.
- To **undo/redo** an action, right-click in the Edit panel and choose either **Undo** or **Redo**, depending upon the action you want to use. For example, if you decide to delete a node, a message asks you to confirm. If you want to undo this delete, right-click in the Edit panel and choose **Undo Delete**. (You can also use the standard keyboard commands **Ctrl+Z** for undo and **Ctrl+Y** for redo.)
- To **Search** for a resource, simply click in the field column (on the left side of the list) and start typing. A Search popup is displayed when you start typing, and shows the term as you type it. The search is "predictive" in that it will navigate to and select matching fields as you type. Click **Enter** to select this resource. For details see ["Searching for Fields in Event Inspector, Resource Editors or CCE"](#) on page 68.

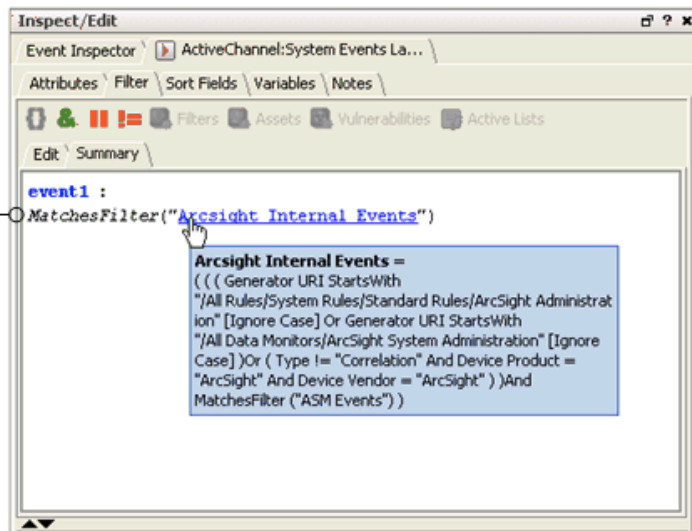


Both tabs provide syntax and error highlighting. As an example of error highlighting, if a condition uses resources that are later removed, references to the missing resources will be highlighted as errors in the condition statements in the CCE.

In the **Conditions "Edit"** tab, logical operators are represented in a tree form. Use this tab to define and edit conditional statements.













In the **Conditions "Summary"** tab, conditions are shown in an easily readable, summary view. In this view, resource references are hyperlinked. Click on the links to go to a resource definition. Use this tab to review condition statements. You cannot edit the Condition on this tab.



Condition Tree Command Buttons

All of the following options are available from buttons at the top of the Conditions Editor and also from right-click menu options. The exception is "In Case" Condition which is only available from a right-click menu option.

Button	Name	Use
	New Event Definition	Insert a new condition tree in the editor.
	AND	Insert an AND condition.

Button	Name	Use
	OR	Insert an OR condition.
	NOT	Insert a NOT condition.
	New "Matches Filter" Condition	This resource-based command browses the Filters tree of the Navigator panel. Note that this operator applies only to rules.
	New "Assets" Condition	This resource-based command browses the Assets tree of the Navigator panel. Note that this operator applies only to rules.
	New "Categories" Condition	This resource-based command browses the Categories tab of the Navigator panel's Assets tree.
	New "Has Vulnerability" Condition	This resource-based command browses the Vulnerabilities tree in the Navigator panel.
	New "InActiveList" Condition	This resource-based command browses the Navigator panel's Active Lists tree.
	New "InCase" Condition	This resource-based command browses the Navigator panel's Cases tree. Note: This option is only available from a right-click menu option. There is no button for it.
	New "Join" Condition	Inserts a JOIN condition. Note: This option applies only to Rules.

Condition Tree Context Menu Commands

Command	Description	Applies To
New Condition	Add a new condition statement below the selected element. Type the statement directly in the tree or choose a field from the pop-up menu.	operator, event field
New Logical Operator	Add a new logical operator to the selected element. (See "Logical Operators" on page 727.)	Event alias, operator, event field
New Constant Condition	Add a Boolean (True/False) AND operator to the selected branch.	operator
New "Matches Filter" Condition	Use the Filter selector to identify a particular filter as a matching argument for a condition.	operator, event field
New "Assets" Condition	Use the Assets selector to identify an asset or group as the argument for a condition.	operator, event field
New "Has Vulnerability" Condition	Use the Vulnerability selector to identify a vulnerability as the argument for a condition.	operator, event field

Command	Description	Applies To
New "InActiveList" Condition	Use the Active List selector to identify a particular active list as the argument for a condition. Tip: Remember that rules that use InActiveList will be constrained by the types of fields used in the active lists you have selected. For example, if an active list field is of the Resource Reference type, it can only refer to other fields containing resource references, not integers or strings.	operator, event field
New "InCase" Condition	Use the Cases resource tree to identify a particular case as the argument for a condition.	operator, event field
New Event Definition	Create and name a new event alias to add to the root. Note: This option applies only to Rules.	root
Set Alias Expiration Time	For rules, set the amount of time that a qualifying event for this alias (only) will be retained in memory for evaluation, based on Manager receipt-time. See "Specifying Rule Thresholds and Aggregation" on page 308 for more information. Note: This option applies only to Rules.	event alias
Set Global Expiration time	For rules, set the amount of time that qualifying events for all aliases will be retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. See "Specifying Rule Thresholds and Aggregation" on page 308 for more information. Note: This option applies only to Rules.	root
Edit	Open a text box in which to change the selected element.	operator, event field
Undo	Undo an action.	all actions
Redo	Redo an action.	all actions
Cut	Cut the selected elements of the condition tree to the Clipboard.	root, event alias, operator, asset, event field
Copy	Copy the selected elements of the condition tree to the Clipboard.	root, event alias, operator, asset, event field
Paste	Paste the conditional element currently on the Clipboard to the end of the selected element in the tree.	root, event alias, operator, asset, event field
Delete	Delete the selected elements of the condition tree.	event alias, operator, asset, event field
Set Matching Time	Sets the maximum time difference between the partially-matched aliases. Note: This option applies only to Rules.	matching event operator

Command	Description	Applies To
Print Conditions and Tree Summary	Prints the condition definition as shown on the Edit tab and the Summary statement. Selecting this menu option brings up a Print Preview dialog where you can view what will print, and set printer options.	event alias, operator, asset
Help	Open the online Help system for information about the type of resource being edited.	root, event alias, operator, asset, event field

Adding Conditions

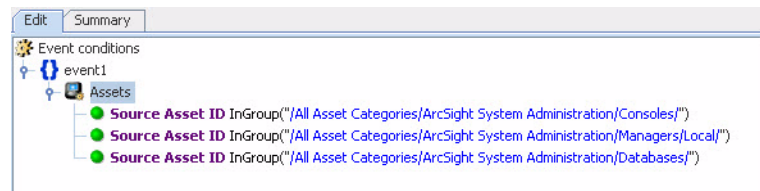
When adding conditions, you have to decide how the new condition will tie to existing conditions. If And is used, the new condition has to occur in addition to existing conditions. If Or is used, the new condition or any existing conditions have to occur. If Not is used, all but the new condition has to occur.

You use the AND, OR, and NOT operators to define relationships between condition statements. When you use AND, the new condition must occur in addition to the selected condition. Using OR means either the selected or new condition must occur. Using NOT means all but the new condition must occur.

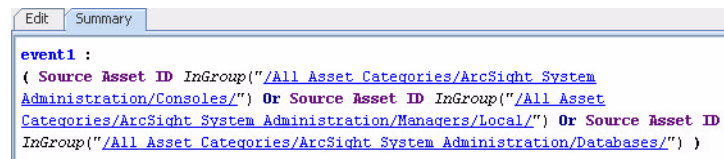


Multiple assets and asset categories added to a single asset condition are always OR'ed together (not AND'ed).

For example, create a new rule, click the **Conditions** tab in the Rule Editor, select **Assets**, and add some asset categories to the condition. (To do this, select them on the Asset Categories tab at the bottom of the Editor and click **Apply**.)



Now click the **Summary** tab to view the detail of the Boolean logic. This shows that the assets are OR'ed together.



If you want to AND an asset condition to other conditions, go back to the **Edit** tab, select the event definition again, and add other conditions based on the fields shown in the lower half of the editor.

To add more condition statements, right-click an existing statement and choose **New Logical Operator**, then **And**, **Or**, or **Not**, or click a logical operator or resource-selection button. Then, create the new condition statement.

Event-definition and Join conditions are allowed (only) with rules to include separate "events" or aliases, or correlation of these separate "events" respectively.

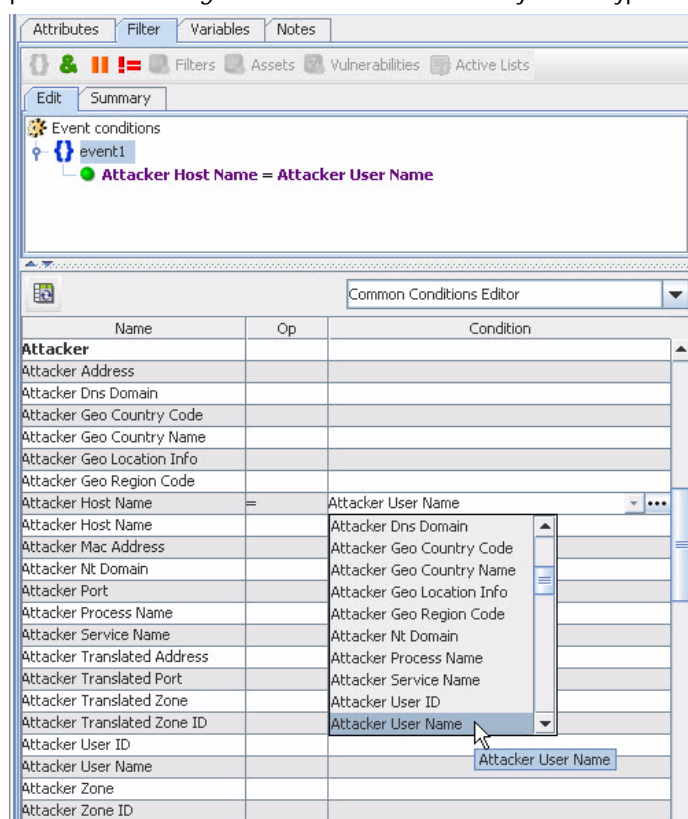
In the data field table, scroll to a data field in the Name column to create a condition statement.

Data fields provide event details from all devices deployed throughout your enterprise. Event details from these devices are normalized into common data fields and stored in the ArcSight Database to allow investigative and analytical comparison of all incoming events. See [“Data Fields” on page 633](#) and [“Timestamp Variables” on page 780](#) for more information.

The data field table displays a **Name**, **Operator**, and **Condition** column. These three columns are combined to create `<data field> <logic operator> <data field value>` condition statements. For example, if monitoring a Cisco Router, you could define a condition statement to specify `Device Product = Cisco Router`: `Device Product` as the data field, equals (=) as the logic operator, and `Cisco Router` as the data field value.

Field Comparisons with Variable or Static Values

Starting with ESM v.4.5, for any field comparison, a drop-down menu of variables is provided for the *right* side of the statement. Or you can type a value here.



Previous to ESM v.4.5, the Common Conditions Editor (CCE) accepted only constant (i.e., *static*) values on the right side of the condition, and you always had to type the right-side value.


In ESM v.4.5, the CCE is enhanced in that field comparisons now provide the ability to compare one field to another field (e.g., `AttackerHostName = AttackerUserName`).

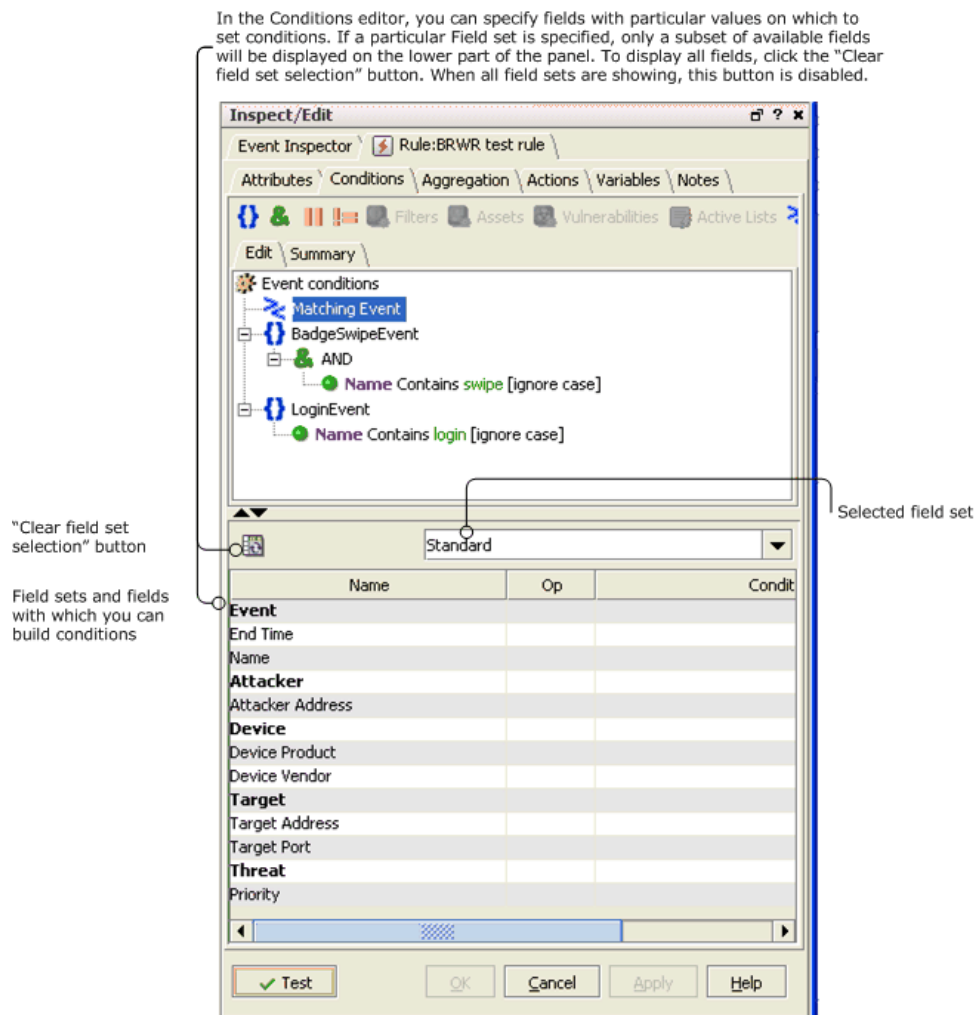
This functionality is available on the Console wherever the CCE is available (in [Rules](#), [Reports](#), [Filters](#), and so on).

Left -side event attributes can be compared to right-side conditions (represented as variables or static values) using operators like equals (=), is not equal to (!=), is less than or equal to (<=), is greater than or equal to (>=), is less than (<), is greater than (>), and so forth.

Using Field Sets

The Common Conditions Editor provides access to all available [Field Sets](#). You can specify fields with particular values as part of conditions statements. See also [“Using Field Sets” on page 101 in Chapter 7, Monitoring Events, on page 91](#).

You can select a particular field set, which limits the fields shown to a subset of all available field sets. If you cannot find a field, click the "Clear field set" button  to clear the field set selection and show the complete list of field sets.



For example, suppose you define a condition to look for two matching events; one in which Event Name contains "swipe" and another in which Event Name contains "login". You can set this condition with the "Standard" field set shown above because it includes the Event Name field in the list of available fields from which to choose. But if you wanted to add conditions based on an Event field for "Correlated Event Count" or Threat field for

"Model Confidence", you would need to clear the Field Set and view all fields to get access to these fields.



Fields shown in italics are *derived* from data in other fields. Derived fields show up in various places on the Console UI including on the Field Set editor, and the Common Conditions Editor (CCE) aggregation tabs (e.g., Rules, Filters, and so forth).

Testing for Zone Relevance

Events include several [Data Fields](#) that are related to zones (see "[Assets](#)" on page 581). In the Common Conditions Editor you can compare these fields with asset groups or categories, to test whether the field's event does or does not correlate with those asset properties. This comparison is performed by the **InGroup** operator.

For example, if an event's Attacker Zone field value and a Source Asset ID's System Asset Categories' Criticality value correlate, then the InGroup operator would test True. You can apply this outcome in your reports, rules, or filters.



The InGroup operator is inserted automatically when you create zone-asset correlation statements in the Common Condition Editor. There is no button or command to manually insert it.

The InGroup operator tests True for specified asset resources and their parents but not for their own peers or their parent's peers.

- 1 In the Conditions tab of any appropriate editor, set a logical operator for a zone-related field (e.g., Destination Zone).
- 2 In the same field, click the ellipses button (...). In the Select a Zone dialog, enter a prompt for the condition, select the **Parameter** check box, then choose a zone from the resource tree.
- 3 Right-click the new statement in the editor and choose **AND**, then right-click the AND statement and choose **New Assets Condition**.
- 4 In the Asset resources panel below, choose the Source, Target, or other type of relevant asset ID.
- 5 For that asset ID type, click the **Assets** or **Asset Categories** tab and select an asset group or category to test with the InGroup operator.
- 6 Click **Apply** in the Assets resources panel to add the asset group or category to the condition statement, with the embedded Ingroup operator.

How to Create a Matching or Join Rule

A matching or join condition is a condition statement that joins two data fields together with the Matching or Join condition logic operator on the Conditions Tab. Creating matching or join conditions using data fields provides the flexibility of creating conditions without knowing the specific data field's values. The following join data field conditions can be created:

- Same data field for two events: `EventOne <data field A> <logic operator> EventTwo <data field A>`. For example, `EventOne Source Address = EventTwo Source Address`. In this example, both event data field must have the same value. This rule is useful when monitoring activity from an unknown Source Address that is generating numerous events.

- Different data fields for two events: `EventOne <data field A> <logic operator> EventTwo <data field B>`. For example, `EventOne Source Address = EventTwo Target Address`. In this example, the Source Address of the first event must equal the Target Address of the second event.
- Different data fields for the same event: `EventOne <data field A> <logic operator> EventOne <data field B>`. For example, `EventOne Source Address = EventOne Target Address`. In this example, the Source Address must equal the Target Address of the same event.



There is a relatively high memory cost for join rules with low-selectivity join conditions (such as same source IP or same target IP). Just like queries in SQL, the more selective the conditions (the conditions on the individual events as well as the join conditions), the less memory it will take to execute, because fewer conditions will match.

When authoring a rule you should order conditions on the events to be correlated (or joined) by placing the most restrictive conditions first, for example, adding join conditions like `"event1's Source Address = event2's Source Address"` or `"event2's Detect Time > event1's Detect Time"`. This will dramatically reduce the memory consumption by the Cross-Correlation Engine, as much as 50% in some cases.

Conditional Statements

This table offers sample conditional expressions you can create using various operators, event fields, and data types.

ArcSight Data Types	Description
Number or Integer	Using numeric (integer) fields, you can specify operators including <code>=</code> , <code>!=</code> , <code><</code> , <code><=</code> , <code>>=</code> , <code>></code> , and <code>In</code> to specify a numeric comparison expression, for example: <code>CustomNumber1 = 50</code> . To use <code>In</code> , you can specify any number of comma-separated values to match (or equal).
String	Using string fields, you can specify operators including <code>=</code> , <code>!=</code> , and <code>In</code> , <code>Contains</code> , <code>Matches</code> , <code>Starts With</code> , <code>Ends With</code> , and <code>Like</code> to define a string comparison expression. For example: <code>ArcSightCategory StartsWith /Attack or ArcSightCategory = /AttackSuccess</code>

ArcSight Data Types	Description
DateTime	<p>Using datetime fields, you can specify operators including <code>=</code>, <code>!=</code>, <code>Between</code>, <code>In</code>, and <code>On</code> to specify a datetime comparison expression. For example: <code>DetectTime Between 4/1/03 11:30:01AM, 4/1/03 4:30:01PM</code>.</p> <p>You can enter datetime values directly or click the ellipsis (...) button to select a date from a pop-up calendar or a special date keyword list. Special date keywords you can use are: <code>Now</code>, <code>1 or 2 hours ago</code>, <code>1 or 2 days ago</code>, <code>1 or 2 weeks ago</code>, or a replay start and end time. You can also use special system variables such as:</p> <ul style="list-style-type: none"> • <code>\$CurrentDateTime</code>: for the date and time the report is run; the system variable is replaced by the current date and time value." • <code>\$CurrentDate</code>: for the date the report is run; the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run. <p>You can specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: <code>\$CurrentDate - 7d</code> for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or <code>\$CurrentDateTime - 12h</code>, which evaluates to the current date time minus 12 hours.</p>
IP Address	<p>Using IP address fields, you can specify operators including <code>=</code>, <code>!=</code>, <code>In</code>, <code>InSubnet</code>, and <code>Between</code> to specify an IP comparison expression. For example: <code>TargetAddress = 178.168.11.211</code>. With the <code>In</code> operator, you can also specify a comma-separated list of IP addresses to match and, with <code>InSubnet</code>, can also specify IP address ranges in CIDR format, or use <code>InSubnet</code> to specify an range of addresses in a specific subnet.</p>

These same rules apply to the conditions editor used in defining rules, creating conditional reports, and filters.

ArcSight Variables

You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as `$Now` and `$CurrentDateTime`. The same is true for time elements, including `s` (second), `m` (minute), `d` (date), `M` (month), `w` (week), and `y` (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign; e.g., "Source Address" would be `$sourceAddress`. Please see the complete discussion in the topic ["Variables" on page 784](#).

Conditions

Conditions are logical expressions (see [Logical Operators](#)) used to qualify [Events](#) or other grouping of elements. Conditions can be specified in a number of places using a common condition editor; for example, to define rules or filters.

Parameterized Conditions

Some conditions can be parameterized, for example in reports, where the exact value specified for a condition match is provided at the time of running the report, through a

parameter pop-up box. This lets report authors give default parameter values, which can be overridden by the user running the report.

Name	Value
Report Parameters	
* Start	8/17/05 4:32:37 PM
* End	8/17/05 5:32:37 PM
Common	
Report File Format	PDF
Report Page Size	Letter [8.5x11 in]
Run Report as	Select a User
Filter results by	Select a Filter
Email To	
Email Format	Send URL

☐ Save Report Output

Figure 22-4 Report Parameters Dialog

This is a convenience for people running the report as it does not require write permissions while running the report, but effectively provides the same flexibility as being able to modify the report. Note that when defining parameters for detect time, you should always include a BETWEEN condition so that the report is limited to a certain time range, and does not scan the entire event table. Otherwise, it can severely impact the ArcSight ESM Manager information-retrieval performance.

- 1 You can select the ellipsis (...) button and then select the **Parameter** check box to create a parameter prompt for selected data fields of a report. When users run the report, they are first prompted to enter values for these parameters. When specifying a report parameter, you can define the prompt that is displayed to users, as well as specify a default value that is displayed in the prompt field.
- 2 In the case-sensitive column (**Aa**), select the check box if the data field needs to be case-sensitive.
- 3 In the negate condition column (the "No" symbol), select the check box to change conditions to **all but this** statements.

For example, if the condition statement is Device Product = Cisco Router and the negate condition check box is selected, all events but those from the Cisco Router will generate a correlation event.



Some conditions can be parameterized such that the exact value is provided at the time of running the report through a parameter pop-up box. This lets report authors give default parameter values, which can be overridden by the user running the report. This is a very useful convenience for people running the report as it does not require write permissions while running the report but effectively provides the same flexibility as being able to modify the report. Note that when defining parameters for detect time, you should always include a BETWEEN condition so that the report is limited to a certain time range, and does not scan the entire event table. Otherwise it can severely impact the performance of ESM Manager, retrieving information from the database.

- 4 Click outside the data field row.

The condition statement (<data field> <logic operator> <data field value>) appears as a branch under the logical operator.

- 5 On the Conditions tab, click **OK**.

These same rules apply to the conditions editor used in creating other ESM resources such as rules and reports.

Console

The ArcSight ESMConsole is a centralized view into an enterprise. A graphical user interface that provides centralized intelligent real-time monitoring to secure your enterprise.

Console settings consist of your color selections, preferences, temporary filters, window sizes, etc., and are saved in a `.ast` file. The current setting file you are using is displayed in the Console title bar (by default, `machine:username.ast`). You can perform operations to save or load `.ast` files stored locally, on the same machine where Console is installed, on save or load `.ast` files stored and maintained by the ESM Manager. After settings are saved in a file, the `.ast` file is listed in the File menu. The File menu lists the last four `.ast` files that have been accessed.

Concerning Console-Manager connections, you may want to note that while each ESM Manager connects to many Consoles, each Console connects to only one Manager. Also, when a Console is connected to a Manager, it affects only that Manager, regardless of how that Manager may be linked within a larger ESM Manager hierarchy.

See related topics [Chapter 6, Working in the Console, on page 57](#) and [Chapter 21, Personalizing the Console, on page 555](#).

Content

ArcSight ESM provides preconfigured [Resources](#), also known as *content*, in the form of [Packages](#). Content packages are automatically installed as a part of ESM to provide out-of-box resource suites that you can start using immediately to monitor and protect your network. Also, you can develop your own custom content with the editors and tools provided in ESM.

Content Packages

ArcSight ESM ships with system content already developed that addresses common security and regulatory use cases. These use cases combine many ESM resources to address multi-faceted issues. You can use system content as is, or modify it with data specific to your network environment.

Starting with ArcSight ESM version 4.0, system content is delivered as packages. (See [“Packages” on page 731](#).) System content packages are automatically installed as a part of ArcSight ESM to provide out-of-box resource suites that you can start using immediately to monitor and protect your network. (See also [“Resources” on page 746](#).)

The content packages provided with a standard installation of ArcSight ESM are:

- ArcSight Administration
- Configuration Monitoring
- Intrusion Monitoring
- Network Monitoring

■ Workflow

Custom Content

The term "custom content" refers to resources and solutions created by customers using ArcSight ESM software. Examples of custom content are user-configured [Rules](#), [Filters](#), [Active Channels](#), [Queries](#), [Trends](#), and [Reports](#) designed to address customer-specific scenarios.

SmartConnector Content

ArcSight continuously develops new SmartConnector event categorization mappings, which are often called "content." All existing content is included with major product releases, such as a v3.0, v3.5, or v4.0 but it is also possible to get regular content updates to stay completely current.

Following the release of ArcSight v3.0 SP1, ArcSight began making available to subscribing customers downloadable packages of new SmartConnector content. These releases occur frequently, generally on a weekly or bi-weekly basis. The download files are offered through a special subdirectory on the ArcSight software server. This directory is visible only to subscribers, who receive a notification e-mail from ArcSight Customer Support when the files are posted.

The content is packaged in [.aup](#) (connector update) files which may be wrapped in [.ZIP](#) files for transmission convenience. You place these [.aup](#) files in the ESM Manager's [/updates](#) directory, where the Manager automatically finds the content and pushes it to the SmartConnectors. The affected SmartConnectors each register an internal event when the update occurs and can notify you by e-mail through the Manager.

This automatic updating feature is part of v3.0 GA and later SmartConnectors and Managers.

You arrange for a content subscription through ArcSight Customer Support. Subscribers also have access to related articles in the ArcSight Customer Support Center's KnowledgeBase.

Correlation

Logically linking events based on multiple conditions.

See [Chapter 15, Identity Correlation, on page 357](#) for more information on using session correlation.

See also, [Chapter 13, Rules Authoring, on page 301](#).

Correlation Rule

A programmed procedure that expresses conditions and actions, and evaluates normal or correlation events. A rule has two parts: a condition and an action.

A condition determines whether a state exists and satisfies related expressions. If so, an action expression defines the response to the condition.

A rule can have one or more conditions. If there is one condition, the rule acts as a filtering tool. If there is more than one condition, the rule acts as a correlation tool. A rule can be

created for any incoming event from one or more event generators, with various conditions, logic statements, and thresholds.

See [Chapter 15, Identity Correlation, on page 357](#) for details on using session correlation.

Customers

To support managed security service providers (MSSPs), and larger enterprises that need to track activity related to cost centers or divisions, ArcSight ESM has the ability to identify particular customers as the source of specific events.

"Customers" can be any client, tenant, or internal identity scheme you designate.

To use the Customers resource in ESM, you first model your existing customer or client base into the Customers resource tree in the Navigator panel, as described in ["Managing Customers" on page 551](#). Then, using the Customer URI values established in the resource tree, you configure the appropriate SmartConnectors to report these values through their Customer URI attributes.

Once you have implemented your Customer resource tree in the Console, and configured the relevant SmartConnectors to report these Customer URIs, you can apply the Customer resources as filter condition arguments.

For example, your Customers resource tree might include a branch that translates into a Customer URI of: [/All Customers/Brokerages/Central States/Kansas City/Jones&Co.](#)

In the SmartConnectors resource tree, for those connectors that apply to this customer, you would apply this same string as the value for those connectors' Customer URI attribute, found under the Network section of the **Connector: Default: Content** tab. Thereafter, events reported by those connectors can be filtered in or out by referencing that branch of the Customers resource tree.

Dashboards

A dashboard is a customizable view of the enterprise that summarizes event information by collectively managing one or more data monitors.

Data monitors are views within the dashboard that can be configured to report on events, filters, rules, and other data or information that is of particular interest to you. Data monitors can be arranged within dashboards in numerous viewing layouts.

When you right-click in a dashboard you can choose from these options.

Dashboard Context Menu Options

Option	Description
Save Dashboard	Save any changes you have made to the dashboard and its data monitors.
Save As	Save the configured data monitors and dashboard under a different name.
Close Dashboard	Close the dashboard and remove it from the Viewer panel.

Option	Description
Dashboard>Zoom In / Zoom Out / Fit in	Visually enlarge or reduce the data monitors presented in the Viewer panel. Size the data monitors to allow them to all appear simultaneously in the current Viewer panel.
Data Monitor>Edit	Edit the current data monitor in the Inspect/Edit panel.
Data Monitor>Disable	Turn off the current data monitor.
Data Monitor>Float / Minimize / Close	Float, minimize, or close the current data monitor.
Show>DataMonitorName	Restore minimized data monitors.
Show Details / Show Detailed Channels	Show the event details for the currently selected element in a data monitor graphic, such as a pie chart, or display each of the monitor's elements in detail in separate active channel grids. This is also called "drilling down."
Investigate	Create an active channel or filter condition based on the highlighted event. The Investigate command uses the event's attribute type (its column heading), and the particular event's field value (e.g., an exact IP address), to formulate filtered channels based on these two factors. The operators can include Create Channel [X = Y] and Add Condition [X = Y] to Editor .
Tools	Choose one of the network tools ESM provides to explore the origin of the selected event item.
Show Scroll Bar	Toggles a scrollbar on and off in the selected datamonitor. Use the scrollbar to show additional rows of tabular data if present.
Export > Data Monitor/Dashboard as ...	Save the selected data monitor or the dashboard in the JPEG (graphic), CSV (comma-separated value or text-based), or HTML file format.

Database

The ArcSight Database is a central repository for all events coming through ESM. Once an event occurs, its [Data Fields](#) such as severity, create time, rules triggered, and so forth are stored in the ArcSight Database. The ArcSight Database stores all enterprise events in a normalized schema. You can then investigate and analyze the event information. The ESM Manager is the only component that communicates with the database.

Schema Redesign

As of ArcSight ESM v.3.x, we have made several improvements in database schema, event field usage, and event categorization.

More Event Fields

As of ArcSight ESM version 3.0, the number of fields in each event was increased. This produced two key advantages:

- Most information reported by sensor devices moved from additional data into the main event fields.

This change made the information accessible from Rules, Filters, and Reports. It also enhanced the process of normalizing the information. For example, the events from a

supported sensor might include three different fields - encryption failure, encryption success, and error - that all contain messages. In the old model, these would have been mapped to additional data with three different tag names. In versions 3.0 and later, these three are all mapped to the 'message' field.

- Greater usage clarification for many fields.

As an example, the 'protocol' field in v2.5 was split into 'transport protocol' and 'application protocol'. And the field 'domain' was split into 'NT domain', 'DNS domain', and 'Device domain'. Because the previous fields could contain many different types of information, it could be difficult to write rules or data monitors that used the variety of possible values. The new fields, with their stricter definitions, are much more useful.

More Efficient Field Usage

Ordinarily, using more fields would cause ESM to occupy more disk space even more rapidly. However, a number of other changes mitigated this issue. The result is that ArcSight ESM events now consume significantly less disk space than events in pre-v.3.0 versions of ArcSight ESM, and provide much faster event storage and retrieval. The design changes that made this possible are:

- The database schema has been normalized so that highly repetitive sets of values are now stored in side tables.

Examples include the Connector and Device description fields. Normally, the values on these fields remain constant for days or weeks at a time. ArcSight ESM v3.x stores the set of values once and then includes a reference to the correct value set in the main event table.

- No single event uses all of the new fields.

Essentially, the v3.x schema defines a super-set of the most commonly used and useful fields presented by sensor events. It requires minimal space to store the empty fields.

- The original (or raw) log entry can also be preserved for each event.

This is controlled on a per-connector basis. This can be particularly useful in conjunction with Turbo Level 1 since a minimal event is generated but the details can still be inspected in the raw event, and with Turbo Level 2 where the data that would have appeared in the additional data table can now be found in the raw event.

- As a result of these changes, event storage and retrieval speeds have increased significantly.

These changes manifest in increased throughput capacity (a higher events-per-second ceiling), enhanced grid performance, and faster report runs.

More Precise Event Categorization

Starting with ArcSight ESM v3.x, events are categorized differently (see [“Categories” on page 606](#)). Before to ArcSight ESM v3.0, an event category was a single URI (such as [/Attack/BruteForce/Success](#)). On this basis it was difficult to include sufficient information to allow proper event correlation.

ArcSight ESM now categorizes events across six dimensions: the object acted on by the event, the action represented by the event, the technique used to achieve the action, whether or not the action succeeded, the security significance of the event, and the class of device that reported the event. While this new scheme is slightly more complex, it has already proven to make rule authoring and data monitor construction much easier.

For example, a Snort SID 103 ([BACKDOOR subseven 22](#)) event would have been categorized as [/Compromise/Backdoor](#) prior in the old model. Such a categorization

lacks detail. Was this an attempt to install a backdoor? Or does it indicate communication between a backdoor and an external connector? Or is an external connector scanning for pre-installed backdoors?

The new categorization model can bring more clarity to the situation. Events describe either an action or a state. Actions are attempted against a particular object and may succeed or fail. There may be many ways to attempt a particular action against an object (such as different ways to exploit an exposed vulnerability). States describe the status of a particular object, and these states may be known to be true -- or they may be hearsay. Events all have some significance to the security profile of the protected network. Finally, it is interesting to know what sort of device is reporting the event.

If we look at Short SID 103, we discover that it is a report of a scan searching for pre-installed subseven 22 backdoors. Now, we would categorize these events

Security Significance	/Recon
Behavior	/Communicate/Query
Technique	/Scan/Service
Device Type	/IDS/Network
Outcome	/Attempt
Object	/Host/Application/Backdoor

In this case, a network intrusion detection system (IDS) would observe an attempt to communicate with a backdoor and infer that this was part of a service scan attempting to discover pre-installed instances of that backdoor. Naturally, this implies an external connector is performing reconnaissance on the protected network.

Data Fields

The events that ESM processes are composed of several attributes, each of which is a data field with its own characteristics. These event-schema data-fields fall into the main groups shown below.

Each attribute has both a **Label** that you see in the Console and a unique **Script Alias** you use to refer to the attribute in filters, rules, or Velocity templates. The **Data Type** lets you know how to handle the attribute, and the **Default Turbo Level** indicates whether an attribute is, by default, classified as **1** (essential, or "fastest") or **2** (optional, or "faster"). Turbo Level 3 ("complete") isn't designated because it applies to additional data not represented here.

The easiest way to view all event fields is on the Event Inspector (Event tab) or [Common Conditions Editor](#) on the Console. (To bring up the Event Inspector select an event in a grid view like an active channel. Right-click and choose **Show event details**. The event's details appear in the Event Inspector.) To view *all* event fields, make sure that no field set is selected to limit the set of fields shown. (Select **Clear** from the drop-down menu above the list of event fields. With no field set selected, the drop-down shows "Select a Field Set".)

Connector

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is

concentrated or otherwise pre-processed, it may be passed to a trusted reporting Final Device before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the ArcSight ForwardingConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Address	connectorAddress	IP address	1	The IP address of the device hosting the SmartConnector.
Connector	Asset ID	connectorAssetId	Resource	1	The asset that represents the device hosting the SmartConnector.
Connector	Asset Name	connectorAssetName	String	1	The connector's asset name.
Connector	Asset Resource	connectorAssetResource	Resource	1	The connector resource.
Connector	Descriptor ID	connectorDescriptorId	ID	1	The connector descriptor.
Connector	DNS Domain	connectorDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the SmartConnector.
Connector	Host Name	connectorHostName	String	1	The name of the device hosting the SmartConnector.
Connector	ID	connectorId	String	1	The identifier associated with the SmartConnector configuration resource. The format is connectorID(1) connectorID(2) ...

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	MAC Address	connectorMacAddress	MacAddress	1	The MAC address associated with the SmartConnector or (which may or may not be the MAC address of the host device.)
Connector	Name	connectorName	String	1	The user-supplied name of the associated SmartConnector or configuration resource.
Connector	NT Domain	connectorNtDomain	String	1	The Windows NT domain associated with the device hosting the SmartConnector.
Connector	Receipt Time	connectorReceiptTime	DateTime	2	The time the event arrived at the SmartConnector.
Connector	Severity	connectorSeverity	Connector Severity Enumeration	1	The normalized ArcSight form of the event severity value provided by the SmartConnector.
Connector	Time Zone	connectorTimeZone	String	1	The time zone reported by the device hosting the SmartConnector or (as TLA).

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Time Zone Offset	connectorTimeZoneOffset	Integer	1	The time zone reported by the device hosting the SmartConnect or (shown as a UTC offset). Note that device times may be less accurate than other sources.
Connector	Translated Address	connectorTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the SmartConnect or.
Connector	Translated Zone	connectorTranslatedZone	Zone	1	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the SmartConnect or.
Connector	Translated Zone External ID	connectorTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Connector	Translated Zone ID	connectorTranslatedZoneID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Translated Zone Name	connectorTranslatedZoneName	String	1	See the common set of resource attributes. Returns the name from the URI. It assumes that the name is always the last field of the URI.
Connector	Translated Zone Reference ID	connectorTranslatedZoneReferenceID	ID	1	See the common set of resource attributes. Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Connector	Translated Zone Resource	connectorTranslatedZoneResource	Resource	1	See the common set of resource attributes. Locates the resource described by this reference.
Connector	Translated Zone URI	connectorTranslatedZoneURI	String	1	See the common set of resource attributes.
Connector	Type	connectorType	String	1	A description of the type of SmartConnect or that reported the event.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Connector	Version	connectorVersion	String	1	The software revision number of the SmartConnect or that reported the event
Connector	Zone	connectorZone	Zone	1	The network zone in which the device hosting this SmartConnect or resides.
Connector	Zone External ID	connectorZoneExternalID	String	1	See the common set of resource attributes.
Connector	Zone ID	connectorZoneID	String	1	See the common set of resource attributes.
Connector	Zone Name	connectorZoneName	String	1	See the common set of resource attributes.
Connector	Zone Reference ID	connectorZoneReferenceID	ID	1	See the common set of resource attributes.
Connector	Zone Resource	connectorZoneResource	Resource	1	See the common set of resource attributes.
Connector	Zone URI	connectorZoneURI	String	1	Returns the URI for this reference.

Attacker

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Address	attackerAddress	IP address	1	The IP address of the device hosting the attacker.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Asset ID	attackerAssetId	Resource	2	The asset that represents the device hosting the attacker.
Attacker	Asset Name	attackerAssetName	String	2	The name of the asset that represents the device hosting the attacker.
Attacker	Asset Resource	attackerAssetResource	Resource	2	See the common set of resource attributes
Attacker	DNS Domain	attackerDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the attacker.
Attacker	FQDN	attackerFqdn	String	2	The fully qualified domain name associated with the device hosting the attacker.
Attacker	Geo	attackerGeo	GeoDescriptor	1	See the common set of geographical attributes.
Attacker	Geo Country Code	attackerGeoCountryCode	String	1	See the common set of geographical attributes.
Attacker	Geo Country Flag URL	attackerGeoCountryFlagUrl	String	1	See the common set of geographical attributes.
Attacker	Geo Country Name	attackerGeoCountryName	String	1	See the common set of geographical attributes.
Attacker	Geo Descriptor ID	attackerGeoDescriptorId	ID	1	See the common set of geographical attributes.
Attacker	Geo Latitude	attackerGeoLatitude	Double	1	See the common set of geographical attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Geo Location Info	attackerGeoLocationInfo	String	Location	See the common set of geographical attributes.
Attacker	Geo Longitude	attackerGeoLongitude	Double	1	See the common set of geographical attributes.
Attacker	Geo Postal Code	attackerGeoPostalCode	String	1	See the common set of geographical attributes.
Attacker	Geo Region Code	attackerGeoRegionCode	String	1	See the common set of geographical attributes.
Attacker	Host Name	attackerHostName	String	2	The name of the device hosting the attacker.
Attacker	MAC Address	attackerMacAddress	MAC address	2	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).
Attacker	NT Domain	attackerNtDomain	String	2	The Windows NT domain associated with the device hosting the attacker.
Attacker	Port	attackerPort	Integer	1	The network port associated with the source of the attack.
Attacker	Process Name	attackerProcessName	String	2	The name of process associated with the source of the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Service Name	attackerServiceName	String	2	The name of service associated with the source of the attack.
Attacker	Translated Address	attackerTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the attacker.
Attacker	Translated Port	attackerTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack. This can happen in a NAT environment.
Attacker	Translated Zone	attackerTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the attacker.
Attacker	Translated Zone External ID	attackerTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Attacker	Translated Zone ID	attackerTranslatedZoneID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Translated Zone Name	attackerTranslatedZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Attacker	Translated Zone Reference ID	attackerTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Attacker	Translated Zone Resource	attackerTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Attacker	Translated Zone URI	attackerTranslatedZoneURI	String	1	See the common set of resource attributes.
Attacker	User ID	attackerUserId	String	2	The identifier associated with the OS or application of the attacker, at the source of the attack.
Attacker	User Name	attackerUserName	String	2	The name associated with the attacker, at the source of the attack.
Attacker	User Privileges	attackerUserPrivileges	String	2	The user-privilege associated with the attacker, at the source of the attack.
Attacker	Zone	attackerZone	Zone	1	The network zone in which the attacker's device resides.
Attacker	Zone External ID	attackerZoneExternalID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Attacker	Zone ID	attackerZoneID	String	1	See the common set of resource attributes.
Attacker	Zone Name	attackerZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Attacker	Zone Reference ID	attackerZoneReferenceID	ID	1	See the common set of resource attributes.
Attacker	Zone Resource	attackerZoneResource	Resource	1	See the common set of resource attributes.
Attacker	Zone URI	attackerZoneURI	String	1	See the common set of resource attributes.

Category

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Category	Behavior	categoryBehavior	String	1	Describes the action taken with or by the object.
Category	Custom Format Field	categoryCustomFormatField	String	1	Describes the content of a custom formatted field, if present.
Category	Descriptor ID	categoryDescriptorId	ID	1	The unique ID for the sensor that reported the event
Category	Device Group	categoryDeviceGroup	String	1	Describes the type of event this event represents.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Category	Object	categoryObject	String	1	Describes the physical or virtual object that was the focus of the event
Category	Outcome	categoryOutcome	String	1	Indicates whether the action was successfully applied to the object.
Category	Significance	categorySignificance	String	1	Characterizes the event from a network-intrusion-detection perspective.
Category	Technique	categoryTechnique	String	1	Describes the method used to apply the action to the object.
Category	Tuple Description	categoryTupleDescription	String	1	The prose description of the event category, assembled from the category components.

Destination

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Address	destinationAddress	IP address	1	The IP address of the destination device.
Destination	Asset ID	destinationAssetId	Resource	2	The asset that represents the device that was the network traffic's destination.
Destination	Asset Name	destinationAssetName	String	2	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Asset Resource	destinationAssetResource	Resource	2	See the common set of resource attributes.
Destination	DNS Domain	destinationDnsDomain	String	2	The Domain Name Service domain name associated with the user at the destination device.
Destination	FQDN	destinationFqdn	String	2	The fully qualified domain name associated with the destination device.
Destination	Geo	destinationGeo	GeoDescriptor	GeoDescriptor	See the common set of geographical attributes.
Destination	Geo Country Code	destinationGeoCountryCode	String	1	The country code.
Destination	Geo Country Flag URL	destinationGeoCountryFlagUrl	String	1	The country flag.
Destination	Geo Country Name	destinationGeoCountryName	String	1	The country name.
Destination	Geo Descriptor ID	destinationGeoDescriptorId	ID	1	See the common set of geographical attributes.
Destination	Geo Latitude	destinationGeoLatitude	Double	1	The destination latitude.
Destination	Geo Location Info	destinationGeoLocationInfo	String	1	The destination location.
Destination	Geo Longitude	destinationGeoLongitude	Double	1	The destination longitude.
Destination	Geo Postal Code	destinationGeoPostalCode	String	1	The destination postal code.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Geo Region Code	destinationGeoRegionCode	String	1	See the common set of geographical attributes.
Destination	Host Name	destinationHostName	String	2	The name of the destination device.
Destination	MAC Address	destinationMacAddress	MAC address	2	The MAC address associated with the network traffic's destination (which may or may not be the MAC address of the host device).
Destination	NT Domain	destinationNtDomain	String	2	The Windows NT domain associated with the destination device.
Destination	Port	destinationPort	Integer	1	The network port associated with the network traffic's destination.
Destination	Process Name	destinationProcessName	String	2	The name of process associated with the network traffic's destination.
Destination	Service Name	destinationServiceName	String	2	The name of service associated with the network traffic's destination.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Translated Address	destinationTranslatedAddresses	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's destination.
Destination	Translated Port	destinationTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.
Destination	Translated Zone	destinationTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device at the network's traffic's destination.
Destination	Translated Zone External ID	destinationTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Destination	Translated Zone ID	destinationTranslatedZoneID	String	1	See the common set of resource attributes.
Destination	Translated Zone Name	destinationTranslatedZoneName	String	1	See the common set of resource attributes.
Destination	Translated Zone Reference	destinationTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Translated Zone Resource	destinationTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Destination	Translated Zone URI	destinationTranslatedZoneURI	String	1	See the common set of resource attributes.
Destination	User ID	destinationUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's destination.
Destination	User Name	destinationUserName	String	2	The name associated with the user at the network traffic's destination.
Destination	User Privileges	destinationUserPrivileges	String	2	The privileges accorded the user at the network traffic destination.
Destination	Zone	destinationZone	Zone	1	The network zone in which the destination device resides.
Destination	Zone External ID	destinationZoneExternalID	String	1	See the common set of resource attributes.
Destination	Zone ID	destinationZoneID	String	1	See the common set of resource attributes.
Destination	Zone Name	destinationZoneName	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Destination	Zone Reference ID	destinationZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Destination	Zone Resource	destinationZoneResource	Resource	1	See the common set of resource attributes.
Destination	Zone URI	destinationZoneURI	String	1	See the common set of resource attributes.

Device

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the ESM Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Action	deviceAction	String	2	The device-specific description of some activity associated with the event
Device	Address	deviceAddress	IP address	1	The IP address of the device hosting the sensor.
Device	Asset ID	deviceAssetId	Resource	1	The asset that represents the device hosting the sensor.
Device	Asset Name	deviceAssetName	String	1	The name of the device.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Asset Resource	deviceAssetResource	Resource	1	The resource the asset represents.
Device	Descriptor ID	deviceDescriptorId	ID	1	The asset's descriptor ID.
Device	Direction	deviceDirection	DeviceDirectionEnumeration	2	Whether the traffic was inbound or outbound.
Device	DNS Domain	deviceDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the sensor.
Device	Domain	deviceDomain	String	2	The specific domain containing the sensor device associated with the event
Device	Event Category	deviceEventCategory	String	2	The category description included with the event as reported by the device.
Device	Event Class ID	deviceEventClassId	String	2	The device-specific identifier associated with this type of event
Device	External ID	deviceExternalId	String	1	The external identifier associated with this sensor device, if provided by the vendor.
Device	Facility	deviceFacility	String	1	The sensor submodule that reported the event
Device	Host Name	deviceHostName	String	1	The name of the device hosting the sensor.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Inbound Interface	deviceInboundInterface	String	1	The NIC card on the sensor device that received the network traffic associated with the event.
Device	MAC Address	deviceMacAddress	MAC address	1	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).
Device	NT Domain	deviceNtDomain	String	1	The Windows NT domain associated with the device hosting the sensor.
Device	Outbound Interface	deviceOutboundInterface	String	1	The NIC card on the sensor device that transmitted the network traffic associated with the event.
Device	Payload ID	devicePayloadId	String	2	The internal identifier associated with a payload object associated with this event.
Device	Process Name	deviceProcessName	String	1	The sensor device process that reported the event.
Device	Product	deviceProduct	String	1	The product name of the sensor device.
Device	Receipt Time	deviceReceiptTime	DateTime	2	The time when the sensor device observed the event.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Severity	deviceSeverity	String	2	The device-specific assessment of event severity. This assessment varies with the device involved.
Device	Time Zone	deviceTimeZone	String	1	The time zone reported by the device hosting the sensor device (shown as TLA).
Device	Time Zone Offset	deviceTimeZoneOffset	Integer	1	The time zone reported by the device hosting this sensor device (shown as an offset from UTC).
Device	Translated Address	deviceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the sensor.
Device	Translated Zone	deviceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the sensor.
Device	Translated Zone External ID	deviceTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Device	Translated Zone ID	deviceTranslatedZoneID	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Translated Zone Name	deviceTranslatedZoneName	String	1	See the common set of resource attributes.
Device	Translated Zone Resource	deviceTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Device	Translated Zone Resource	deviceTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Device	Translated Zone URI	deviceTranslatedZoneURI	String	1	See the common set of resource attributes.
Device	Vendor	deviceVendor	String	1	The vendor who manufactured or sold the sensor device.
Device	Version	deviceVersion	String	1	The software revision number of the sensor device.
Device	Zone	deviceZone	Zone	1	The network zone in which the sensor's device resides.
Device	Zone External ID	deviceZoneExternalID	String	1	See the common set of resource attributes.
Device	Zone ID	deviceZoneID	String	1	See the common set of resource attributes.
Device	Zone Name	deviceZoneName	String	1	See the common set of resource attributes.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device	Zone Reference ID	deviceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been persisted and given a unique database identifier.
Device	Zone Resource	deviceZoneResource	Resource	1	See the common set of resource attributes.
Device	Zone URI	deviceZoneURI	String	1	See the common set of resource attributes.

Device Custom

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device Custom	Date1	deviceCustomDate1	DateTime	2	First customDate
Device Custom	Date1 Label	deviceCustomDate1Label	String	2	First customDate label
Device Custom	Date2	deviceCustomDate2	DateTime	2	Second customDate
Device Custom	Date2 Label	deviceCustomDate2Label	String	2	Second customDate label
Device Custom	Descriptor ID	deviceCustomDescriptorId	ID	2	Custom descriptor ID
Device Custom	Number1	deviceCustomNumber1	Long	2	First customNumber
Device Custom	Number1 Label	deviceCustomNumber1Label	String	2	First customNumber label
Device Custom	Number2	deviceCustomNumber2	Long	2	Second customNumber

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Device Custom	Number2 Label	deviceCustomNumber2Label	String	2	Second customNumber label
Device Custom	Number3	deviceCustomNumber3	Long	2	Third customNumber
Device Custom	Number3 Label	deviceCustomNumber3Label	String	2	Third customNumber label
Device Custom	String1	deviceCustomString1	String	2	First customString
Device Custom	String1 Label	deviceCustomString1Label	String	2	First customString label
Device Custom	String2	deviceCustomString2	String	2	Second customString
Device Custom	String2 Label	deviceCustomString2Label	String	2	Second customString label
Device Custom	String3	deviceCustomString3	String	2	Third customString
Device Custom	String3 Label	deviceCustomString3Label	String	2	Third customString label
Device Custom	String4	deviceCustomString4	String	2	Fourth customString
Device Custom	String4 Label	deviceCustomString4Label	String	2	Fourth customString label
Device Custom	String5	deviceCustomString5	String	2	Fifth customString
Device Custom	String5 Label	deviceCustomString5Label	String	2	Fifth customString label
Device Custom	String6	deviceCustomString6	String	2	Sixth customString
Device Custom	String6 Label	deviceCustomString6Label	String	2	Sixth customString label

Event

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Additional Data	additionalData	AdditionalData	3	Reference to additional data.
Event	Aggregated Event Count	(not applicable)	(not applicable)	(not applicable)	A derived field that reports the number of actual events collectively represented by the event in question.
Event	Application Protocol	applicationProtocol	String	2	A description of the application layer protocol. May be set, but defaults to Target Port lookup (FTP).
Event	Base Event Count	baseEventCount	Integer	1	The number of events upon which this event is based (e.g., type == BASE ACTION).
Event	Base Event IDs	baseEventIds	ID	2	The array of event IDs that contributed to generating this correlation event. This is populated only in correlated events.
Event	Bytes In	bytesIn	Integer	2	Number of bytes transferred into the device during this transaction (this would typically be associated with entries in HTTP logs).

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Bytes Out	bytesOut	Integer	2	Number of bytes transferred out of the device during this transaction (this would typically be associated with entries in HTTP logs).
Event	Concentrator Connectors	concentratorConnectors	ConnectorDescriptor	2	The chain of concentrators that forwarded the event This is not yet exposed in the user interface.
Event	Concentrator Devices	concentratorDevices	DeviceDescriptor	2	The list of devices that concentrate events, if applicable. This is not exposed in the user interface.
Event	Correlated Event Count	(not applicable)	(not applicable)	(not applicable)	A derived field that reports the number of actual events that had to occur to cause a correlation event to occur.
Event	Crypto Signature	cryptoSignature	String	2	The signature of the event object (meaning in this alert, as opposed to the occurrence represented by the event). Not yet supported.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Customer	customer	Customer	1	The "customer" resource reference. This is used in MSSP environments to describe the client or divisional entity to whom the event applies.
Event	Customer External ID	customerExternalID	String	1	Returns the external ID for this reference.
Event	Customer ID	customerID	String	1	Returns the ID for the resource in this resource reference.
Event	Customer Name	customerName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event	Customer Reference ID	customerReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Customer Resource	customerResource	Resource	1	Locates the resource described by this reference.
Event	Customer URI	customerURI	String	1	Returns the URI for this reference.
Event	End Time	endTime	DateTime	1	Event ends (defaults to deviceReceiptTime).

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Event ID	eventId	ID	1	Long value identifying an event.
Event	External ID	externalId	String	2	A reference to the ID used by an external device. This is useful for tracking devices that create events that contain references to these IDs (e.g., ManHunt).
Event	Generator	generator	null	1	The "generator" resource reference (the resource that generated the event. This is the subcomponent in the connector that generates the event.
Event	Generator External ID	generatorExternalID	String	1	Returns the external ID for this reference.
Event	Generator ID	generatorID	String	1	Returns the ID for the resource in this resource reference.
Event	Generator Name	generatorName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Generator Reference ID	generatorReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Generator Resource	generatorResource	Resource	1	Locates the resource described by this reference.
Event	Generator URI	generatorURI	String	1	Returns the URI for this reference.
Event	Locality	locality	LocalityEnumeration	2	The locality associated with the event.
Event	Message	message	String	2	A brief comment associated with this event.
Event	Name	name	String	1	An arbitrary string that describes this type of event. Event details included in other parts of an event shouldn't be used in the event name.
Event	Originator	originator	OriginatorEnumeration	1	Holds the value of Source Destination. This determines whether source and destination should be translated to attacker and target or they should be inversed.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Persistence	persistence	PersistenceEnumeration	2	There are two states: Persisted or Transient. Events default to being Transient and are marked as Persisted as soon as they reach the Batch Alert Persistor or when they are loaded by the Alert Broker.
Event	Raw Event	rawEvent	String	1	The original log entry reported by the sensor (synthesized when the sensor does not log to a file or text stream).
Event	Rule Thread ID	ruleThreadId	String	2	A single rule can issue many events, based on several triggers, starting with On First Event and ending with On Threshold Timeout. All such events for a single Rule and a single Group By tuple will be marked with the same identifier using this attribute.
Event	Session ID	sessionId	Long	2	Tags for events created by a correlation simulation, as part of a particular simulation.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Start Time	startTime	DateTime	1	Event begins (defaults to deviceReceiptTime).
Event	Transport Protocol	transportProtocol	String	1	The format of the transmitted data associated with the event from a network transport perspective (e.g., TCP, UDP).
Event	Type	type	TypeEnumeration	1	One of the event types: Base, Correlation, Aggregation, or Action.
Event	Vulnerability	vulnerability	Vulnerability	2	The vulnerability resource that represents the vulnerability or exposure that may be exploited by this event and is present on the targeted device according to our network model.
Event	Vulnerability External ID	vulnerabilityExternalID	String	2	Returns the external ID for this reference.
Event	Vulnerability ID	vulnerabilityID	String	2	Returns the ID for the resource in this resource reference.
Event	Vulnerability Name	vulnerabilityName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event	Vulnerability Reference ID	vulnerabilityReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event	Vulnerability Resource	vulnerabilityResource	Resource	2	Locates the resource described by this reference.
Event	Vulnerability URI	vulnerabilityURI	String	2	Returns the URI for this reference.

Event Annotation

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Audit Trail	eventAnnotationAuditTrail	String	2	The text log of annotation changes. Changes are recorded as sets of comma-separated-value entries.
Event Annotation	Comment	eventAnnotationComment	String	2	A text description of the event or associated information.
Event Annotation	End Time	eventAnnotationEndTime	DateTime	2	The timestamp for an eventannotation.
Event Annotation	Event ID	eventAnnotationEventId	ID	2	The event ID for the annotation event.
Event Annotation	Flags	eventAnnotationFlags	FlagsValueSet	2	The state of the collaboration flags.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Manager Receipt Time	eventAnnotationManagerReceiptTime	DateTime	2	The time the Manager received the event annotation.
Event Annotation	Modification Time	eventAnnotationModificationTime	DateTime	2	The time the annotation was modified.
Event Annotation	Modified By	eventAnnotationModifiedBy	User	2	The user ID of the person who last edited this annotation.
Event Annotation	Modified By External ID	eventAnnotationModifiedByExternalID	String	2	Returns the external ID for this reference.
Event Annotation	Modified By ID	eventAnnotationModifiedByID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Modified By Name	eventAnnotationModifiedByName	String	2	Returns the name from the URI (the last field of the URI).
Event Annotation	Modified By Reference ID	eventAnnotationModifiedByReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Event Annotation	Modified By Resource	eventAnnotationModifiedByResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Modified By URI	eventAnnotationModifiedByURI	String	2	Returns the URI for this reference.
Event Annotation	Stage	eventAnnotationStage	Stage	2	The current disposition of the event. This enables annotation workflow.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Stage Event ID	eventAnnotationStageEventId	ID	2	The reference to an internal identifier for another event. It is used by 'Mark Similar'.
Event Annotation	Stage External ID	eventAnnotationStageExternalID	String	2	Returns the external ID for this reference.
Event Annotation	Stage ID	eventAnnotationStageID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Stage Name	eventAnnotationStageName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event Annotation	Stage Reference ID	eventAnnotationStageReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.
Event Annotation	Stage Resource	eventAnnotationStageResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Stage Update Time	eventAnnotationStageUpdateTime	ID	2	The time of the last stage change (in UTC).
Event Annotation	Stage URI	eventAnnotationStageURI	String	2	Returns the URI for this reference.
Event Annotation	Stage User	eventAnnotationStageUser	User	2	The user associated with the current stage. This implements assignment within workflow.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Event Annotation	Stage User External ID	eventAnnotationStageUserExternalID	String	2	Returns the external ID for this reference.
Event Annotation	Stage User ID	eventAnnotationStageUserID	String	2	Returns the ID for the resource in this resource reference.
Event Annotation	Stage User Name	eventAnnotationStageUserName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Event Annotation	Stage User Reference ID	eventAnnotationStageUserReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.
Event Annotation	Stage User Resource	eventAnnotationStageUserResource	Resource	2	Locates the resource described by this reference.
Event Annotation	Stage User URI	eventAnnotationStageUserURI	String	2	Returns the URI for this reference.
Event Annotation	Version	eventAnnotationVersion	Integer	2	The editing version number which increments with each change. This enables optimistic locking.

File

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
File	Create Time	fileCreateTime	DateTime	2	The time the file was created (in UTC).
File	Hash	fileHash	String	2	The hashcode associated with the file's contents (e.g., MD5).
File	ID	fileId	String	2	The external identifier associated with the file.
File	Modification Time	fileModificationTime	DateTime	2	The time the file was last changed (in UTC).
File	Name	fileName	String	2	The name of the file.
File	Path	filePath	String	2	The directory path to the file in the file system.
File	Permission	filePermission	String	2	The user permissions associated with the file (sensor specific).
File	Size	fileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
File	Type	fileType	String	2	The type of file contents (sensor specific).

Final Device

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the ESM Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Address	finalDeviceAddress	IP address	2	The IP address of the trusted reporting device.
Final Device	Asset ID	finalDeviceAssetId	Resource	2	The asset that represents the trusted reporting device.
Final Device	Asset Name	finalDeviceAssetName	String	2	The name of the trusted reporting device.
Final Device	Asset Resource	finalDeviceAssetResource	Resource	2	The resource represented by the trusted reporting device.
Final Device	Descriptor ID	finalDeviceDescriptorId	ID	2	The descriptor ID of the trusted reporting device.
Final Device	DNS Domain	finalDeviceDnsDomain	String	2	The Domain Name Service domain name associated with the trusted reporting device.
Final Device	External ID	finalDeviceExternalId	String	2	The external ID for the trusted reporting device, if provided by the vendor.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Facility	finalDeviceFacility	String	2	A facility or capability of a device. This accomodates concentrators (e.g., like syslog, which has a concept of device logging for "parts" of a device).
Final Device	Host Name	finalDeviceHostName	String	2	The host name of the trusted reporting device.
Final Device	Inbound Interface	finalDeviceInboundInterface	String	2	The NIC card on the sensor device that received the network traffic associated with the event.
Final Device	MAC address	finalDeviceMacAddress	MAC address	2	The MAC address associated with the trusted reporting device.
Final Device	NT Domain	finalDeviceNtDomain	String	2	The Windows NT domain associated with the trusted reporting device.
Final Device	Outbound Interface	finalDeviceOutboundInterface	String	2	The NIC card on the trusted reporting device.
Final Device	Process Name	finalDeviceProcessName	String	2	The process name of the trusted reporting device.
Final Device	Product	finalDeviceProduct	String	2	The product name of the trusted reporting device.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Time Zone	finalDeviceTimeZone	String	2	The time zone reported by the trusted reporting device.
Final Device	Time Zone Offset	finalDeviceTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the trusted reporting device. Note that connector and device times are not always reliably accurate.
Final Device	Translated Address	finalDeviceTranslatedAddresses	IP address	2	If network address translation is an issue, this is the translated IP address of the trusted reporting device.
Final Device	Translated Zone	finalDeviceTranslatedZone	Zone	2	If network address translation is an issue, this is the network zone associated with the translated IP address of the trusted reporting device.
Final Device	Translated Zone External ID	finalDeviceTranslatedZoneExternalID	String	2	Returns the external ID for this reference.
Final Device	Translated Zone ID	finalDeviceTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Final Device	Translated Zone Name	finalDeviceTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Translated Zone Reference ID	finalDeviceTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Final Device	Translated Zone Resource	finalDeviceTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Final Device	Translated Zone URI	finalDeviceTranslatedZoneURI	String	2	Returns the URI for this reference.
Final Device	Vendor	finalDeviceVendor	String	2	Device vendor.
Final Device	Version	finalDeviceVersion	String	2	The software revision number of the trusted reporting device.
Final Device	Zone	finalDeviceZone	Zone	2	The network zone in which the trusted reporting device resides.
Final Device	Zone External ID	finalDeviceZoneExternalID	String	2	Returns the external ID for this reference.
Final Device	Zone ID	finalDeviceZoneID	String	2	Returns the ID for the resource in this resource reference.
Final Device	Zone Name	finalDeviceZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Final Device	Zone Reference ID	finalDeviceZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Final Device	Zone Resource	finalDeviceZoneResource	Resource	2	Locates the resource described by this reference.
Final Device	Zone URI	finalDeviceZoneURI	String	2	Returns the URI for this reference.

Flex

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Flex	Date1	flexDate1	DateTime	2	First flexDate.
Flex	Date1 Label	flexDate1Label	String	2	Label of first flexDate.
Flex	Number1	flexNumber1	Long	2	First flexNumber.
Flex	Number1 Label	flexNumber1Label	String	2	Label of the first FlexNumber.
Flex	Number2	flexNumber2	Long	2	Second flexNumber.
Flex	Number2 Label	flexNumber2Label	String	2	Label of the second FlexNumber.
Flex	String1	flexString1	String	2	First flexString
Flex	String1 Label	flexString1Label	String	2	Label of the first FlexString.
Flex	String2	flexString2	String	2	Second flexString.
Flex	String2 Label	flexString2Label	String	2	Label of the second FlexString.

Manager

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Manager	Receipt Time	managerReceiptTime	DateTime	1	The time at which the current Manager first received the event.

Old File

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Old File	Create Time	oldFileCreateTime	DateTime	2	The time the file was created (in UTC).
Old File	Hash	oldFileHash	String	2	The hashcode associated with the file's contents (e.g., MD5).
Old File	ID	oldFileId	String	2	The external identifier associated with the file.
Old File	Modification Time	oldFileModificationTime	DateTime	2	The time the file was last changed (in UTC).
Old File	Name	oldFileName	String	2	The file's name.
Old File	Path	oldFilePath	String	2	The directory path to the file in the file system.
Old File	Permission	oldFilePermission	String	2	The user permissions associated with the file (sensor specific).
Old File	Size	oldFileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
Old File	Type	oldFileType	String	2	The type of the file's contents (sensor specific).

Original Connector

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain will include handling by **Connector** stages that are the ESM Manager SmartConnectors that facilitate Manager-to-Manager connections.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original Connector	Address	originalConnectorAddress	IP address	2	The IP address of the device hosting the first reporting SmartConnector.
Original Connector	Asset ID	originalConnectorAssetID	Resource	2	The asset that represents the device hosting the first reporting SmartConnector.
Original Connector	Asset Name	originalConnectorAssetName	String	2	The first reporting connector's asset name.
Original Connector	Asset Resource	originalConnectorAssetResource	Resource	2	The first reporting connector's resource.
Original Connector	Descriptor ID	originalConnectorDescriptorId	ID	2	The first reporting connector's descriptor.
Original Connector	DNS Domain	originalConnectorDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the first reporting SmartConnector.
Original Connector	Host Name	originalConnectorHostName	String	2	The name of the device hosting the first reporting SmartConnector.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original Connector	ID	originalConnectorId	String	2	The ID of the connector. The format is connectorId(1) connectorId(2) ...
Original connector	MAC address	originalconnectorMacAddresses	MAC address	2	The MAC address associated with the first reporting Smartconnect or (which may or may not be the MAC address of the host device.)
Original connector	Name	originalconnectorName	String	2	User-supplied name of the first reporting connector.
Original connector	NT Domain	originalconnectorNtDomain	String	2	The Windows NT domain associated with the device hosting the first reporting Smartconnect or.
Original connector	Time Zone	originalconnectorTimeZone	String	2	The time zone reported by the device hosting the first reporting Smartconnect or.
Original connector	Time Zone Offset	originalconnectorTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the first reporting connector's time zone. Note that device and connector times may not be reliably accurate.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	Translated Address	originalconnectorTranslatedAddress	IP address	2	If network address translation is an issue, this is the translated IP address of the device hosting the first reporting Smartconnector.
Original connector	Translated Zone	originalconnectorTranslatedZone	Zone	2	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the first reporting Smartconnector.
Original connector	Translated Zone External ID	originalconnectorTranslatedZoneExternalID	String	2	Returns the external ID for this reference.
Original connector	Translated Zone ID	originalconnectorTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Original connector	Translated Zone Name	originalconnectorTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Original connector	Translated Zone Reference ID	originalconnectorTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	Translated Zone Resource	originalconnectorTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Original connector	Translated Zone URI	originalconnectorTranslatedZoneURI	String	2	Returns the URI for this reference.
Original connector	Type	originalconnectorType	String	2	A string that describes the type of the first reporting connector. This is not the same as the device type.
Original connector	Version	originalconnectorVersion	String	2	The software revision number of the Smartconnect or that first reported the event.
Original connector	Zone	originalconnectorZone	Zone	2	The network zone in which the device hosting the first reporting Smartconnect or resides.
Original connector	Zone External ID	originalconnectorZoneExternalID	String	2	Returns the external ID for this reference.
Original connector	Zone ID	originalconnectorZoneID	String	2	Returns the ID for the resource in this resource reference.
Original connector	Zone Name	originalconnectorZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Original connector	Zone Reference ID	originalconnectorZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and is uniquely identified in the database.
Original connector	Zone Resource	originalconnectorZoneResource	Resource	2	Locates the resource described by this reference.
Original connector	Zone URI	originalconnectorZoneURI	String	2	Returns the URI for this reference.

Request

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Request	Client Application	requestClientApplication	String	2	The client application (such as a web browser) used to issue the request.
Request	Client Application	requestClientApplication	String	2	A description of the client application used to initiate this request, e.g., the HTTP User connector.
Request	Context	requestContext	String	2	A description of the content from which the request originated, e.g., the HTTP Referrer.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Request	Cookies	requestCookies	String	2	Cookie data offered by the client application as part of the request.
Request	Method	requestMethod	String	2	The style of the request, i.e., for an HTTP request this could be PUT or GET.
Request	Protocol	requestProtocol	String	2	The communication protocol used when issuing the request.
Request	URL	requestUrl	String	2	A universal resource locator associated with the event.
Request	URL Authority	requestUrlAuthority	String	2	The URL component used for authentication and authorization.
Request	URL File Name	requestUrlFileName	String	2	The URL component that refers to the file containing the resource.
Request	URL Host	requestUrlHost	String	2	The URL component that specifies the host device where the resource resides.
Request	URL Port	requestUrlPort	Integer	2	The URL component that specifies the port to contact on the host device where the resource resides.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Request	URL Query	requestUrlQuery	String	2	The URL component that specifies the query to use to request the resource.

Source

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Address	sourceAddress	IP address	1	The IP address of the source device.
Source	Asset ID	sourceAssetId	Resource	2	The asset that represents the device that was the network traffic's source.
Source	Asset Name	sourceAssetName	String	2	See the common set of resource attributes.
Source	Asset Resource	sourceAssetResource	Resource	2	See the common set of resource attributes.
Source	DNS Domain	sourceDnsDomain	String	2	The Domain Name Service domain name associated with the user at the source device.
Source	FQDN	sourceFqdn	String	2	The fully qualified domain name associated with the source device. This has no value if either the host name or DNS domain are without a value.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Geo	sourceGeo	GeoDescriptor	1	The geographical information.
Source	Geo Country Code	sourceGeoCountryCode	String	1	Country Code.
Source	Geo Country Flag URL	sourceGeoCountryFlagUrl	String	1	County Flag.
Source	Geo Country Name	sourceGeoCountryName	String	1	Country Code.
Source	Geo Descriptor ID	sourceGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Source	Geo Latitude	sourceGeoLatitude	Double	1	See the common set of geographical attributes.
Source	Geo Location Info	sourceGeoLocationInfo	String	1	See the common set of geographical attributes.
Source	Geo Longitude	sourceGeoLongitude	Double	1	See the common set of geographical attributes.
Source	Geo Postal Code	sourceGeoPostalCode	String	1	See the common set of geographical attributes.
Source	Geo Region Code	sourceGeoRegionCode	String	1	See the common set of geographical attributes.
Source	Host Name	sourceHostName	String	2	The name of the source device.
Source	MAC Address	sourceMacAddress	MAC address	2	The MAC address associated with the network traffic's source (which may or may not be the MAC address of the host device).

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	NT Domain	sourceNtDomain	String	2	The Windows NT domain associated with the source device.
Source	Port	sourcePort	Integer	1	The network port associated with the network traffic's source.
Source	Process Name	sourceProcessName	String	2	The name of the process associated with the source of the network traffic.
Source	Service Name	sourceServiceName	String	2	The name of the service associated with the network traffic's source.
Source	Translated Address	sourceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's source.
Source	Translated Port	sourceTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Translated Zone	sourceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device that was the network traffic's source.
Source	Translated Zone External ID	sourceTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Source	Translated Zone ID	sourceTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Source	Translated Zone Name	sourceTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Source	Translated Zone Reference ID	sourceTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Source	Translated Zone Resource	sourceTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Source	Translated Zone URI	sourceTranslatedZoneURI	String	1	Returns the URI for this reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	User ID	sourceUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's source.
Source	User Name	sourceUserName	String	2	The OS- or application-based name associated with the user at the network traffic's source.
Source	User Privileges	sourceUserPrivileges	String	2	The privileges afforded the user at the network traffic's source.
Source	Zone	sourceZone	Zone	1	The network zone where the source device resides.
Source	Zone External ID	sourceZoneExternalID	String	1	Returns the external ID for this reference.
Source	Zone ID	sourceZoneID	String	1	Returns the ID for the resource in this resource reference.
Source	Zone Name	sourceZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Source	Zone Reference ID	sourceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Source	Zone Resource	sourceZoneResource	Resource	1	Locates the resource described by this reference.
Source	Zone URI	sourceZoneURI	String	1	Returns the URI for this reference.

Target

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Address	targetAddress	IP address	1	The IP address of the device hosting the attacker.
Target	Asset ID	targetAssetId	Resource	2	The asset that represents the attacked device's host.
Target	Asset Name	targetAssetName	String	2	See the common set of resource attributes.
Target	Asset Resource	targetAssetResource	Resource	2	See the common set of resource attributes.
Target	DNS Domain	targetDnsDomain	String	2	The Domain Name Service domain name associated with the attacked device.
Target	FQDN	targetFqdn	String	2	The fully qualified domain name associated with the attacked device.
Target	Geo	targetGeo	GeoDescriptor	1	The geographical information.
Target	Geo Country Code	targetGeoCountryCode	String	1	Country code.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Geo Country Flag URL	targetGeoCountryFlagUrl	String	1	County flag.
Target	Geo Country Name	targetGeoCountryName	String	1	Country name.
Target	Geo Descriptor ID	targetGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Target	Geo Latitude	targetGeoLatitude	Double	1	Latitude.
Target	Geo Location Info	targetGeoLocationInfo	String	1	Location information.
Target	Geo Longitude	targetGeoLongitude	Double	1	Longitude.
Target	Geo Postal Code	targetGeoPostalCode	String	1	Postal code.
Target	Geo Region Code	targetGeoRegionCode	String	1	Region code.
Target	Host Name	targetHostName	String	2	The name of the attacked device.
Target	MAC Address	targetMacAddress	MAC address	2	The MAC address associated with the target of the attack (which may or may not be the MAC address of the host device).
Target	NT Domain	targetNtDomain	String	2	The Windows NT domain associated with the attacked device.
Target	Port	targetPort	Integer	1	The network port associated with the target of the attack.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Process Name	targetProcessName	String	2	The name of the process associated with the attack's target.
Target	Service Name	targetServiceName	String	2	The name of service associated with the attack's target.
Target	Translated Address	targetTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the attacked device.
Target	Translated Port	targetTranslatedPort	Integer	1	If network address translation is an issue, this is the translated port associated with the attack.
Target	Translated Zone	targetTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the targeted device.
Target	Translated Zone External ID	targetTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Target	Translated Zone ID	targetTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Translated Zone Name	targetTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Target	Translated Zone Reference ID	targetTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Target	Translated Zone Resource	targetTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Target	Translated Zone URI	targetTranslatedZoneURI	String	1	Returns the URI for this reference.
Target	User ID	targetUserId	String	2	The OS- or application-based identifier associated with the attacker, at the target of the attack.
Target	User Name	targetUserName	String	2	The OS- or application-based name associated with the attacker, at the target of the attack.
Target	User Privileges	targetUserPrivileges	String	2	The privileges afforded the attacker, at the target of the attack.
Target	Zone	targetZone	Zone	1	The network zone in which the attacked device resides.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Target	Zone External ID	targetZoneExternalID	String	1	Returns the external ID for this reference.
Target	Zone ID	targetZoneID	String	1	Returns the ID for the resource in this resource reference.
Target	Zone Name	targetZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Target	Zone Reference ID	targetZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Target	Zone Resource	targetZoneResource	Resource	1	Locates the resource described by this reference.
Target	Zone URI	targetZoneURI	String	1	Returns the URI for this reference.

Threat

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Threat	Asset Criticality	assetCriticality	Integer	2	The relative measure of the importance of the targeted device, on a scale of 0 to 10.

Group	Label	Script Alias	Data Type	Default Turbo Level	Description
Threat	Model Confidence	modelConfidence	Integer	2	The relative measure of ArcSight's confidence in its model of the attacked device, on a scale of 0 to 10.
Threat	Priority	priority	Integer	1	The relative measure of importance of investigating this event on a scale of 0 to 10. This field incorporates Model Confidence.
Threat	Relevance	relevance	Integer	2	The relative measure of likelihood that this event succeeded, on a scale of 0 to 10.
Threat	Severity	severity	Integer	2	The relative measure of possible damage to network security represented by the event on a scale of 0 to 10. It may be noted that event severity is supplied by the device; ArcSight severity is supplied by the Smartconnect or; and attack severity is supplied by the threat evaluation process.

Resource Attributes

Attribute Suffix	Description
External ID	The user-defined identifier associated with a configuration resource.
ID	The internal identifier associated with a resource (a UUID).
Reference ID	The internal identifier associated with the resource reference (an integer).
Type Name	The type of configuration resource.
URI	The URI associated with the resource (e.g., /All Users/Administrators/Mlow).

Geographical Attributes

Attribute Suffix	Description
Descriptor ID	The internal ID of the geographical reference.
Country Code	The identifier for the national-political state in which a device resides.
Country Flag URL	The URL of an image of the flag of the national-political state in which the device resides.
Country Name	The name of the national-political state where a device resides.
Latitude	The latitude of a device (Float).
Location Info	Other, free-form text information about the device's location.
Longitude	The longitude of a device (Float).
Postal Code	The postal code of the device's location, as assigned by the national-political state where it resides.
Region Code	The identifier of the sub-region of the national-political state where a device resides. The style of the identifier varies with the host country.

Data Monitors

Data monitors are views within [Dashboards](#) that can be configured to report on [Events](#), filters (see [Filters](#)), [Rules](#), and other areas that are of particular interest to you. Data monitors can be arranged on dashboards in numerous viewing layouts. Data monitors collect summary information (from the ESM [Database](#)) on top events, most recent event activity, partial rule occurrences, hourly event counts, or event averages.

Data Monitors on Dashboards

Once data monitors are created, they can be used to display information on dashboards. You can add one or more data monitors to the same dashboard to create a collection of different "instrument panel" monitors appearing in the Dashboard display in the Viewer panel. Both the data monitors themselves and dashboards on which they are published can be shared among multiple Console users.

Permissions on Data Monitors

Data monitors display only those events for which you have permission. In addition, if you do not have access to a data monitor, the data monitor will not function. Administrators can limit visibility of or control access to dashboards and data monitors by changing access control lists (ACLs) as needed. For more about this, see ["Managing Permissions and Resources" on page 443](#) and ["Controlling Who Has Permissions to Deploy Data Monitors" on page 452](#).

Data Monitor Types

The ESM Console offers several predefined types to choose from when creating a new data monitor. The following topics describe the parameter entries and other options you can specify for each supported data monitor type.

The Data Monitor type is specified when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 117](#). (Also, the data monitors provided with ArcSight ESM are examples of these various types of data monitors.)

Asset Category Count Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 117](#).

This data monitor enumerates the number of real-time hits (events) that occur per asset category, by priority, within a time interval.

Table 22-1 Asset Category Count Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	<p>Select this check box to "switch on" the monitor and collect data from the ESM Manager. If cleared, the monitor is "off" and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 118.</p>

Parameter	Description
Root Asset Group	Click this field to choose an asset-category resource group to monitor.
Levels	Set the number of resource hierarchy levels below the chosen Root Asset Group to monitor. A value of "1" monitors only the next level down. A value of "-1", on the other hand, monitors all levels.
Aggregation	Turn on (True) or off (False) the ability to aggregate all hits to the asset group URI, including those above the leaf level, to reveal disparities or unanticipated counts that may merit drilling down.
Show Root URI	Choose whether to display (True) or not display (False) the complete URI for affected asset categories.
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the asset categories.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

Event Correlation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

This data monitor provides flow-volume level correlation between two different event streams. The data monitor specifies two filters to identify two sub-streams of events within the overall stream of events coming into ESM Manager. It then reports how closely the volume of events in the two streams correlate, that is, when the volume of events in Stream 1 decreases, does the volume in Stream 2 increase, decrease, or just change with no relation to the changes in Stream 1? For example, if a network intrusion detection system (NIDS) were deployed in front of several web servers in a cluster, one might expect that the flow of reported events from each NIDS would be roughly equivalent. If the event flow from one of the NIDS suddenly rose or fell out of sync with the other NIDS, then it might indicate a possible problem.

Table 22-2 Event Correlation Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.
Filter 1	Select a filter for the first event flow.

Parameter	Description
Filter 2	Select a filter for the second event flow.
Restrict by Filter	Choose to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves.
Number of Samples	Number of samples to keep in memory to perform calculations.
Sampling Interval	Enter the interval (in seconds) for performing correlation calculations.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Alarm Condition	<p>Condition on which to fire an alarm, for example: $c > 90 \ \&\& \ x > 0 \ \&\& \ y > 0$. In this example, c represents the correlation count from -100 to +100, x and y represent the actual count of events.</p> <p>Please see “Data Monitor Expressions” on page 720 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.</p>

The formula for calculating the correlation values displayed in data monitors is:

$$cor = \frac{1}{N} \sum ((x_j - \bar{x}) \cdot (y_j - \bar{y})) / (\sigma_x \cdot \sigma_y)$$

where \bar{x} is the mean of x_j and σ_x is the variance of x .

The data monitor sampler takes all samples in memory and continually calculates correlation values using this formula. As an example, you could define an event correlation data monitor that displays a correlation between the number of times a network is being reconnoitered, and if that is related to the number of attacks that the network is receiving.

Event Graph Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

This data monitor draws real-time diagrams of selected event activity. In effect, it does automatically and in real-time what you can do manually, as described in [“Graphing Attacks” on page 125](#).

Table 22-3 Event Graph Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.

Parameter	Description
Enable Data Monitor	Select this check box to "switch on" the monitor and collect data from the ESM Manager. If cleared, the monitor is "off" and displays no data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 118 .
Target Node Identifier	Choose an event attribute to use as the identifier for target nodes. The default attribute is Target Address. Note that while all attributes are available, not all are appropriate choices for this purpose.
Source Node Identifier	Choose an event attribute to use as the identifier for source nodes. The default attribute is Source Address. Note that while all attributes are available, not all are appropriate choices for this purpose.
Event Node Identifier	The fields that are available to use to uniquely identify the event type in a transaction.
Max Event Count	Set the greatest number of most-recent events the graphic will show.
Show Source/Target Nodes as	When one source-event target chains to another, you can choose to graph a source/target IP address as a single (simple) node, or to graph both the source and target instances of such an IP address (distinct).
Restrict by Filter	Choose a filter resource with which to restrict the events that the graphic includes.
Show Event Nodes	Choose a basis for visually expanding or aggregating event nodes, relative to their source and target node instances. See "Changing User Preferences" on page 556 for the option details.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

Event Reconciliation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 117](#).

The Event Reconciliation data monitor correlates events arriving from one sensor with events arriving from another sensor. When qualifying events occur on either or both sensors, the Event Reconciliation data monitor issues a new event to signal it.

You typically use this data monitor to determine the effectiveness of a firewall or IDS deployed in your environment.

One application is to place identically configured NIDS on either side of a firewall to determine which attacks are blocked by the firewall and which are not. Identical NIDS may also be wired in series to guarantee that none of the NIDS have been tampered with. Different NIDS may be wired in series to compare what each detects, either for evaluation purposes or to predict what attacks they may be missing as a group.

For example, you could define an event reconciliation data monitor that displays information about the number of events originating within the outside IDS (IDS1), and the inside IDS (IDS2), and the events that are filtered through the firewall. This presumes that

events have the same custom string 1 source address, and that the target address field values are similar.

The Event Reconciliation and [Session Reconciliation Data Monitors](#) are similar in many respects. Their main difference is in the way each handles the scope of reconciliation sessions. Event Reconciliation focuses on accomplishing a certain number of event matches; Session Reconciliation permits an indeterminate number of matches while appropriate events continue to occur.

Table 22-4 Event-Reconciliation Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>
Filter 1 Population Fields	Select a filter for the first device's event flow.
Filter 2 Population Fields	Select a filter for the second device's event flow.
Event Expiration Time	This is the amount of time (in seconds) that an event is kept in memory while seeking a matching event from the other device's event flow.
Correlation Interval	The interval (in seconds) to require between correlation events.
Correlate On	<p>Choose an event-receipt circumstance for generating a reconciliation event. The options are as follows.</p> <ul style="list-style-type: none"> • Matching Events • Filter 1 Events Only • Filter 2 Events Only
Correlation Thresholds	<p>This specifies the threshold(s) at which correlation events are created for the events specified in the Correlate On parameter. This field takes one number or a comma-separated list of three numbers. If you specify one number, it is used as the threshold for all the conditions. If you specify three numbers, they are applied respectively to the Correlate On values.</p>
Restrict by Filter	<p>Specifies whether to restrict the data monitor to a particular filter. Filtering reduces the number of events the data monitor has to process. From the drop-down menu, double-click a filter or accept the default to receive all events.</p>
Matching Time Window	The period of time (in seconds) within which two appropriate events need to be received to qualify as a match.

Parameter	Description
Matching Fields	The set of fields to consider when establishing whether two events match.
Filter 1 Fields	Fields passed by Filter 1 that can be included in resulting correlation events. These correlation events will contain a union of the Filter 1 and Filter 2 Fields.
Filter 2 Fields	Fields passed by Filter 2 that can be included in resulting correlation events. These correlation events will contain a union of the Filter 2 and Filter 1 Fields.
Availability Interval	Sets the number of seconds to use as the interval between data monitor updates.

The data monitor displays a table view of qualifying events. You can sort on individual fields to display the most interesting cases on top. The following fields generate correlation events.

Correlation-Event-Generating Fields

The Event Reconciliation Data Monitor displays a table view of qualifying events. You can sort on individual fields to display the most interesting cases on top. The following fields generate correlation events.

Table 22-5 Correlation-Event-Generating Fields

Correlation Event	Fields
Moving Average Event Fields (and the group-by fields are set)	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Custom Number 1	$\text{abs}(\text{count} - \text{moving_avg}) / \text{moving_avg} * 100$
Custom Number 2	$\text{count} - \text{moving_avg}$
Custom Number 3	statistics
Base Event Count	count
eventCategory, CustomString 1	if (count - statistics = 0): eventCategory = /datamonitor/movingaverage/threshold Custom String 1 = datamonitor:002 if(< 0) eventCategory = /datamonitor/movingaverage/threshold/fallingCustom String 1 = datamonitor:003otherwise: eventCategory = /datamonitor/movingaverage/threshold/risingCustom String 1 = datamonitor:004
Statistics Events (and the group-by fields are set)	
Event Name	Name of the data monitor
ArcSight Category	metaevent
Event Category	/datamonitor/statistics/<Statistics Name>

Correlation Event	Fields
Custom String 1	datamonitor:006
Custom Number 1	count
Custom Number 2	statistics
Correlation Data Monitor	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Event Category	/datamonitor/correlation
Custom String 1	datamonitor:007
Custom Number 1	Filter 1 count
Custom Number 2	Filter 2 Count
Custom Number 3	Correlation Value
Event Reconciliation (the rule chain and matching fields are set)	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Event Category	Event Reconciliation
Custom String 1	Filter 1 Events/Filter 2 Events/Matching Events
Event Type	Correlated

Geographic Event Graph Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

This data monitor draws a real-time geographic map of selected events. In effect, it does automatically and in real-time what you can do manually, as described in [“Graphing Attacks” on page 125](#).

Table 22-6 Geographic Event Graph Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	<p>Select this check box to “switch on” the monitor and collect data from the ESM Manager. If cleared, the monitor is “off” and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>

Parameter	Description
Max Event Count	Set the greatest number of most-recent events the map will show.
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the graphic.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

Hierarchy Map Data Monitor

The data monitor type is chosen when you create a new data monitor. (For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).) This data monitor draws an image made up of proportionally sized panels where each panel represents a group of events selected by group fields selected in the source node identifier. A source-node criteria could be a combination of fields.

Enhancements for ESM v.4.5

As of ESM v.4.5, the Hierarchy Map data monitor includes the following enhancements.

- The data monitor now shows the complete hierarchy, with the hierarchy path built not just by using the delimiter within a field value but also across different field values. (Previous versions of the data monitor did not show the complete hierarchy.)
- *Group By* fields now provide options to specify a list of delimiters for use by each selected Group by field. By default, no delimiters will be used, if no delimiters are specified then the whole field will be taken as a single level for hierarchy. (Previous versions built the hierarchy path within a field value based on only one type of separator, a forward slash, which did not support fields that use other separators like a backward slash, “\”, or a dot, “.”)

Group By fields also provide an option to set the maximum depth level of hierarchy within a field. The default depth level is equal to the number of delimiters in the field. Entering 0 for this option signifies no depth level for the selected field, effectively defining the field as a single-level hierarchy.
- A list of *Group Attributes* can be specified as a drill-down display to show when a user drills down into a group. For each attribute, the user can select a field and a function (max, min, count, average, count unique) on that field value.
- Enhanced visualization tools for *label*, *size by*, and *color by* provide fine-grained control of hierarchy map display with regard to Group By and Group Attributes fields and values.

Use Cases

Following is a list of example use cases for which the improved ESM v.4.5 Hierarchy Map data monitor would be a useful monitoring tool.

- Display the number of matches for all the rules within a given time frame, with the hierarchy groups based on the File path field of the rule audit events. The value will be the count of the events for each group. The goal would be to show which rules fired the most in a given timeframe.
- Show table space usage of ArcSight ESM correlation resources, particularly session lists and active lists.
- Show memory usage for ArcSight ESM correlation resources, particularly session lists and active lists.

- Show assets hierarchy by networks, zones and subnets. Within subnets, the assets can be sub-divided into asset ranges.
- Show assets hierarchy divided by the location of assets, where the value on the map is the count of the events targeting those assets.
- Show assets hierarchy divided by the location of assets, where the value on the map is the count of the assets within those locations.
- Monitor ArcSight ESM resource distribution; that is, how many rules, reports, data monitors and so on are being used in the system, where the count is system storage space.
- Display events by device to show how many events are generated from each device in a given time frame (for example, the past two days).
- Show assets by the number of attacks each receives, to determine which assets are the most vulnerable.

The following topics show how to create a hierarchy map data monitor. Woven into these topics is a simple example that shows how to map high priority, significant events and targeted systems.


Defining a Hierarchy Map Data Monitor

First, create a new data monitor and select **Hierarchy Map** as the Data Monitor Type in the Data Monitor editor. (For information on how to create a data monitor and define the type, see [“Creating a Data Monitor” on page 117](#).)

To define the details of the Hierarchy Map Data Monitor, specify these attributes in the editor.

Table 22-7 Hierarchy Map Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	Select this check box to “switch on” the monitor and collect data from the ESM Manager. If cleared, the monitor is “off” and displays no data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the graphic.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

Parameter	Description
Source Node Identifier	<p>This is a <i>group by</i> identifier. Blocks in the hierarchy map will represent events or objects that have matching values for all fields chosen here. Also, identifiers specified here will be available as Label By, Size By, and Color By choices on the displayed data monitor.</p> <p>Choose one or more event attributes by which to group events. The default attribute is Category Behavior, but you can include multiple attributes.</p> <p>For example, if you select only Category Behavior for this field, events will be grouped by category behavior (e.g., all events with a category behavior value of /Access will be shown in one block, all events with a category behavior of /Authentication/Verify in another block, and so on).</p> <p>If you select more than one source node identifier, each block in the hierarchy map will represent events or objects that have the same values for all identifiers.</p> <p>For example, if you select Category Behavior and Event Name as source node identifiers, then each block in the map will represent events of the same behavior and event name.</p> <p>See “Specifying the Source Node Identifiers” on page 701 for more information.</p>
Group Attributes	<p>Starting ESM v.4.5, you can specify one or more <i>group attributes</i> for fields with numerical values (e.g., calculate the maximum priority of all events in a field group). The attributes you specify here are shown as drilldown tooltips when you mouse over a field on a hierarchy map display. You can add these attributes by specifying a label, a field, and a function to apply to the field. The functions can be applied on numeric fields only. See “Specifying Group Attributes” on page 703 for more details.</p> <p>Also, group attributes specified here will be available as Label By, Size By, and Color By choices on the displayed data monitor.</p>
<div>  <p>If data monitor attributes are changed (edited) while a user is viewing the data monitor in a dashboard, the current data is flushed and the map defaults to red until new data arrives and the map display is redrawn.</p> </div>	

Adding Variables


To add a variable, click the Variables tab. For more on using variables in resources, see [“Variables” on page 784](#).

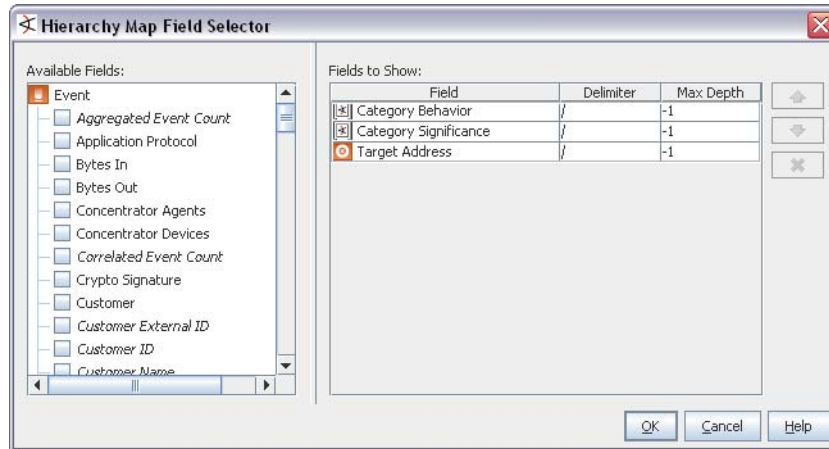
Specifying the Source Node Identifiers

Source node identifiers are “group by” attributes. For example, if you select only Category Behavior for this field, events will be grouped by category behavior. Each block in the hierarchy map will represent a different type of category behavior (e.g., /Authentication, /Authentication/Verify, /Execute Response/Informational, etc). If you select both Category Behavior and Target Address here, each block in the hierarchy map will represent events with the same category behavior on the same target system (IP address or host name).

To specify one or more Source Node Identifier (Group By) fields, click in the **Source Node**

Identifier field, then click the button  to open the Field Selector dialog. Specify the

fields by which you want to group events or objects by clicking Available Fields checkboxes, which adds them to “Fields to Show”. (To remove a field, select it under Fields to Show and click the delete button . Click up/down arrows to re-order fields.)



For example, we can group by Category Behavior, Category Significance, and Target Address. This will provide meaningful groups (events with the same category behavior, significance, and target address), and give us some interesting label, size, and color display options for mapping significant events and targeted systems on the data monitor.

Hierarchy Levels and Group Delimiters


You can specify how many levels of hierarchy you want to display for a field group by specifying one or more (a group of) delimiters and the maximum depth of hierarchy to display. For example, if you have a field value, <http://www.foo.com>, for which you have specified the depth level (Max Depth) as 2 with delimiters set to a group (consisting of `://.`), you will see:

- First level: <http://>
- Second level: <http://www.foo.com>

For the same example, if you set the Max Depth to 3, you get:

- First level: <http://>
- Second level: <http://www>
- Third level: <http://www.foo.com>

To select a field to display and set its hierarchy depth level:

- 1 Open the Hierarchy Map Field Selector dialog by clicking the browse button  that is displayed when you click in the Source Node Identifier field.
- 2 To add a field, check (click) the checkbox next to the field in the **Available Fields** scroll box. As you select a field, it will be displayed in the Fields column in the “Fields to Show” table on the right side of the dialog.
- 3 Double-click the **Delimiter** column for the field you just selected and enter one or more delimiters based on which you want to show the hierarchy depth.

By default, a forward slash (/) is set as the delimiter. To set a single level of hierarchy, delete the “/” and do not specify any delimiters. Also, set the **Max Depth** (as explained in the next step) to zero for that field. If you set a comma (,) as a delimiter, the hierarchy in the panel will display a backslash (\).

- 4 To specify the depth of the field hierarchy within a field, double-click the **Max Depth** cell for the field.



Negative integers are not allowed. If you enter a negative integer, it will default to -1 which represents a depth level equal to the number of delimiters in the field.

If you leave this field blank, it will default to a depth level equal to the number of delimiters in the field and -1 will be displayed in the Max Depth column.



To display the whole field as a single level of hierarchy, set the **Max Depth** value to 0.

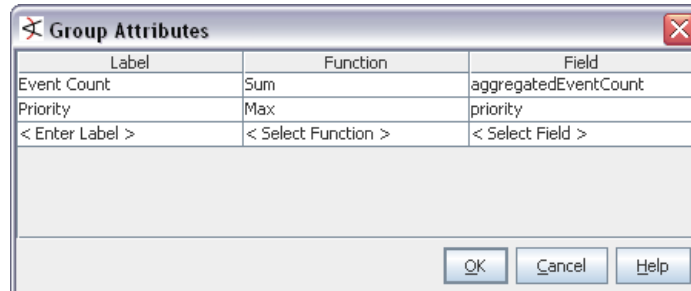
Specifying Group Attributes

Optionally, you can specify group attributes, which are functions on numerical fields. These attributes are shown as mouse-over tooltips on groups (blocks) on a displayed hierarchy map. They will also be available as label, size, and color options.

For each attribute you want to add, provide a label, a function, and a field to which to apply the function. This can be done on numeric fields only. For example, if you add an Event Count label, select the Sum function, and apply this to the aggregatedEventCount field, the function will find the sum of event count value.

To add group attributes:

- 1 Click the **Group Attributes** cell. A browse button  is displayed.
- 2 Click the browse button . The Group Attributes dialog opens.



- 3 Click the **Label** column and enter a name for the attribute you want to create. You can add multiple labels.
- 4 Click the **Function** column for a label and select a function to be applied to a field that you select in the next step. You can set a function for a numeric field only.
- 5 Click the **Field** column against a label and select a field to which to apply the function.

For example, we'll create two labels, Event Count and Priority, and map them as follows.

Label	Function	Field
Event Count	Sum	aggregatedEventCount
Priority	Max	priority

On the displayed map, the mouse-over tooltip on each block (group) will show both the event count and the highest priority event(s) included in that block. Also, specified group

attributes (Event Count and Priority, in this case) will be available as Label By, Size By, and Color By options on the data monitor.

Hierarchy Map Display and Visualization Controls

Once you create a Hierarchy Map Data Monitor, you need to add it to a dashboard to display it and make further adjustments to the display.

Map Display and An Example

If no dashboards are displayed in the Viewer, simply right-click the Data Monitor you created, and select **Add to Dashboard As->Area Map**. This will create a new, untitled dashboard and add the data monitor to it. (You can also add it to an existing dashboard.)

The hierarchy map shown in [Figure 22-5](#) is an example of the data monitor displayed on a dashboard.

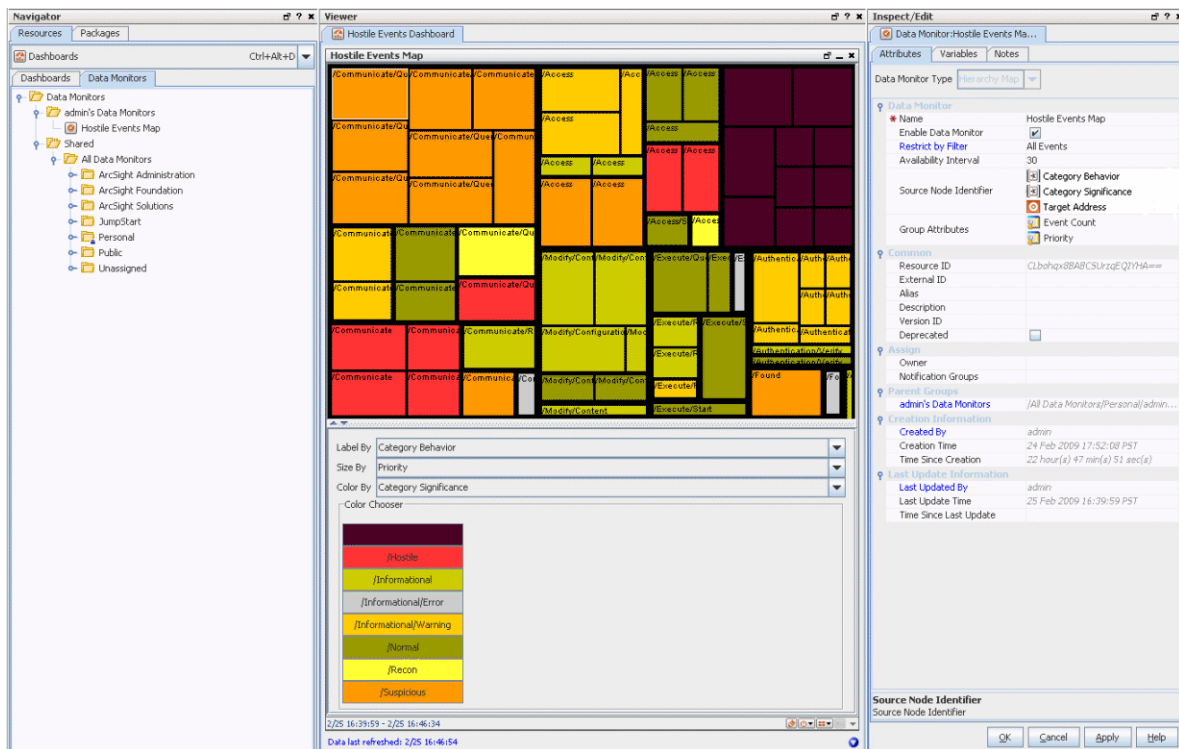


Figure 22-5 Example of a Dashboard with a Hierarchy Map Data Monitor. You can choose “Hierarchy Map” as the Data Monitor type when you create a new Data Monitor. To display the data monitor, add it to a Dashboard.



- Before you can edit the visualization controls on the Hierarchy Map data monitor, you need to first add the data monitor to a dashboard and display the dashboard, as described just before figure above.
- If data monitor attributes are changed (edited) while a user is viewing the data monitor in a dashboard, the current data is flushed and the map defaults to red until new data arrives and the map display is redrawn.

The **example** data monitor in [Figure 22-5](#) shows events grouped by category behavior, significance and target address. The labels show category behavior, and the blocks are sized by priority and colored by significance. Mouse-over tooltips show event count and priority for each group. Note that we can change the display on-the-fly by choosing a

different label, size, and color options. For example, instead of coloring the blocks by Category Significance, we could color by Target Address. Or, instead of labeling by Category Behavior, we could label by Target Address. In this way, we can get quick, real-time, graphical overviews of network activity and adjust options to emphasize different details.

Labels, Size, and Color Controls

The visualization controls for Hierarchy Map Data Monitors are **Label By**, **Size By**, and **Color By** controls. (You might need to float the Viewer panel and expand the floating Viewer to see these controls. See [“Floating a Console Panel” on page 556](#).)

- **Label By** - Select a label. The value of the label you select will be displayed on each block.



- The **default** for “Label By” is all the fields specified for the source node identifier and the event count for that grouping. This shows as “Default” in the field. (The values available for use in the Label By field come from the attributes defined for Source Node Identifier and Group Attributes fields on the data monitor Editor. See [“Source Node Identifier” on page 701](#) and [“Group Attributes” on page 701](#) for more information.)
- If “Label by” is set to something other than the default, the last (bottom-most) field value in the hierarchy will not show on the map because the custom Label by setting will overwrite it. However, data for all fields, including the last field, is always taken into account on the map.

Use the default “Label By” option to show/visualize the complete hierarchy, including the last field value.

- **Size By** - Select an identifier or attribute by which you want to size the blocks. Once you select the Size By attribute, the blocks will be resized proportionate to the value selected. Only attributes that have numeric values are available, because you cannot size a block based on a non-numeric value.



The values available for use in the Size By field come from the attributes defined for the Group Attributes field on the data monitor Editor. See [“Group Attributes” on page 701](#) for more information.

- **Color By**- Select identifier or attribute by which you want to color the blocks.



The values available for use in the Color By field come from the attributes defined for Source Node Identifier and Group Attributes fields on the data monitor Editor. See [“Source Node Identifier” on page 701](#) and [“Group Attributes” on page 701](#) for more information.

If you select a non-numeric field, you can change the color for any discrete value. If you select a numeric field, you get the option to select either a color for a discrete value or a color for a range of values. (For more on this option, see [“Selecting Colors for the Blocks” on page 706](#).)

After you select label, size, and color values, be sure to save the dashboard. The next time you open the dashboard, the attributes you saved will be applied to the next set of data.

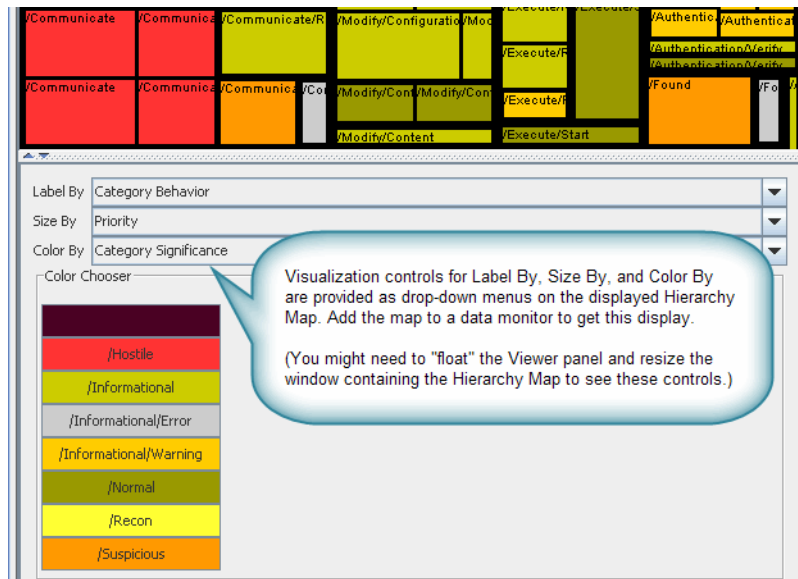


Figure 22-6 Label By, Size By, and Color By Controls. Format controls for the Hierarchy Map are available as drop-down menus on the map display in a data monitor.



After an edit of tree map attributes, there might be a time lag before there is a visual indication of the updates. You can force a redraw of the tree map by dragging the slider to resize the panel that contains the map.

Selecting Colors for the Blocks

You can color the blocks by selecting any of the Source Node Identifiers or Group Attributes that are displayed in the **Color By** drop down menu. For example, if you select Priority in the **Color By** menu, then all blocks that have the same priority will be displayed in the same color, such as all blocks with priority 1 may be displayed in red and all blocks with priority 2 may be displayed in blue, and so on.

If the Color By attribute you select is discrete but non-numeric, you can define the colors for each value of the attribute. For attributes that have numeric values, you can individually assign a color per attribute value or specify a range and assign a color for that range. However, if the Color By attribute is Priority, you cannot specify a range. This is because there are already predefined colors for each level of priority. You will be allowed to change a predefined color to a color of your choice for each priority level.

Below the Label By, Size By and Color By fields, is the Color Chooser box. This box displays all the values for the **Color By** group/field that you select. To individually assign a color for an attribute:

- 1 Click the **Discrete** radio button (This button is visible only if you selected a numeric Color By attribute).
- 2 Double-click a value button to open the **Color Chooser** dialog.
- 3 Select a color that you want to display for all the boxes for which that value is applicable.
- 4 Click **OK**.

All the boxes that have that value will be displayed in the new color.

You can set a threshold for the maximum number of discrete values for which you can set a color. Set the `console.ui.hmDataMonitor.discrete.threshold` property in the `console.defaults.properties` file. If the number of discrete values exceeds this threshold, for all values that cross the threshold, the color will be set to white.

To assign a color for a range of values (for numeric fields only):

- 1 Click the **Range** radio button.
- 2 Click **Add** button to set a range and a color for that range. The Add a color mapping dialog opens.
- 3 Select a value from the **Min Attribute Value** and **Max Attribute Value** menus to set the range.

For example, if you want to set a range for Priority that falls in 3-to-6 range, select 3 from the Min Attribute Value menu and 6 from the Max Attribute Value menu.
- 4 Click the Color Chooser button to open the color chooser.
- 5 Select a color by clicking it and click **OK**. The color you choose will be used to display all values falling in that range. In our range example in step 3, all blocks that display priority of 3, 4, and 5 will have the color you just chose for the 3-6 range.



If new data comes in after you change the color mapping but before you save the new mapping, you will get a dialog asking you whether you want to save the changed mapping. If you select **Yes**, the Data Monitor will not be refreshed with new data until you save the new mapping. When you save it, the new mapping will be applied to the existing blocks and all future data displayed on the dashboard.

If you select **No**, the new color mapping will be applied to the existing data on the dashboard, but will not be saved in the database. So, as soon as new data arrives, the new color mapping will be overwritten by the original color mapping that exists in the database.

Hourly Counts Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

The Hourly Counts Data Monitor displays the total count of events on an hourly basis along with their Priority. The hourly count for the first hour segment starts when you open the dashboard. For example, if you open the dashboard at 2:25 PM, though the first time segment displays **14:00 - 15:00**, the count will begin at **2:25 PM**.

Table 22-8 Hourly Counts Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .

Parameter	Description
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data.
Restrict by Filter	Choose a filter resource to restrict the data monitor's contents.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

As an example, you could design an Hourly Counts data monitor that displays hourly counts of data being collected, for example, the number of events that ESM Manager receives.

Last N Events Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

The Last N Events data monitor orders events based on its configuration. In the Table Viewer, the monitor displays the most recent events by Priority, Event Name, Protocol, and Category. With the BarChartTable configuration, the order is by Priority and Event Name. The PieChart configuration is ordered by Priority.

Table 22-9 Last N Event Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Restrict by Filter	Choose a filter resource to use as an additional restriction on the events displayed.
# of Events	Specify how many events the data monitor displays.
Field Names	Choose field names to include in the data monitor display. By default, the data monitor includes EventName, EventCategory, ArcSight Severity, and Protocol fields. You can select additional fields or remove currently selected fields by Shift or Ctrl-clicking field names in the drop-down list.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

As an example, you could design a Last N Events data monitor that displays the latest N events that meet the condition specified in the dashboard definition.

Last State Data Monitor



The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

This monitor is somewhat different than others in that it provides an extra level of abstraction that you can use to simplify the information presented to operators. Sometimes called "indicator lights" or "heads-up displays," these monitors show graphics that translate more complex values into simple, rapidly observable results such as green/amber/red "signal lights" or checkmark/asterisk/exclamation point symbols. "Last State" data monitors could also be called "most recently known state" monitors.

Last State data monitors are built on the information collected by [Active Lists](#). The qualifying events in active lists are identified on the basis of selected key fields such as Source Zone and Source Address (see [Data Fields](#)).

Having focused on the events that apply, you then select a field to use as the basis of the values the indicators will simplify. For example, the Priority field has a range of values you could divide into sub-ranges that you choose to translate into good/okay/bad groups.

With a value-range and status-scheme decided, you can map the field values to the status names, and the status names to the visual indicators operators will see.

In dashboards, you can see Last State data monitors as **Table** or **Tile** views. Click the **View as icon** () button at the lower-right corner to choose. When in Tile view, you can use the **Customize** button () to change the way data is ordered in the tabular (tiled) presentation. The customization choices are **by row-and-column** and **by cell**. Row-and-column is quicker to set up than cell because there are fewer adjustments, but cell does give you the option to set the contents of each tile in the data monitor.

In ArcSight v3.5 these tiled views are "fixed," meaning that the tiles in the array will hold their positions, relative to each other and to the dashboard.

Also in v3.5, you can right-click an entry in a Last State data monitor and choose **Remove Entry**. However, keep in mind the data monitor's **Availability Interval** setting. Removal does not visibly take place until the next refresh, during which time a new instance of the entry could occur. Depending on the entry and the interval, a removed entry may appear to have remained.

Table 22-10 Last State Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	<p>Select this check box to "switch on" the monitor and collect data from the ESM Manager. If cleared, the monitor is "off" and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>

Parameter	Description
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Use as Timestamp	Choose whether to use the device's reported end-time or the ESM Manager's receipt time as the definitive timestamp.
Restrict by Active List	Choose an active list from the resource tree to use as the primary guide for event selection.
Restrict by Filter	Choose a filter resource to use as an additional restriction on the events summarized through the indicators, if necessary.
Key Fields	Choose the fields to use as identifiers for the indicators, and the order in which to display them.
Value Fields	Select the field(s) that will provide the range(s) of values to be mapped into indicators, and the order in which they will be evaluated.
Mapping	<p>Use the Define Status Map dialog box in two steps: first, on the Statuses tab, to associate status Titles with Image graphics, then, on the Mapping tab, to associate Value items contained by the Value Fields with the Statuses titles just defined. Be sure to define and select one "catch all" status to react to values that may fall outside the range you set.</p> <p>In the Value field, associate only one value at a time with the Status values you've defined. For example, if the values 0, 1, and 2 should all be associated with a Status of "Okay," enter each digit separately and click Add.</p>
Max Number of Indicators	Set the greatest number of qualifying indicators the data monitor will show. If more indicators are generated, the displayed set will be the those with the most recent event traffic.
History Function	Use this option to add a Min or Max column to grid views that shows the minimum or maximum value for the indicator, over the most-recent time period specified by History Time Range.
History Time Range	Used with the History Function. The (most recent) period of time, in minutes, for which to retain minimum or maximum value information for an indicator. For example, a value of 60 could cause an indicator's Max column in a table to show its highest registered value over the previous hour.
Timeout	Used with the History Function. Sets the time limit, in seconds, after which the Min and Max column values are purged if not already updated.

Moving Average Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 117](#).

The Moving Average data monitor displays the moving average of events by a selected data field. The display provides a running count of events within a specified time frame and generates an event when the moving average changes significantly.

If a Moving Average data monitor is configured to display multiple graphs simultaneously, you can open it using the Statistics Chart or Tile format options described in ["Managing Dashboards" on page 114](#).

This data monitor calculates its statistics based on the number of requested samples. Until a full set of samples accumulate, the statistics approach their nominal value. This is indicated by appending /Partial to the event category if the values represent an incomplete sample. The purpose is to prevent false positives. This is most applicable to [/DataMonitor/MovingAverage/Threshold/](#) events.

When either the Moving Average or Statistics data monitors gain or lose a value grouping during processing (e.g., Priority), they issue an internal event. The data monitor's event categorization shows a Value/Add or Value/Remove suffix. This makes it possible to detect anomalous drops to zero, which can otherwise be missed if the monitor is removed because the discard threshold and a [Threshold/Falling](#) event could not be sent (due to exceeding the Maximum Alarm Frequency setting).

With ArcSight ESM v3.5 and newer, both the Moving Average and Statistics data monitors gained a new **Stats Value Field**. When used, this attribute focuses the monitor's statistical analysis on the numeric value of a specified field rather than on the quantitative flow of events. Analyzing numeric fields within events enables a broad number of possibilities for status monitoring, especially with custom strings and ArcSight [Audit Events](#).

Also with ArcSight ESM v3.5 and newer, a new **Value Calculation** field offers additional time-sensitive options for monitoring in second or minute increments. Monitoring per-second can catch abrupt spikes or drops; monitoring per-minute allows the same capability but may be more appropriate for larger integer values.

Table 22-11 Moving Average Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 118 .
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.
Sorted By	Sort by the values found in fields or by the percentage of change in those values.
Sampling Interval	Type the time interval used to calculate the moving average, in seconds. For example, if the Sampling Interval is 5 minutes, the moving average is calculated every 5 minutes. The default is 300.
Number of Samples	Type the number of Sampling Intervals to use to calculate the moving average, in seconds. The most recently stored Sampling Intervals are used to calculate the moving average. For example, if five Number of Samples are used, the last five Sampling Intervals are used to calculate the moving average.
Number of Visible Groups	Set the number of rows of results to display in the data monitor for each combination of ordering fields specified in the Group By parameter.

Parameter	Description
Value Calculation	<p>Controls the way the time-based accumulation of values is evaluated against the number of events involved.</p> <p>The default is Sum of values, which is the sum of all Stats Value Field event values.</p> <p>Average value per event divides the value by the number of events in the unit.</p> <p>Average value per second divides the value by the number of seconds in the unit.</p> <p>Average value per minute divides the value by the number of minutes in the unit.</p> <p>For finer time-sensitive value calculations, also consider using the Number of Samples and Sampling Interval so results are neither too shallow or too acute to be meaningful.</p>
Alarm Change Threshold (%)	<p>Specifies the moving average threshold, the percent change from the moving average, that will send a threshold exceeded event to the ESM Console. The threshold exceeded event is sent to the ESM Console and can be used to create a rule. For more information on rules, see "Creating Rule Actions" on page 310. Type in a percentage. The default is 50.</p>
Stats Value Field	<p>Specify a particular numeric field within events to use for statistical evaluation, rather than the overall flow of events. For example, specifying the Priority field would focus the data monitor on changes to the value of the Priority field in events, instead of on changes to the number of events encountered.</p> <p>The default is Aggregated Event Count, which is the sum of all aggregated events.</p> <p>Tip: Events can be <i>aggregated</i> at the Connector on specified fields. This pares down the number of events of the same type that the Manager must process.</p>
Restrict by Filter	<p>Specifies whether to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves. From the drop-down menu, double-click a filter or accept the default to receive all events.</p>
Group Discard Threshold	<p>Specifies the minimum event counts needed to generate a threshold exceeded event. For example, event count could change from 1 to 2, a 100% change that results in a threshold exceeded event. To prevent these types of changes from generating a threshold exceeded event, specify the minimum event counts needed. If you want all events generated regardless of the event count, type 0.</p>
Availability Interval	<p>Set the number of seconds to use as the interval between monitor updates.</p>

For example, you could design a Moving Average data monitor that displays the moving average of events on a per-source-address basis.

ESM also provides a report "ArcSight Reports/Custom Reports/Moving Average Report", in which you can specify the name of the dashboard as a parameter (same as the moving average event name), and specify the detect time range to report on.



You can also have a rule trigger based on the moving average of events coming in, independent of defining reports based on moving average events.

Rules Partial Match Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

Displays rules that have partial matches and the total number of partial match events within a specified time frame. For more information on partial matches, see [“Creating Rule Actions” on page 310](#).

Table 22-12 Rules Partial Match Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Number of Windows To Display	Type the number of Window Sizes to display. The default is 5.
Window Size	Specifies the time interval used to report partial match counts, in seconds. For example, if using 1 hour as the Window Size, each window displays partial match counts in hour intervals. The default is 3600.
Fixed or Sliding	Specifies when to begin the Window Size time interval. Choose Fixed to begin at time units, such as every hour, 1:00, 2:00, and so forth, or Sliding to begin at the current time and move backwards in Window Size time intervals. For example, if the window size is 10 minutes, and the current time is 1:15 PM and Fixed was selected, the window time frames would be 1:00 to 1:09 and 1:10 to 1:15. If Sliding was selected, window time frames would be 1:00 to 1:04 and 1:05 to 1:15.

For example, you could design a Rules Partial Match data monitor that displays all events that have partially matched and enabled real-time rule conditions, and are currently stored in memory.

Session Reconciliation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

The Session Reconciliation data monitor correlates events on the basis of their occurrence within a relevant time period, as established by a "session" event. When an event is qualified as session-initiating by the Session Filter, a session begins. The session persists until it times out or a new primary event occurs. Point events (occurring within the session time period) cause a correlation event that contains selected information from both events.

You typically use this data monitor to watch network devices that involve longer-term concerns, such as DHCP leases.

The [Event Reconciliation Data Monitor](#) and Session Reconciliation Data Monitor are similar in some respects. Their main difference is in the way each handles the scope of reconciliation sessions. Event Reconciliation focuses on accomplishing a certain number of event matches; Session Reconciliation permits an indeterminate number of matches while appropriate events continue to occur.

The Session Reconciliation data monitor automatically compensates for session-initiating events that arrive out of order.

Table 22-13 Session Reconciliation Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>
Restrict by Filter	Specifies whether to restrict the data monitor to a particular filter. This filter precedes the Session Filter and Point Filter . From the drop-down menu, double-click a filter resource.
Session Filter	The filter for those events that will initiate data-monitoring sessions. Compare to Point Event Filter.
Point Event Filter	The filter for the events that may match the events that initiate data-monitoring sessions. Compare to Session Filter.
Active Session Timeout	The time (in minutes) to allow before timing out a session if no new session events or point events occur.
Expired Session Timeout	The amount of time (in minutes) to retain a record of expired or replaced active sessions so that late or out-of-order point events can be properly processed.
Events to Generate	<p>Choose which types of correlation events are eligible to generate when session and point events match.</p> <ul style="list-style-type: none"> Point Event Matched Sessions - A session/point event-match occurred. A correlation event was generated containing the events' selected information. No Session Matched Point Event - A point event occurred without a live matching session. No information is included in the correlation event. Session Expired Event - Session expiration or replacement generates an event. Note that expiration or replacement is not complete deletion. Session Pruned Event - Complete deletion of the session generates an event.
Matching Fields	The set of fields to consider when establishing whether two events match.
Reporting Interval	The interval (in seconds) to require between correlation events.

Parameter	Description
Aggregation Threshold	The number of matches to use as the threshold for generating a correlation event.
Point Event Holding Period	The amount of time (in seconds) to retain point events to allow late or out-of-order session events to arrive and initiate sessions.
Session Inclusion Fields	The fields to add to the generated event, from the session-initiating event, when correlation occurs.
Point Inclusion Fields	The fields to add to the generated event, from the point event, when correlation occurs.
Availability Interval	Sets the number of seconds to use as the interval between monitor updates.

Statistics Data Monitor



The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

Provides a broader generalization of Moving Average data monitor functionality, except that it allows selection of other statistical methods in addition to Moving Average. Statistical methods include Average, Moving Average, Standard Deviation, Skew and Kurtosis, as well as Moving Average. These added capabilities could be used to detect anomalous behavior that could not be detected using moving average alone.

For example, monitoring the standard deviation of event data allows alarms to be triggered when there are sudden shifts in the rate of change of an event flow. This would allow alarms to be triggered when the protected network has been infected with a worm, but not when the network traffic rises due to normal use.

With ArcSight ESM v3.5 and newer versions, both the Statistics and Moving Average data monitors gained a new **Stats Value Field**. When used, this attribute focuses the monitor's statistical analysis on the numeric value of a specified field rather than on the quantitative flow of events. Analyzing numeric fields within events enables a broad number of possibilities for status monitoring, especially with custom strings and ArcSight [Audit Events](#).

In dashboards, you can see Statistics data monitors as **Statistics Chart** or **Tile** views.

Click the **View as icon** button () at the lower-right corner to choose. When in Tile view, you can use the **Customize** button () to change the way data is ordered in the tabular (tiled) presentation. The customization choices are **by row-and-column** and **by cell**. Row-and-column is quicker to set up than cell because there are fewer adjustments, but cell does give you the option to set the contents of each tile in the data monitor.

When either the Moving Average or Statistics data monitors gain or lose a value grouping during processing (e.g., Priority), they issue an internal event. The data monitor's event categorization shows a [Value/Add](#) or [Value/Remove](#) suffix. This makes it possible to detect anomalous drops to zero, which can otherwise be missed if the monitor is removed because the discard threshold and a [Threshold/Falling](#) event could not be sent (due to exceeding the Maximum Alarm Frequency setting).

In newer versions of ArcSight ESM (v3.5 and later) these tiled views are "fixed," meaning that the tiles in the array will keep their positions, relative to each other and to the dashboard.

Table 22-14 Statistics Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>
Alarm Trigger Condition	<p>Enter a conditional expression on which to trigger alarms.</p> <p>You can use any mathematical expression that employs these two variables: <i>c</i> (the count in the current Sampling Interval), and <i>s</i> (the calculated statistics value for that interval).</p> <p>For example, this expression would trigger when the current count goes beyond 500: <code>c >= 500</code>. An expression that triggers when the statistics reach 500 would be: <code>s >= 500</code>.</p> <p>As a matter of interest, the Moving Average data monitor is in effect a special case of the Statistics data monitor, based on this expression: <code>s != 0 && (abs((c - s)/s) * 100) > 0.5</code> where 50 is the percent of change you specify in the Moving Average data monitor.</p> <p>Concerning custom numbers for devices, <code>Custom Number 1 == variable c</code>; and <code>Custom Number 2 == variable s</code>.</p> <p>Please see “Data Monitor Expressions” on page 720 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.</p>
Group Discard Condition	<p>Enter a condition (a filtering expression) by which to remove certain result rows from consideration in statistical calculations, based on the result ordering set in the Group By attribute.</p> <p>Please see “Data Monitor Expressions” on page 720 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.</p>
Sampling Interval	Enter the time interval for recalculating event statistics, in seconds. For example, if the Sampling Interval is 5 minutes, the moving average is calculated every 5 minutes.
Stats Value Field	Specify a particular numeric field within events to use for statistical evaluation, rather than the overall flow of events. For example, specifying the Priority field would focus the data monitor on changes to the value of the Priority field in events, instead of on changes to the number of events encountered.
Number of Samples	Specify the number of most-recent Sampling Intervals to retain in memory and use to calculate event statistics. For example, if you set it to retain 5 sampling intervals, the last five periods (as specified in the Sampling Intervals attribute) are used to calculate the moving average.
# of Groups to Display	Set the number of rows of results to display in the data monitor for each combination of ordering fields specified in the Group By parameter.

Parameter	Description
Restrict by Filter	Choose to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves.
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.
Statistics Type	Choose the type of statistical calculation the data monitor will perform. The available types are Average, Identity, Kurtosis, Skew, Standard Deviation, and Variance.
Sorted By	Choose to sort results by value, sample count, statistics, or triggering criteria.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.

The Statistics Data Monitor is similar to the moving average data monitor; in fact, the Statistics data monitor specifying a statistics type of "Average" displays the same results as the Moving Average data monitor. The difference between the two is that the statistics monitor parses mathematical conditions rather than the fixed threshold values as they are used in the moving average event.

System Monitor Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

The System Data Monitor provides measurements based on ESM Manager internal monitoring system Java classes and attributes. A number of system monitors that may be particularly useful to ESM administrators are provided as predefined System Data Monitors that you can include in your dashboard displays to monitor system performance.

Table 22-15 System Monitor Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Monitor Types	From the drop-down menu, select the name of ArcSight Java class for which you want to display attribute measurements, for example, Throughput meter or Status

System Monitor Attribute Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

The System Monitor Attributes Data Monitor is similar to System Monitor, except that, rather than providing measurements for all attributes of a specified Java class, focuses on a single specific attribute of a given ArcSight Java class. (Used primarily for measurements on attributes that provide complex data structures.) A number of predefined system monitors are provided that you may want to include in your dashboard displays to monitor system performance.

Table 22-16 System Monitor Attribute Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118 .
Monitor Types	From the drop-down menu, select the name of ArcSight Java class for which you want to display attribute measurements, for example, Throughput meter or Status.
Attribute Name	Specify the individual attribute of the specified ArcSight Java class for which you want to display information. You can obtain the names of specific attributes in a class by viewing the results of a System Monitor defined for that class.

Top Value Counts Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 117](#).

Displays top events by selected data field, the total number of events, and the event Severity within the total number of events with the Table and BarChartTable viewer configurations.

Top Value Counts uses a new aggregation mechanism (in ArcSight ESM v.3.0 and newer) that precisely and predictably controls the time dimension of the data being evaluated. "Bucketized" means that the monitor evaluates a specific number of time-based event data units of a certain size (buckets). As time increments forward, the evaluation refreshes, using the most recent set of qualifying buckets.

Table 22-17 Top Value Counts Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name.

Parameter	Description
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the ESM Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 118.</p>
Bucket Size in Seconds	<p>The time dimension for individual event data units. A number of these units make up the value used in Number of Buckets. For example, you might use a value of 300 to create five-minute buckets. Bucket size and frequency (increasing freshness and resolution) does have a performance cost so it is wise to set buckets to run only as small and fast as actually necessary.</p>
Number of Buckets	<p>The overall time dimension to evaluate, expressed as the appropriate number of Bucket Size units. For example, to evaluate the most recent hour using five-minute buckets, you would enter 12. Bucket size and frequency (increasing freshness and resolution) does have a performance cost so it is wise to set buckets to run only as small and fast as actually necessary.</p>
Time Field	<p>Choose the specific event timestamp to use to apply events to time buckets.</p>
# Top Entries	<p>The number of entries to show as "top" values.</p>
Restrict by Filter	<p>Choose to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves.</p>
Aggregate Field	<p>Specifies which data field to monitor. For example, if monitoring top 10 source IP addresses, select the Source Address data field from the drop-down menu. For more information, see “Data Fields” on page 633.</p>
Value Field	<p>Specify what the data monitor will use when determining the top value counts: the number of matching events, or the sum of a particular data field value in all matching events.</p> <ul style="list-style-type: none"> To count events, leave this field empty. (This is equivalent to selecting the Aggregated Event Count field. When the Value Field is not specified, the data monitor uses the data field specified in the Aggregate Field to count events.) To sum the values from a particular data field, use the data field selector for the "Value Field" attribute to select the desired field. <p>In either case, counts from aggregated events will be properly adjusted.</p>
# of Distinct Events	<p>Specify how many events the data monitor holds internally. It is important to limit the number of events in order to conserve ESM Manager resources, especially when there can be a very high number of distinct data field values.</p>
Availability Interval	<p>Sets the number of seconds to use as the interval between monitor updates.</p>

Data Monitor Expressions

Certain data monitor parameters can specify their own conditional expressions with which to flexibly define triggers or results. For example, you use these expressions in the Statistics data monitor's Alarm Trigger Condition and Group Discard Condition parameters to evaluate when to send an alarm or to remove result rows from statistical calculations.

The type of expression supported is a conventional infix mathematical expression with each basic expression separated by parentheses.

All common arithmetic operators are supported. Boolean operators are also fully supported and Boolean expressions evaluate as either 1 or 0 (true or false).

Supported Data Monitor Expression Operators

All common arithmetic operators are supported. Boolean operators are also fully supported and Boolean expressions evaluate as either **1** or **0** (true or false).

Operator	Symbol
Power	\wedge
Boolean Not	!
Unary Plus	+ x
Unary Minus	- x
Modulus	%
Division	/
Multiplication	*
Addition	+
Subtraction	-
Less Than or Equal	<=
More Than or Equal	>=
Less Than	<
Greater Than	>
Not Equal	!=
Equal	==
Boolean And	&&
Boolean Or	

Supported Data Monitor Expression Functions

Name	Function
Sine	sin()
Cosine	cos()

Name	Function
Tangent	tan()
Arc Sine	asin()
Arc Cosine	acos()
Arc Tangent	atan()
Hyperbolic Sine	sinh()
Hyperbolic Cosine	cosh()
Hyperbolic Tangent	tanh()
Inverse Hyperbolic Sine	asinh()
Inverse Hyperbolic Cosine	acosh()
Inverse Hyperbolic Tangent	atanh()
Natural Logarithm	ln()
Logarithm Base 10	log()
Angle	angle()
Absolute Value / Magnitude	abs()
Random Number (between 0 and 1)	rand()
Modulus	mod()
Square Root	sqrt()
Sum	sum()

Device

Please see [“Assets” on page 581](#) for a discussion of network devices.

Event Inspector

The Event Inspector is a tool for examining [Events](#) details. It is located in the ESM [Console](#)'s Inspect/Edit panel. To open the Event Inspector, double-click an event line in a grid view (see [“Views” on page 800](#)).

There are two panels in the Event Inspector. The top panel displays selected events with associated rules. The events listed here have a set of right-click menu commands similar to

those described in [“Using Grids” on page 105](#). The bottom panel displays event details for one or more events that have been selected from the top panel. If you select more than one event from the top panel, only their common values are displayed in the bottom panel.

The Event Inspector can display the chain of events that trigger a rule (see [“Rules” on page 753](#)) and generate a correlation event. From the Event Inspector you can view each event and rule in the chain for details.

Depending on the information available for an event, you may also be able to review its business significance in the Impact Analysis tab or its actual content in the Payload tab.

See also: [“Inspecting and Editing” on page 66](#).

Field Sets

The overall set of event-attribute fields is defined in [Data Fields](#), but you can make or use custom subsets with the Field Set Editor (see [“Field Sets” on page 723](#)). Choose a set name to see only that predefined set of fields.

Events

Events begin at network [Devices](#) that can sense and record instances of security-sensitive activity. Examples include a database record change, a syslog entry, a firewall transit, a router access, or scanning a door access card.

Such initial events are typically recorded in logs, and are sometimes called **base** or **raw** events.

When numerous source devices are reporting large volumes of relatively similar events, it is desirable to funnel these events through central event **concentrators** that forward a much-reduced set of representative or summary events.

When these events reach ArcSight [SmartConnectors](#), several things can happen.

- All received events are **normalized** (restructured) to make their information consistent and ready for analysis.
- All received events are **categorized** (appended with classification information) using ArcSight's event categorization taxonomy.
- If appropriate and the SmartConnector is configured to do so, events are **aggregated** to issue fewer and more meaningful events and to reduce network traffic.
- If appropriate and the SmartConnector is configured to do so, selected events are **filtered** out, to eliminate them as a further traffic or processing burden.
- For certain devices, the option may be available for the SmartConnector to apply analysis rules to incoming events and to issue **correlation** events concerning them.

At SmartConnectors, filtering **removes** events from the system. Aggregation **replaces** events with fewer new ones bearing summary information.

When the events from SmartConnectors pass to ESM [Managers](#) they can again be considered **base** events in the sense that they are in a state prior to processing. More specifically, any event within ESM that is subject to further processing, even if the result of previous processing, can be considered a base event.

All base events entering the ESM Manager are subject to:

- **Correlation** to derive more intelligence from the events. Correlation **adds** new events containing the results of correlation activity. You apply correlation through the ESM rules and data monitors in their respective resource trees of the Navigator panel. Correlation events have flash icons in grid views.
- **Filtering** to selectively see and report on events. Filtering within the Manager does not actually discard events. You apply filtering with the resources in the Filters tree in the Navigator panel.

Note that all aggregation actually occurs at SmartConnectors, not within the ESM Manager. You apply aggregation through the resources in the [Rules](#) tree of the Navigator panel.

Strictly speaking, within ESM there are only **base**, **aggregation**, and **correlation Events**. It is important to note that any such event in the system can (if the right rules and data monitors are present) become the input to produce new correlation events. You should also note that the Manager's rules engine is designed to prevent infinite loops.

Apart from the events that originate on the network, and the correlation events ESM issues in response to them, ESM generates many other events of its own for a variety of purposes.

These internal events can be divided into [Audit Events](#) and [Status Monitor Events](#). You can use audit events to track, or react to, system **activity** at all levels of operation from data monitors to the database. [Status Monitor Events](#) are valuable for getting system **state** information. Please review these topics ("[Audit Events](#)" on page 583 and "[Status Monitor Events](#)" on page 766) to become familiar with the characteristics of all the available events.

You can apply all ESM analytic tools to any events present, whether base or correlation, originating externally or internally.

Field Sets

Field sets are named subsets chosen from the available [Data Fields](#). Field sets can help you quickly focus a grid view, Event Inspector, or other field array on a particular context such as customer accounts or vulnerability.

Field sets are a shareable resource that you can manage and apply through the Field Sets resource tree in the Active Channels section of the Navigator panel. (In the Navigator, choose **Active Channels**, and click the **Field Sets** tab.) These field sets also support the new [Variables](#) data fields. Field sets supercede and include the previous concept of column sets.

ESM comes with a list of default field sets for out-of-the-box use, and to serve as examples.

See "[Using Field Sets](#)" on page 101 (in [Chapter 7, Monitoring Events](#), on page 91) for information on how to create custom field sets, modify existing ones, and share them with other ESM Manager administrators or operators.

See "[Sortable Field Sets](#)" on page 765 for information on creating and using sortable field sets.

See "[Using Field Sets](#)" on page 623 (in the [Common Conditions Editor](#) reference topic) for information on how to access field sets to build conditions.

Filters

You use filters to specify criteria that narrows the scope of monitored data and reduces the number, or constrains the nature, of the [Events](#) displayed through the [Console](#). Filtering criteria are based on the Console's event [Data Fields](#), used in various combinations and with various conditions placed on their content. As you apply more restrictive filter parameters, the number of events reaching the Console may decrease, but the likelihood increases that the events are significant.

For example, you can create a filter that contains every firewall for the western region of the United States, and create another filter that contains every Intrusion Detection System (IDS) for the same region. You can also be more specific, by creating a filter wherein you only want to view firewalls and IDSs with certain IP addresses because they are labeled as **suspicious** IP's or IP's that may pose a possible threat to an enterprise. On the other hand, you can create filters that only contain networks that are labeled as **friendly** and seem to pose no threat at all, but you still want to monitor them. For display purposes, you can select a unique color for any filter. If an event matching the filter's conditions is generated, the event appears in the grid view in the specified color.

Applying filters to get optimum results is a core skill for network security analysis. While it isn't possible to anticipate specific solutions here, you should know the most efficient way to use the ESM Console's filtering tools.

Filtering Options


In the Console, filtering is available in multiple ways, and how you choose to use these options can have a significant effect on your ability to precisely, flexibly, and rapidly author new analyses over the long term.

The primary event-filtering options are:

- **Filters resources:** The Navigator panel's Filters resource tree is (or should be) your master repository for filtering solutions. Using the Filters tree is the best way to work out an organized filter library. You can and should use the filters you develop here, through the Filters Editor, in other resources such as active channel views, reports, or rules. You can even use filter resources in other filter resources. By basing your solutions on hierarchical, resource-based filters, you gain the type of leverage granted by stylesheets.
- **Active Channels resources:** The active channel resources in the Navigator panel can each store an individual filtering solution that is unique to a given channel or based on a Filters resource. When you use an existing active channel to create another, you carry forward and perhaps modify its filter.
- **Active Channel Editor:** You use the Active Channel Editor to create or modify the filters in individual active channels. Changes you make to active channels through this editor are limited to those channels and channels created from them. Such changes shouldn't be considered long-term or enterprise-wide.
- **Inline view filters:** In any active channel grid view you can use the fields of the grid's top line to select filtering event-attribute values for certain columns, which will be used with implied AND operators to impose ad hoc filters. These filters are not retained with the prior active channel, but you can give the revised channel a name and save it through the Active Channel Editor.
- **Event-based filters:** Another quickly applied and contextual category of event filtering is offered by the event-attribute **Investigate** command. When you right-click an event attribute in a grid view you can choose Investigate and one of several filtering options that vary based on the data involved. Like inline filters, **Investigate**

filters apply only to the current view and are temporary unless saved in a different named view.

- **Inline Filters:** You can add an inline filter to a channel view by clicking the Edit Inline

Filter () button at the top right of the grid view to display the inline filtering fields. (For more information see, [“Filtering Grid Views with Inline Filters” on page 109.](#))

You should always remember that your most primary filter is the one imposed by your ESM system administrator. Each ESM user operates under the constraints of the access control lists (ACLs) configured for their user identity. These ACLs automatically filter out some portion of the total available event flow before it reaches you. Any filter you use or create adds to this fundamental constraint.

For more about putting filters to work, see [“Managing Filters” on page 480.](#)

Grid View

A grid view is a type of view in the ESM [Console](#), or in an [ArcSight Web](#) client, that shows [Events](#) summary information organized in rows and columns, or other types of information such as for certain [Resources](#). As new events occur, they are inserted at the top of the grid as new rows. Rows contain events while columns contain data fields. You can learn about working with grids in [“Using Grids” on page 105.](#)

iDefense

If your ArcSight ESM system is integrated with a VeriSign iDefense database, you can view iDefense incident reports for events that have vulnerabilities associated with them.

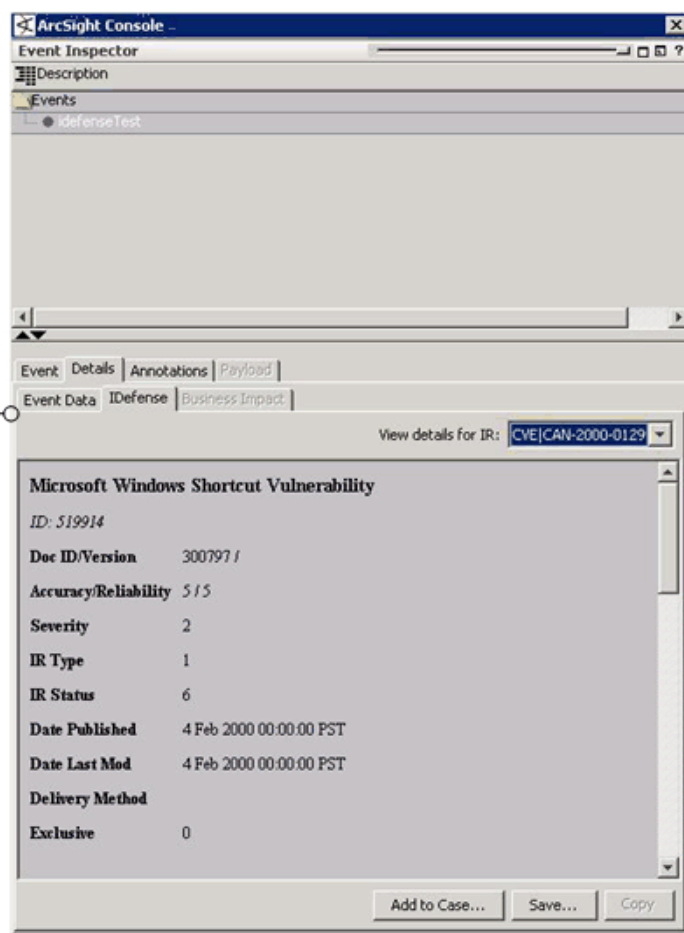
To view iDefense information for an event:

Select an event in a channel, right-click, and choose Show Event Details.

If there is iDefense information available for the selected event, the iDefense tab will be enabled. Click the **iDefense** tab, then choose an incident report from the **View details for IR** menu at the top right of the iDefense sub-tab. The reports are displayed on the iDefense tab.

This option is available only if you have the third party iDefense software installed and configured to interact with the Arcsight ESM, and if the selected event has a vulnerability ID associated with it. In that case, an iDefense tab is available as a sub-tab under the Details tab for the selected event. The iDefense reports provide more details on the vulnerability.

Typically, multiple incident reports are available for a selected event. To view a report, choose a report name from the **View details for IR** drop-down menu.



Inspect/Edit Panel

Located on the right side of the ESM [Console](#), the Inspect/Edit panel contains all the various [Resources](#) editors you use to create and modify analytic tools, as well as the Event

Inspector you use to examine the contents of [Events](#). Using the Event Inspector and the resource editors is explained in the topics that relate to events and those resources.

Job Scheduler

See [“Scheduling Jobs” on page 756](#).

Knowledge Base

The Knowledge Base is a problem-solving database that can contain information on event data, associated if-then-else rules, cases, and so forth. All information is derived from community expertise within your enterprise or based on your internal practices and policies.

Compare Knowledge Base articles to [Reference Pages](#), which provide built-in reference information about certain resources.

When you create a Knowledge Base article, you provide a URL or directory path to a specific vulnerability or exposure. You can add notes to Knowledge Base articles to relay information about the article. Using a note, you can write reminders, messages to the next shift, or any related information. Articles display in the Console or in an ArcSight Web client, with associated links and article information. Knowledge Base articles are stored in these default groups:

- **Shared:** lists Knowledge Base groups and articles to which the logged-in user has access:
 - ◆ **All Knowledge Base:** lists all ESM user Knowledge Base groups and articles.
 - ◆ **Personal Knowledge Base:** lists each user's own Knowledge Base groups and articles.
 - ◆ **Public Knowledge Base:** lists Knowledge Base groups and articles accessible to all users.
 - ◆ **Unassigned:** lists Knowledge Base articles that do not belong to a group.

Logical Operators

This table describes the logical operators you can use in condition statements. Certain operators don't appear in circumstances where they are not applicable.

Logic Operator	Description
=	equals Use this operator when the entire string is known, such as for an event Name or User name.
!=	not equals Use this operator to exclude one or more known values, such as events involving a specific network domain or user.
<	less than
<=	less than or equal to
>=	greater than or equal to
>	greater than

Logic Operator	Description
Between	event occurs within the specified date-time bracket
In	standard SQL operator for membership test
Contains	contains the specified substring Use this operator to exclude a large set of events, such as all events whose name contains "virus." Use this operator with caution as it is relatively slow and prone to matching more events than you intended.
StartsWith	starts with specified substring Use this operator for testing URIs such as event categories or resource locations (e.g., Customer or Connector locations in their respective Navigator trees), or to test the root of a hostname (e.g., if your web servers are named WebServer1, WebServer2, etc., you could use "hostname startsWith WebServer").
EndsWith	ends with specified substring Use this operator for domain names. For example, you might want to match events involving the .mil domain.
Like	standard SQL operator for simple pattern matching for string type: "_" wildcard for single character; "%" wildcard for multiple characters
Matches	for extended regular expression pattern-matching for string types using Perl 5 syntax Supports regular expressions (regex). Note that Matches is used in rules only.
InSubnet	for IP addresses in the specified subnet
InActiveList	event appears in the specified active list
On	event occurs on this date
Is	tests true for the selected state, null or not-null Use this operator to test whether or not a value has been supplied. You would use this in rules to tell the difference between a string that does not match versus a string that was not supplied. For example, you could use this to find all events that were missing their event names.
BitAnd	equals, for bitmap fields

Managed Security Service Providers (MSSPs)

Managed Security Service Providers (MSSP) can use slicing and dicing query-trend approaches to create focused reports for multiple customers built from what are initially broad range queries.

Manager

The ESM Manager is the component that manages, cross-correlates, filters, and processes all security-event occurrences in your enterprise. The ESM Manager includes a Cross-Correlation Engine, Connector Data Manager, tracking and resolution functions, and analytics and reporting capabilities. The ESM Manager also accesses the ArcSight Database.

Navigator Panel

Located on the left side of the ESM [Console](#), the Navigator panel contains all the trees you use to organize analytic and operational [Resources](#), tools, and targets. These resources come in many types, such as active lists, connectors, rules, and users, all of which are summarized in the topic ["Navigating" on page 58](#).

Notifications

"Notifications" usually refers to the event-related messages ESM can send to e-mail addresses, pagers, or cell phones.


Sending notifications is one among several rule actions that can be performed when a rule is triggered (See ["Rules" on page 753](#)). When you create a rule and add a Send To Notifier action, you will be able to select the notification group that will receive the message. For more information on rule actions, see ["Creating Rule Actions" on page 310](#).

The key entities in the notification structure are Notification Groups, Escalation Levels, and Destinations.

Notification Operation

When a rule that has a notification action triggers, the ESM notification engine notifies all **active** destinations in the first escalation level within that group. The notification engine then waits for a certain time period to receive an acknowledgment to that notification.

You can acknowledge notifications by any one of these methods:

- Reply to the e-mail or page (requires a two-way pager), depending on the type of destination.
- Click the **Notifications** button () in the Console's toolbar to use the Notifications Manager in the Viewer panel. (See ["Managing Received Notifications" on page 482](#).)
- Use ArcSight Web's Notifications feature to read and respond.

The length of time that the notification engine waits for acknowledgement depends on the event severity, and can be configured through the context (right-click) menu's Wait Time setting.

If no acknowledgment is received within the specified time interval, the same notification is escalated to the next level within the group.

This process repeats until there are no more escalation levels or the notification is acknowledged by any of the recipients. The one exception to this procedure is the escalation procedure carried out for **informative** notifications (the Informative option was set while defining the notification action in the rules editor). In this case, notifications are only sent to the first escalation level in the group and do not require acknowledgment.

SMTP is used to send e-mail. An SMTP server must be configured either at install time or through Context (right-click) menu e-mail settings. For notifications, the relevant fields are "from address", which designates the e-mail address of notification e-mail sent from ESM, and the "outgoing e-mail server," which is the SMTP server ESM uses to send e-mail. It is important to ensure that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses.

POP3 and IMAP can be used to check for e-mail acknowledgments. You can specify these options at install time, or through Context (right-click) menu e-mail option settings. For acknowledgements, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager providers with host and port information using the Context (right-click) menu Pager Settings option.

Notification Groups are the point of interface between the rules engine that specifies the notification action and the notification engine that sends out the notification. Within each notification group, there can be any number of escalation levels. Each escalation level can contain multiple destinations.

ESM provides the following groups to assist you manage and organize groups and destinations.

Destination Group	Purpose
Shared	Notification groups and destinations to which logged-in users have permission.
All Destinations	All groups and notification destinations (only Administrators have permissions to this group). Administrators who have inspect and edit permission on the All Destinations group also have permission to change notification settings.

Testing Notification Escalations

Escalation procedures are tested by generating an internal Low Severity event. This event triggers the escalation within the group tested as though a real Low Severity event occurred. Notifications are immediately sent to all destinations within the 1st level (1). If 1st level destinations do not respond to the notifications within the set wait time for Low Severity events (default is 2 hours), the test notification escalates to the 2nd level (2), and so on.

Notification Destinations

Notifications are sent to destinations. Notification destinations may optionally be associated with a user, and when that is done, destination information, such as e-mail address, phone, and pager number, is automatically populated from the user's profile. You can also change the user's destination information without changing the user's profile.

Each destination can be an e-mail, pager, or cell phone contact and have an associated start and end time, which is the time period during the day when the destination is expected to be active. Each destination can also be optionally associated with a user. Associating a destination with a user has these effects:

- When the destination receives a notification and the user is logged into an ESM Console, the user is notified through the notification status button on their display.
- Notifications sent to this destination can also be seen and acknowledged by the user in an ArcSight Web client.

Notification destinations can be managed with drag and drop functionality. You can move or copy notification destinations into escalation levels within the same or other notification groups from the Administration window. If a group is deleted, the destinations within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Notification Acknowledgements

Once you receive a notification, it is important that you acknowledge it within the allotted time window, to prevent automatic escalation to the next-level notification destination.

Immediately acknowledging and resolving significant events is crucial to securing any enterprise. Use the ESM Console's Notifications Manager, or an ArcSight Web client, to check status and help resolve issues. (See also ["Managing Received Notifications" on page 482.](#))

Packages

A **Package** is an ESM resource that contains a set of related resources. A package of resources can be installed or unloaded as a unit. ArcSight Solutions are delivered as packages, but you can create your own packages, as well.

A **Bundle** is a file (with extension `.arb`) that contains one or more packages. You can import and export bundles and install and uninstall the packages that the bundles contain. When you import a bundle, the source file is saved as a file resource (see ["Managing File Resources" on page 488](#)). You can view the original package contents (the package archive) or the current package contents at any time.

An **uninstalled package** is a package that has been imported or created, but not yet installed in the system resource tree (see ["Resources" on page 746](#)). Packages that have been installed can also be manually uninstalled. The default behavior is to install the package when it is imported.

When a package is deleted, the resources it contains can be left in the system resource tree or they can be deleted along with their package.

Packages can have dependencies on other packages or on ESM features such as Pattern Discovery. Two ArcSight Solution packages may share a third package in common, for example.

See also: ["Managing Packages" on page 491.](#)

Partitions

Because the amount of security-event information retained in the ArcSight [Database](#) can be voluminous, it is important to be able to "package" chronological sections of past data for archiving and reasonable retrieval and reuse.

Since ArcSight ESM v2.5, ArcSight has offered integrated, automatic database partition management. The Database Partition Manager and its initial configuration are established during installation, as described in the ESM Installation and Configuration Guide. In ArcSight ESM v3.0 and newer versions, the ESM [Console](#) makes it possible for

administrative users to supervise partitioning activity through a Partitions resource tree in the [Navigator Panel](#).

A database partition is a time-delimited record of database activity. The default period is a day. You use partitions as a means of controlling, storing, and restoring volumes of past security-event information to facilitate later forensic analysis and auditing.

The overall database partition lifecycle includes active (in the database), inactive (archived outside the database), and reactivated (restored to the database) phases. Partitions are generated automatically per schedule, and remain in the Active Partitions branch of the Partitions resource tree according to the time limits set initially during installation. Once a partition's upper bound passes beyond the lower bound of the retention period, it is archived and compressed and refiled in the **Archived Partitions>Inactive Partitions** branch. Once archived, it remains there unless you reactivate it, which moves it to the **Archived Partitions>Reactivated Partitions** branch.



Notes:

- Only partitions beyond the current retention period are eligible for archiving.
 - Only ESM users with Administrator privileges can interact with the Partitions resource tree.
 - With Oracle databases, past partitions can be compressed online, stored offline, and be restored to the database at any time.
-

For information on working with partitions from the ESM Console, see [“Managing Partitions” on page 547](#).

Pattern Discovery

ArcSight's Pattern Discovery can detect subtle, specialized, or long-term patterns that might otherwise go undiscovered in the flow of events. This topic discusses pattern concepts. To use pattern discovery, please see [“Pattern Discovery” on page 127](#) in [Chapter 7, Monitoring Events, on page 91](#).

A pattern is a distinct, repeating network transaction (event) that is uniquely identified by its source and target IP addresses. Patterns are further qualified by the involvement of selected attributes such as event names or categories. There are, of course, many such patterns and most are normal or benign. The point is to establish and mask out normal traffic in order to let new or atypical traffic stand out. Separating “signal from noise” in this way makes possible very early (day zero) detection and very subtle (low and slow) detection. Once detected, such traffic can be analyzed or responded to using all of ESM's capabilities.

Pattern discovery uses a **profile** to specify potentially qualifying events on the basis of attributes and time spans. When you apply a profile, manually or on a schedule, it captures a **snapshot** of the events that did qualify, on the basis of raw associations. The contents of snapshots are then reviewed by an analyst to identify event **patterns** to explore in pattern views or the Pattern Inspector.

You define profiles in the Profile Editor in the Inspect/Edit panel. You manage your profiles, snapshots, and discovered patterns through the Profiles, Snapshots, and Patterns tabs of the Navigator panel's Patterns resource tree.

You use the Viewer panel to observe the graphical results of executed snapshots and the patterns those snapshots discover.

Pattern Concepts

A pattern can be any recurring relationship between one or more pairs of source and target IP addresses, that you deem to be significant in relation to certain event attributes. You can regard the patterns you discover as benign or hostile, depending on your policies and postures.

Event-pattern profiles are also constrained by Start and End time limits, filters, and by minimum numbers of associated events (pattern length) and times discovered (occurrences, or pattern support).

Once captured in snapshots, you can examine the event data as raw association information in graphical snapshots, or as graphical patterns in the Patterns tab of the Patterns resource tree.

Each box in a pattern view represents one pattern. The line items in the box are the individual events that were discovered to have associations. Each event component of a pattern (box) relates to the chain of links from which the pattern was derived, in the visual snapshot.

A snapshot view is a graphic hierarchy of related event nodes. The "support" value for each node is the number of times that event occurred in conjunction with its related events. This overall hierarchy is a raw presentation of the events, useful for analysts but not meaningful to operators.

The discovered events all share the attributes specified in the profile. The pattern-discovery process first tests for equality in the values found for the specified attributes. Secondly, it tests for a selected transaction scheme. When the specified minimum number of event relationships reoccur, a pattern exists.

Discovering Patterns

ESM identifies patterns by first dividing the event stream into multiple transactions. For example, all of the events with a given source and target IP address may constitute a transaction - they represent all the traffic flowing from that source to that target. It may also be helpful to cluster transactions into super-transactions to identify patterns that involve cascading exploits toward multiple devices (that is, device A attacks device B which, in turn, attacks device C).

The events occurring in each transaction are then characterized using a subset of the event fields (e.g., the event name or the event category).

Finally, events that frequently occur together in multiple transactions are identified and grouped together. These events are further sub-grouped by support level. For instance, events A and B may occur together 2,000 times while events C and D occur in the same transactions but only 10 times. Pattern Discovery would create two patterns in this case: one for A and B and a second one for C and D. To give another example, events F, G, and H may occur together in the same transactions 100 times while F and G occur without H in 5 additional transactions. All of these occurrences would be rolled together into the same pattern. F and G would have a support of 105 while H would have a support of 100.

Pattern Analysis

Pattern analysis, overall, falls into two basic phases: initial collection, identification, and sorting, and on-going routine processing.

Initial Phase

To accomplish phase one, you generally use broader profiles and more frequent snapshots in an attempt to capture examples of **all** the patterns that appear in your networks.

Once collected, there is a period of initial analysis in which you identify the patterns that are normal or benign. Making these evaluations requires in-depth knowledge and familiarity with the traffic in your enterprise, as well as using ESM's analysis tools. There is no set procedure for this basic collecting and sorting process.

However, the best method for moving officially "uninteresting" patterns **out** of the analysis workflow is to use annotation. While it is possible to use filters for this purpose, it is more reliable to move patterns by annotation to a stage such as **Closed** because this assures that the pattern has actually been inspected and classified.

Routine Pattern Processing

In an environment where the routine event patterns are mostly known and appropriately classified, you focus on the new and as-yet unclassified.

The basic approach to routine pattern analysis consists of two phases: managerial (or triage or workflow initiation), and analysis.

Workflow Management

As ArcSight Pattern Discovery turns up new or unclassified patterns, a designated user needs to review them and start them through the workflow.

Newly discovered patterns are handled by using the Annotations feature to assign them to a stage such as **Follow-up**, or simply **Closed**, and optionally to a particular ESM user.

Specific procedures and decisions, of course, depend on the internal processes of your enterprise and the patterns encountered.

Pattern Analysis

As an analyst dealing with day-to-day pattern discoveries, your basic process can be as follows.

Using the appropriate filters, view the patterns that are new and assigned to you in the Pattern Inspector.

Review these patterns in the Pattern Inspector and compare their transactions historically to those found in other snapshots, using the Snapshot menu.

Use the Show Related Events feature to gain more intelligence about the sources and targets that appear in the patterns.

Remember that events in a grid view are subject to all the ordering, graphing, filtering, reporting, and inspection tools available in the Viewer panel.

Visualize the source and target relationships using Show Event Graph.

Pattern Disposition

Acting on reviewed patterns can include:

- Assigning a new stage or user
The pattern may need further analysis or some other handling, by another user, or can simply be closed. Use the **Annotate Pattern** command to make this disposition.

■ Creating a rule

If a pattern represents activity that needs to be reported, monitored, evaluated, or otherwise acted upon automatically, use the Create Rule command to build a rule based on the pattern's items.



Remember to express an appropriate Time Frame value in the Aggregation tab of the Rules Editor. The scope of a rule's time frame is critical to its effectiveness.

■ Deploying a rule

Once created, if a rule is of value to the enterprise, you should copy or move it to the Rules/Shared/All Rules/Real-time Rules group in the Navigator panel's Rules resource tree.

Pattern Expertise

On a work-a-day basis, the following points will help you make the best use of ArcSight Pattern Discovery.

Workflow

Pattern discovery analysis may also be scheduled. For example, once per hour the prior hour may be analyzed using three different profiles. The patterns discovered by each profile will be stored in a designated group in the Patterns resource tree.

Each pattern also has certain annotation features associated with it that will be familiar to users of trouble-ticket systems. Each pattern can be flagged as being at a given stage (e.g., Queued, Acknowledged, Under Investigation, Under Observation, Normal Activity, etc.). Patterns may also be assigned to an ESM user for further investigation.

Initially, many new patterns will be observed and will need to be characterized. Does the pattern represent a threat or is it a result of normal activity on the network? Should a rule be generated? Or is more observation of the pattern required in order to understand it?

Over time, only a few new patterns will be observed each day. These will be delivered in the Queued stage. In the simplest workflow, the ArcSight operator must resolve these patterns or assign these patterns to others for resolution each day.

When patterns are observed again, ArcSight can be instructed to either quietly mark the pattern as observed again or to bring the pattern to the attention of the operator.

Visualization

ESM v3.0 event graphs have a clustering ability that makes them very useful when illustrating the interactions represented by a pattern resource.

Suppose events F, G, and H occur together in the same transactions 100 times while F and G occur in 5 additional transactions. All these occurrences would be rolled together into the same pattern. The event graph would cluster the 100 sources where F, G, and H occur together. It would also cluster the sources where only F and G occurred.


To use a somewhat more concrete example, one cluster might represent a Nimda Worm's attempts to infect IIS installations. The second cluster might represent successful infections.

Applications

Pattern Discovery can be used to characterize the traffic on newly protected networks (e.g., new customers for MSSPs, new divisions for large corporations, etc.). It can also characterize traffic from new sensors.

Pattern Discovery is also a key element in the ongoing operation of an ESM installation. Using periodic, scheduled analysis, operators can always be kept up to date as new event patterns appear. Frequently, these patterns will indicate new worm or exploit behavior.

Payload

"Payload" refers to the **information carried in the body of an event** network packet, as distinct from the packet's "header" data. (See ["Events" on page 722](#).) While security event detection and analysis usually centers on header data, packet payload () may also be forensically significant.

As described in ["Showing Event Payloads" on page 145](#), you can retrieve, preserve, view, or discard payloads using the ESM [Console](#). Since event payloads are relatively large, ESM does not store them by default. Instead, you can request payloads from devices, for selected events, through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console. (See ["SmartConnectors" on page 762](#).)

Typically, devices discard payloads after a certain period of time. To make it possible to retrieve payloads after normal expiration, they can be stored in the ArcSight [Database](#). Preserved payloads can be kept available as long as needed, then discarded.

Payloads are downloaded and stored only on demand. Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

A payload that has already been downloaded and stored in the ArcSight Database can either be manually selected and deleted, or removed based upon the event-retention policy.

If the payload's format is not recognized by the ArcSight Database, its data will not be lost; instead it appears "unparsed" in the event. The event name attribute generally contains the complete data in this case.

Prioritization Fields

ESM [Events](#) include fields whose values help you evaluate each event's overall priority and importance, and determine which events you should investigate first. The prioritization field values take into account a number of factors including:

- Vulnerability of the Target Asset
- Active List Contents
- Open Ports on the Target Asset
- Asset Criticality

The following table lists the event prioritization fields and describes how values for each field are calculated.

Data Field	Description
Model Confidence	<p>Is the target asset modeled in ESM and, if so, to what degree? This factor depicts the confidence we have in our model. This value depends heavily on whether target assets of interest are modeled in the system.</p> <p>If the only data point for an asset is its ID, then it is likely that this is either an asset range, or an asset that was modeled manually. The fact that the target asset is in the system at all provides some degree of model confidence. Model confidence is higher, though, if the target asset has been scanned for open ports and vulnerabilities.</p>
Asset Criticality	How important is the Asset? This factor encompasses the criticality of the attacked asset.
Relevance	Does it appear probable that the attack succeeded? This factor performs an open port correlation (check to see if the target port is open) and vulnerability correlation (check to see if one of the exploited vulnerabilities is exposed).
Severity	How serious is this attack? This factor encompasses the severity of the event (ArcSight Severity), the severity of the exploited vulnerability (how much it is exposed), any user-supplied filter weighting, and the presence of the Source IP Address in various compromised and hostile active lists.
Priority	Should this event be investigated right away or not? This factor encompasses the criticality of the targeted Asset, user-specified weighting using Filter/weighting pairs, attack severity, and attack success from the other prioritization field values. This value is used to prioritize the investigation of events.

Please also see [“Priority Calculations and Ratings” on page 737](#).

Priority Calculations and Ratings

Priority is defined as a value used to prioritize the investigation of [Events](#). This topic describes the calculations used to determine an event's *priority rating* ([“Priority Rating” on page 740](#)).

The calculation of event priority field values is controlled by formulas and weighting specified in the file `$ARCSIGHT_HOME/config/server/ThreatLevelFormula.xml`, which is located with the ESM [Manager](#).

The priority value assigned to an event is essentially the severity the event was assigned by the original reporting SmartConnector, as modified by the weighting schemes set in `ThreatLevelFormula.xml` for model confidence, relevance, severity, and asset criticality.

Each of the factors in `ThreatLevelFormula.xml` evaluates to a value in the range of 0 to 10, and that value has a specific degree of positive or negative influence (weight) on the original SmartConnector severity value. See [“Prioritization Fields” on page 736](#) for definitions of these factors.

The priority formula consists of 4 factors that combine to generate an overall priority rating. Each of the criteria described in the table below contributes a numeric value to the priority formula, which calculates the overall importance, or urgency, of an individual event.

All values fall in the range between 0 and 10, where 0 is low and 10 is high. A high priority factor generally indicates an event with a higher risk factor. Not every high priority event is necessarily a threat, however. For example, if a critical e-mail server fails, the priority of the events reporting it may be very high, although it does not necessarily represent a threat to your network.

Table 22-18 Calculating Priorities

Threat Level Factor	Factor Weighting
SmartConnector Severity	Connectors report severity values based on the device, the situation, and their configuration. The values range from 0 to 10, and display as Unknown, Low, Medium, High, and Very High. For example, a value of 6 often translates to Medium.
Model Confidence and Relevance	<p>Model Confidence and Relevance (MCR) each have a range of 0 to 10 and are combined to give a net value in the 0 to 10 range. (For example, a Model of 10 and a Relevance of 5 would return a value of 0.5.) This combined factor establishes the degree of support for the original SmartConnector severity value. A combined MCR of 10 would be full support for an Connector severity value, e.g., a 6 would remain a 6. Also note that an MCR value of 0 will always force a priority value of 0.</p> <p>The actual formula for MCR is relevance divided by relevance plus model, minus relevance times model, divided by 10, or:</p> $\text{MCR} = R / (R + M - R \times M / 10)$
Severity	An event's potential attack Severity has a range of 0 to 10, with the highest value (10) adding a weight factor of 30%. In other words, if a SmartConnector originally reported a value of 6, and Model Confidence and Relevance supported it, then a Severity value of 10 would add 30% to the 6, boosting it to 7.8. A Severity value of 0 would add nothing.
Criticality	<p>Asset criticality measures how important the target asset is in the context of your enterprise as set by you in the network modeling process by using the standard asset categories /System Asset Categories/Criticality/Very High, High, Medium, Low, and Very Low.</p> <p>Asset Criticality ranges from 0 to 10. The criticality multiplication factor is:</p> $1 + ((c - \text{criticalityZeroPoint}) / 10) * \text{criticalityBoost} / 100$ <p>Assuming criticality boost = 20 and criticality zero point = 8, the criticality factor weighting will be:</p> <p>C (criticality) value of 10 = $1 + ((10-8)/10) * 0.2 = 1.04$</p> <p>C value of 8 = $1 + ((8-8)/10) * 0.2 = 1$</p> <p>C value of 6 = $1 + ((6-8)/10) * 0.2 = 0.96$</p> <p>C value of 4 = $1 + ((4-8)/10) * 0.2 = 0.92$</p> <p>C value of 2 = $1 + ((2-8)/10) * 0.2 = 0.88$</p> <p>C value of 0 = $1 + ((0-8)/10) * 0.2 = 0.84$</p>

You can modify the formula XML file to customize weighting to reflect your own security priorities and environment.



Changes made to the ThreatLevelFormula.xml file must conform to the format described in [\\$ARCSIGHT_HOME/schema/xml/arc-sight-threatLevelFormula.dtd](#).

The priority calculation formulas are made up of basic elements organized by operators called "Sum" and "Difference." These elements are based on simple condition expressions.

- ["Priority Elements" on page 739](#)
- ["Priority Operators" on page 739](#)

Priority Elements

The basic formula elements each return a positive numeric value or zero. Individual element values can be configured by changing the Value attribute associated with the XML element for each condition.

Some of the elements are predicates that test a specific condition. If the condition for a specific element is satisfied, these elements return a positive value; otherwise, the element returns zero.

Predicate elements can also be negated using the Negated attribute. In that case, they return a specified value if the condition is not satisfied, and zero if the condition is satisfied.

Table 22-19 Priority Calculation Elements

Prioritization Element	Description
HasOpenPort	Takes a non-zero value if the target asset has a particular port open.
HasVulnerability	Takes a non-zero value if the target asset is vulnerable to the attack captured by the alert under consideration.
HasVulnerabilityMapping	Takes a non-zero value if the signature of the context event has not been mapped to a vulnerability.
HasValue	Takes a non-zero value if the specified event attribute has a value.
InActiveList	Takes a non-zero value if the target address belongs to one of the active lists whose URI is provided in the formula.
Constant	Evaluates to a constant non-zero value. It does not rely on event-specific conditions or any other variable; it remains constant, as the name implies.

Priority Operators

There are two aggregation operators used in the priority calculation formula, **Sum** and **Difference**. The **Sum** operator adds the values of all of the elements that it contains. The **Difference** operator subtracts the sum of all of the values of the subsequent elements from the value of the first element it contains.

Both operators have two attributes, **maxValue** and **weight**.

MaxValue Attribute

MaxValue is used to clip the result after the operator aggregation is carried out. After aggregating, the result is also normalized, which is achieved by dividing the result with [MaxValue](#). For example, if we have an element like

```
<SUM maxValue = 100>
```

and it has two child elements, each of which evaluate to 80, the pre-normalization value will still be 100 and not 160. After normalization, the final result for this example will be 1. Similarly, there is an implied lower limit or minimum value of zero on these elements.

Weight Attribute

The Weight attribute is used to scale the result after operator aggregation and normalization are carried out. So, as in the example previously described, if the aggregating element was:

```
<SUM maxValue = 100 weight = 7>
```

the result after normalization is 1, and after scaling, it becomes 7.

Each of the formulas have an implied maxValue of 10 since each of the four fields in the alert take values in the range 0-10 (inclusive).

Priority Rating

The priority of an event is a calculated overall rating based on **agentSeverity** adjusted by Model Confidence, Relevance, Severity, and Criticality using a detailed formula. (See [“Priority Calculations and Ratings” on page 737](#).) All five factors are fields in the ESM event schema, and can thus be used in correlation.

The priority rating is color coded and displayed in [Active Channels](#). You can sort events in the grid view according to priority. Priority is a good basis for deciding what to look at first in your event monitoring workflow, and priority is one of many useful criteria on which to build filters, rules, reports, and data monitors.

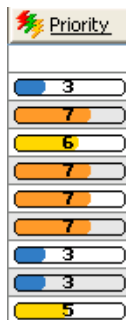







Figure 22-7 Priority Ratings in Active Channels. The Priority column in the default live channel view shows the overall priority rating for each event based on calculations from the other five priority criteria.

The score and color scale used in the priority display are as follows:

Priority	Color	Description
0-2	Green 	Very low. This event is likely a routine function, such as routine file access or a successful authentication by an authorized user. An event that may have started out with a higher priority can become very low priority when it is proved to have failed.
3-4	Blue 	Low. This event is likely a common function, such as a setting change or a scheduled system scan.
4-6	Yellow 	Medium. This event is a potential concern, such as pre-attack scan activity, policy violations, and identified vulnerabilities. Medium priority events are often hostile attempts whose success or failure is not confirmed.
7-8	Orange 	High. This event is a concern, such as attack formations, potential breaches, or misuse, including traffic to a dark address space, incorrect registry values, or a SYNflood.
9-10	Red 	Very high. This event is a grave concern, such as verified breaches or a DHCP packet that does not contain enough data. Items with a very high priority should be investigated immediately.

Queries

A query is an ArcSight resource that defines the parameters of the data you want to report on derived from an ArcSight data source. Queries are used in [Reports](#) either directly or as the basis for [Trends](#) reporting.

Queries can use as a data source the ArcSight Database of events, cases, notifications, modeled network objects (assets), trend data, active list, or session list. Reports then bind data results from queries and/or trends into a display format based on a report template.

See [“Building Reports” on page 205](#) for an overview of all reporting tasks and tools, including how to build queries or trends and how to use a provided or custom [Templates](#).

Queries and Trends

You can use the result of a query as the basis for one or more ESM reports or trends. For a detailed description of how queries and trends can be used together, see [“Query-Trend Relationships in Reporting” on page 242](#).

Building and Running Queries

You can access queries and associated editors in the Reports resource in the ESM Console.

See [“Building a Query” on page 230](#) for information on how to navigate to and use the Query Editor to define query settings (as described in [“Defining Query Settings” on page 230](#)).

Query Viewers

Query Viewers are a type of resource for defining and running SQL queries on other ESM resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results.

Previous to v.4.5, the only way to run SQL queries against ESM events and resources was to run reports, which use SQL queries and trend-queries. Starting with ESM v.4.5, you can use query viewers to run the same queries used for reports, and get results quickly. Then, if desired, you can generate a simple report directly from the query viewer results. Full-featured ESM reporting (with queries, trends, and templates) is still offered for more robust reporting requirements (see [“Building Reports” on page 205](#)), but query viewers provide a shortcut to running those same SQL queries apart from reporting.

Query viewers provide high-level summaries to monitor system health, reveal trends, and allow for drill-down investigation of all types of resources. Query viewers can work with trend tables rather than event tables, and so can return results much faster than [Active Channels](#).

See [“Query Viewers” on page 161](#) for information about using and building query viewers.

Reference Pages

Certain [Resources](#) among those you find in the trees of the [Navigator Panel](#), or events you see in the Viewer Panel ([“Views” on page 800](#)), have pointers to additional reference information. To check for this information, you right-click an individual event, resource, or resource group and choose **Reference Pages**.

If there are pointers available, you see the Reference Pages dialog box. Select one or more items and click **View** to open them in Web Viewer tabs. If no content is available, click **OK** in the “none found” dialog box.

Some reference page pointers are pre-populated by ESM. You can edit these, or add new references, through the **Group Editor** (as described in [“Editing Groups” on page 61](#)). In the Group Editor, use the Group Page text field to specify URLs to reference pages for the group as a whole. Use the **Group Children's Page** field to specify URLs to reference pages for the individual items within the group. Member URLs can be in the form of templates that use the names of ArcSight [Data Fields](#) to query for particular files.

Note also that all the content formerly available through the feature called “Vendor Pages” continues to be available from Reference Pages.

Reports

Reports are an ArcSight resource that provide captured views or analyses of information that can be viewed in the ESM [Console](#) in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). You can also view previously generated and archived reports in an [ArcSight Web](#) client.

ESM allows you to create reports on all events, cases, notifications, and assets stored in the ArcSight Database.

Reports gather data based on [Queries](#) and [Trends](#), and use report [Templates](#) to determine display and file formats.

For an overview of reporting in Arcsight ESM, including information on queries, trends, and templates, see [Chapter 11, Building Reports, on page 205](#).

Working with Report Templates, Queries, and Trends

Reports are based show results of pre-defined queries and trends using custom-designed or provided templates. Once you have source data defined in queries and/or trends, you can design reports to present the data in charts and tables.

The Reports resource includes the following tabs and editors for the following elements that make up reporting:

- Templates ([“Using Report Templates” on page 209](#))
- Queries ([“Defining Query Settings” on page 230](#))
- Reports ([“Defining Report Settings” on page 253](#))
- Archives ([“Archiving Reports” on page 294](#))
- Trends ([“Defining Trend Settings” on page 245](#))

A Report Wizard is provided for creating reports quickly. (See [“End-to-End Reporting Examples” on page 272](#) for an example of using the report wizard.) From within the wizard you can choose a data source (one from among available [Queries](#), [Trends](#), [Active Lists](#), or [Session Lists](#)) and one of the available [Templates](#) to use for the report.

Viewing and Managing Reports

You have the flexibility to broaden or narrow the data extracted from the ArcSight Database using report parameters and conditional logic statements. You can also create delta reports to show the difference between two sets of parameters. With this flexibility, you can create custom reports that are tailored to meet your reporting needs. ArcSight also makes one other distinction. ESM provides display groupings of "Report Definitions", where you define what report you want to generate, and "Report Output", where the actual reports are generated and stored.

Archived Reports

Once a report is created, it can be saved (archived). Archived reports are retrieved for immediate viewing, without requiring you to regenerate the report. In addition, you can schedule a report for automatic archiving, on a yearly, monthly, weekly, daily, or hourly basis. All reports are displayed at the ESM Console in the Report Viewer. You can also run, archive, and delete reports through ArcSight Web clients.

Report Groups

Reports can be created and edited in the <user ID>'s Reports group or the Public Reports group on the Report Definitions tab. Reports can be deleted based on your permissions. Reports created in the <user ID>'s Reports group is available only to that user and those to whom the user gives inspect or edit permission. Reports created in the Public Reports group are available for all users to create, edit, or delete. Reports can then be run from the Reports resource tree and the Viewer panel. For more information, see [“Running Reports” on page 287](#).

You can manage reports in the Reports window of the ESM Console. The Reports resource tree has two tabs: Report Definitions where reports are managed and Report Output where

archived reports are stored for viewing. The Report Definitions tab lists and organizes all reports in one of the following groups.

Report Groups	Description
<code><user_ID></code> 's Reports	Reports the user has created.
Shared Reports	Reports that other users have already shared with the logged-in user.
ArcSight Reports	Reports provided as defaults by ESM, which you can use as-is or to create custom reports.
Public Reports	Reports to which all users have read permission.

If you have Administrator access you will have another group named All Reports that contains all user report groups and their reports.

The Reports Output tab lists all archived reports. Archived reports are listed as a file on the Report Output tab for quick access and retrieval. When you archive a report from the Report Definitions tab, that report is sent to the Report Output tab. If other users archive a report and share it, the report is listed in the Shared group on the Report Output tab.

Delta Reports

A delta report is one that shows the difference between two sets of parameters used in a single report. The report also shows the data for each of the parameters.

When you run or archive a delta report an internal event is sent to the ESM Manager. This event contains the following data fields and values.

Delta Report Field	Description
Event Name	Delta Report Generated (Report: <code><ReportName></code>), where <code><ReportName></code> is the name of the report.

Rules can be created using the delta report data fields.

Report Parameters

For date parameters, type in the text fields, click the drop-down arrows or click the time buttons to select a time range.

For date and time data fields, you can also type an actual date value, such as 10/12/2002 8:54:00 AM, or you can use special system variables such as:

- `$CurrentDateTime`: for the date and time the report is run, the system variable is replaced by the current date and time value when the report is run.
- `$CurrentDate`: for the date the report is run, the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run.

You can also specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: `$CurrentDate - 7d` for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or `$CurrentDateTime - 12h`, which evaluates to the current date time minus 12 hours.

Select a **Report File Format** from the drop-down menu.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and will appear differently. In addition, Excel format is more memory intensive than PDF.

Running Reports

For information on how to run a new or archived report, see [“Running Reports” on page 287](#).

ArcSight Provided Reports

ESM provides over 200 reports listed in the ArcSight Reports group which you can use to immediately generate reports or use as templates to create or customize your own reports.

The ArcSight Reports group contains all reports further subcategorized in one of these report subgroups.

Report Group	Description
By Attribute	Provides various reports providing details based on connector type, severity, device, event name, source, target, and target port.
By Event Direction	Provides reports based on inbound or outbound attack and alert direction.
By Event Volume	Provides reports based on most frequent and least frequently occurring events.
By Sensor	Provides report by type of sensor or connector, for example, firewall, router, intrusion detection, etc.
By System Object	Provides reports by type of object, for example, active lists, assets, cases, and notification.
Custom Reports	Provides varied example reports demonstrating moving averages and vulnerability.
Example Canned Reports	Provides reports showing various types of asset reports and different report layout designs.
Internal Reports	Provides various reports providing information on ESM system usage, performance, rule operation, and resources.

You can run each of the reports to see the type of detail and information each provides. In addition, you can view the notes, settings, and conditions set on each tab to see how each report is constructed. To use a report as a template for creating or customizing your own reports, copy an existing report to a new report group (using drag and drop to copy an existing report to the new report group). You can then rename the new report and start making changes to the new report.

Report Templates

Report templates are a component of ESM Reporting resource tools.

To provide more flexibility in reporting, ESM now offers powerful report template tools including a rich offering of ready-made templates and a template design wizard for more customized [Reports](#). Template definitions determine how data from [Queries](#) and [Trends](#) is

displayed in a report. You can create and adjust templates to specify which data is displayed, what visual elements are used (variations on tables, charts, graphs, and so on), the layout of those elements, the report output file format, and much more. A template consists of report design elements, such as headers, footers, title bars, charts, and tables, arranged on a page according to a layout specification.

Templates can accommodate input from multiple queries and show multiple visual elements, such as three charts and a table each pulling from a different data source, in a single report.

For more information on templates, see [“Using Report Templates” on page 209](#).

See [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools.

Resources

ESM manages the logic used to process events as objects called **resources**. Active channels, data monitors, filters, cases, assets, queries, trends reports, rules, and packages are all examples of resources.

A resource defines the properties, values, and relationships used to configure the functions ESM performs. Resources can also be the output of such a configuration (such as archived reports, or Pattern Discovery snapshots and patterns).

ESM has over 30 different types of resources and comes with hundreds of these resources already configured to give you functionality as soon as the product is installed. These resources are presented in the Navigator panel of the ESM Console and ArcSight Web interfaces.

This topic provides an overview on working with resources in the ESM Console. Resources in general are discussed in more detail in the topic “ESM Resources” in *ArcSight ESM 101*.

Valid and Invalid Resources

Valid resources show up in the Navigator with their associated icons as described in the [“Navigating” on page 58](#). A resource can “break” or become “invalid” either because it is constructed improperly (for example, when an active list schema does not match the underlying table) or because another resource it depends on is missing from the database (for example, when a rule references an unavailable filter). The latter can happen when a resource used in other resources is deleted from the Manager, or not retained during an upgrade, import, or export.

Invalid resources show up in the Navigator as broken or torn.

For example, the Navigator displays a valid filter like this: , and an invalid filter like this:



A valid resource is fully available to other resources that reference it, and can participate in the [Events](#) flow, [Trends](#), [Reports](#), [Data Monitors](#), [Active Channels](#), [Filters](#), [Rules](#), and so forth.



An invalid resource cannot participate in the event flow or other resources in real time. For example, invalid [Assets](#) cannot participate in event asset resolution. Correlated events in

which the source or target address points to the invalid asset are not generated. Similarly, an invalid rule does not trigger and generate correlation events.

Fixing and Validating Resources

When a resource becomes invalid, its Editor includes a **Validate** button that you can use to test and validate the resource after you fix it. Clicking the **Validate** button on a resource that was previously broken results in a check of the resource logic and dependencies. If the system determines the resource is now valid, the resource icon in the Navigator is updated to reflect a working resource. If the system determines the resource is still broken, it displays an error message describing the problem.

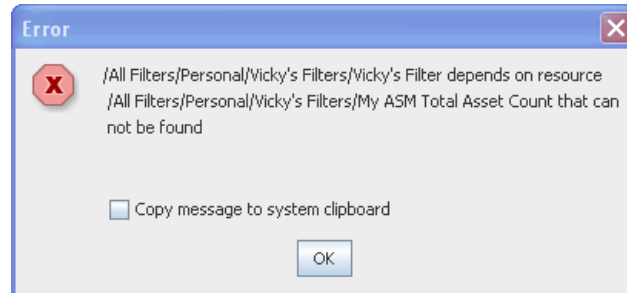
The general flow of steps to fix and validate a resource are:

- 1 Identify an invalid resource. Sometimes problems with filters (see [Filters](#)) or [Rules](#) (which are used in many other resources) are a result of broken resources. (A valid resource looks like this: , and an invalid resource looks like this: )

For example, if "My Top Threats" filter depends on "My Hotlist" filter, removing "My Hotlist" filter breaks "MY Top Threats" filter.

A scheduled job (like a scheduled rule group or archived report) can also break if one of the resources it depends on is missing. The broken icon for a scheduled job shows up on the Current Jobs list. (See ["Scheduling Jobs" on page 756](#).)

- 2 If you do not already know why a resource is broken, open its editor (double-click the resource in the Navigator panel) and click the **Validate** button in the resource editor. This will give you an error message that describes the problem. The error dialog includes a Copy button for copying longer messages to an external editor.



- 3 Fix the problems with the resource. This may involve adding back in missing resources or rebuilding the resource to fit various other requirements as described in ["Troubleshooting \(Requirements for Valid Resources\)" on page 749](#) below.

To continue with our example, adding back in the filter "My Hotlist" would fix the problem we mentioned in [Step 1](#).

- 4 In the resource editor(s), click **Apply** to save changes to the resources you modified.



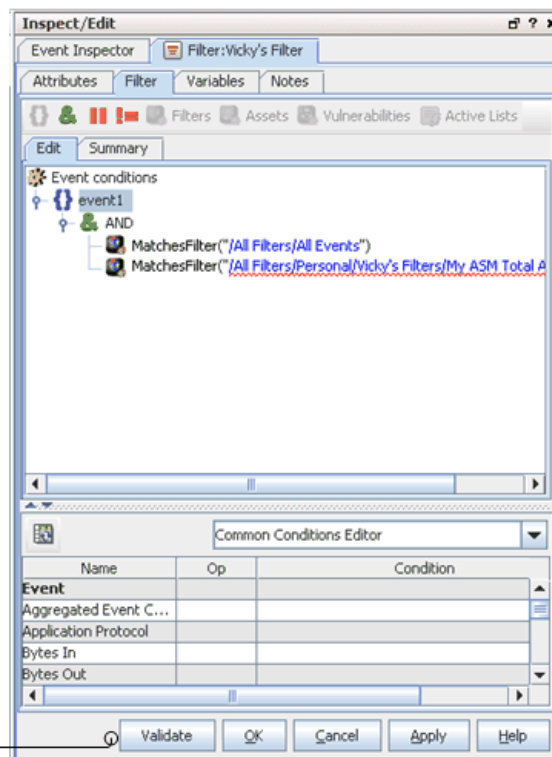
For problems that can be validated on the local client, you can click **Validate** before clicking **Apply** and if the resource is fixed its "working" icon is immediately reflected in the Navigator. However, for other types of problems; you need to **Apply** the changes to the resource before you **Validate** the resource. This is because some types changes must be processed on the Manager to determine dependencies and relationships to other data not available on the local client.

If you think you have fixed a resource but it is still not showing as fixed in the Navigator, make sure you Apply all the changes you made to it and then click Validate again.

- 5 In the resource editor for the resource that was broken, click **Validate**. If the resource passes validation, its icon in the Navigator updates to reflect a working resource.

In the resource Editor for the resource that was broken, click Validate button. If the resource passes validation, its icon in the Navigator updates to reflect a working resource. Otherwise, the broken icon remains and an error message describes the problems.

Some problems require saving fixes to the Manager, so be sure to click **Apply** and save changes to resources you fix before you click **Validate**.



To validate a scheduled job, click the **Open scheduled jobs list** tool button (🕒) to display scheduled jobs in the Viewer, right-click the job you want to validate, and choose **Validate** from the context menu. If the job passes validation, its icon in the Current Jobs list updates to reflect a valid task.

Troubleshooting (Requirements for Valid Resources)

The most common cause of an invalid resource is a dependency issue; another resource that the broken resource depends on is missing from the database. Some resources have additional requirements or limits that can also affect validity. Following is a summary of requirements for creating valid resources.

If any of these requirements are not met, the resource will break. To fix the resource, edit its definition to be in line with these requirements.

- **All Resources** - If the definition for a resource references another resource, the referenced resource must be available in the Manager database. This requirement is true for all types of resources.
- **Devices and Assets** - Each asset address must be unique within a zone, an asset can belong to one zone only, and the asset IP address must fall within the address range of its network zone.
- **Device and Asset Ranges** - Start addresses must be less than end addresses, asset ranges must be within the address range of the associated network zone, and asset ranges should not overlap another asset range in the same zone.
- **Zones** - Start addresses must be less than end addresses and network zones should not overlap other zones in the same network.
- **Reports** - Report templates cannot contain more than 20 charts or more than 15 tables.
- **Active Lists** - Active List schema must match the underlying table and must not include programming errors.

For more information, see the *ArcSight ESM Administrator's Guide* topic on "Resource Validation".

Automatic and Manual Validation

You can validate individual resource manually through the Console with the **Validate** button as described above.

Resource validation takes place automatically during an upgrade, [Packages](#) import or export, or when you insert or update a resource. (Administrators can use a stand-alone, command-line utility on the Manager machine for validating resources and generating validation reports on an off-line Manager. This is often useful after an upgrade.)

For more information, see the *ArcSight ESM Administrator's Guide* topic on "Resource Validation".

Resource Attributes

The [Resources](#) that ESM processes are composed of several attributes, each of which is a data field with its own characteristics. The data fields common to all resources are described below.

Each attribute has both a **Label** that you see in the Console and a unique **Script Alias** you use to refer to the attribute in filters, rules, or Velocity templates. The **Data Type** lets you know how to handle the attribute. (Also, see ["Resources"](#) on page 746 for information

locked and unlocked resources, and [“Common Resource Attribute Fields” on page 552](#) for information on viewing and/or editing these fields in resource editors.)

Group	Label	Script Alias	Data Type	Description
<i>Resource Type</i>	Name	name	String	The name of the resource.
Common	Resource ID			Read-only field that shows the ArcSight ESM system resource ID.
	External ID	externalId	String	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. Your ESM administrator can advise you on the correct values for this field, if applicable. For Vulnerability resources, this field will be filled in with an ID of the format <standards body> <id>, such as CVE CVE-1999-200.
	Alias	alias	String	An identification string suitable for referencing resources within ESM. A given alias will appear in place of the resource's name everywhere it may be seen. Your ESM administrator can advise you on the correct values for this field, if applicable.
	Description	description	String	An editable text description of the resource or other related information. This text appears as a tooltip to any ESM user who has Console access to the resource.
	Version ID			A string showing a globally unique version ID for the resource.
	Deprecated			Indicates whether a resource is current or obsolete. If this field is blank, the resource is current. If this field is check marked, the resource is "deprecated" or obsolete. Click the box to toggle the checkmark on or off.
Assign	Owner	owner	String	One or more ESM users who are interested in this resource.
	Notification Groups	notificationGroups	String	The ArcSight user groups selected from the Users resource tree who should be notified about this resource.

Group	Label	Script Alias	Data Type	Description
Parent Group	groupName Link		Resource Group	Each resource group containing this resource. A resource exists in more than one group when you choose Link instead of Copy or Move.
Creation Information	Created By	userName	User	The identity of the ArcSight user who created this resource.
	Creation Time	creationTime	DateTime	The time that the resource was created.
	Time Since Creation	timeSinceCreation	String	The elapsed time, in days, hours, minutes, and seconds since this resource was created.
Last Update Information	Last Updated By	lastUpdatedBy	User	The identity of the ArcSight user who last updated this resource.
	Last Update Time	lastUpdateTime	DateTime	The time that the resource was last updated.
	Time Since Last Update	timeSinceLastUpdate	String	The elapsed time, in days, hours, minutes, and seconds since this resource was last updated.

Rule Actions

Rule actions are automatic procedures that occur when all rule [Conditions](#) and threshold settings have been met. (See also [“Rules” on page 753](#).) You can choose to be notified of a triggered rule at the ESM [Console](#) or through the Notifier (see [“Notifications” on page 729](#)), have information about the [Events](#) that triggered the rule sent to a case or active list (see [“Cases” on page 605](#) or [“Active Lists” on page 574](#)), or automatically execute a command line function. You can also assign more than one rule action to any rule.

The task steps for these activities are available in [“Creating Rule Actions” on page 310](#).

Active List Rule Actions

The Active List rule action automatically organizes rule associated IP addresses in active lists. Once a rule is triggered, the Active List rule action adds IP addresses from events that have triggered the rule to an active list. The Active List rule action can also move or remove IP addresses from active lists. Rules can also be created on active lists.

When the rule is triggered, the rule action takes all associated addresses (source or target) and adds those addresses to an active list. For example, if a rule is triggered with an action that has Source Address and Suspicious List selected, all source addresses are sent to the Suspicious List in the Active Lists resource tree.

Execute Connector Command Rule Actions

Beginning in ArcSight v3.0, rule actions can automate the process of sending commands to SmartConnectors and through them to the devices they support. While all SmartConnectors can respond to the basic commands (e.g., start, stop, pause, continue,

and terminate) some that represent more complex devices can respond to more complex commands. For example, rule actions can tell the Check Point Firewall SmartConnector to tell its device to block a particular IP address. See [“Creating Rule Actions” on page 310](#) for a description of the actual steps involved.

It may be helpful to note that this feature is in effect an automated solution for using the capabilities described in [“Sending Control Commands to SmartConnectors” on page 517](#).

The specific SmartConnectors that support this capability, and the additional commands they can process, are subject to change. Consult your ESM administrator or representative for more information.

Rule Conditions

A rule is a programmed procedure that can analyze network [Events](#) and generate additional correlation events, as determined by security policy. (See also [“Rules” on page 753](#).) When creating rules, you define the rule events and [Conditions](#), thresholds, and [Rule Actions](#). Conditions define which events trigger the rule, thresholds set when a correlation event is generated, and actions state which responses are taken when a correlation event is generated. To define rule events and conditions, thresholds, and actions, begin by determining the following:

- Which event occurrences do I want to be aware of? This determines the rule's **events** and **conditions**.
- How many times do I want the event or events to occur and within what time frame? This determines the rule's **threshold**.
- What actions should automatically occur when an event is generated? When should those actions occur? This determines the rule's **actions**.

A rule requires at least one event and one condition. When you create or edit a rule, the ESM Console provides a Conditions tab in which you can specify events and define the conditions for a rule. (The Conditions tab is described in the topic on the [“Common Conditions Editor” on page 616](#).)

Rules are first constructed by creating condition statements. Condition statements contain a data field, logic operator, and data field value; so you can create complex logical expressions by combining one or more individual conditions to match the events you want to trigger a rule.

When you first create a new rule, a default event named [event1](#) appears as a branch under the Correlate tree for the new rule. (The event name is also commonly referred to as the event “alias”.) You can use this name or select a different event to use in the condition. Since rules can have numerous events, event names should be unique and descriptive within the same rule. For example, if monitoring Cisco Router denied events, [Cisco Router denied](#) could be the event name. The event name appears as a branch under the Correlate tree.

When defining the condition for an event, the Conditions tab provides three columns, Name, Operator, and Condition. These three columns are combined to create `<data field> <logic operator> <data field value>` condition statements. For example, if monitoring a Cisco Router, the condition statement could be [Device Product = Cisco Router: Device Product](#) as the data field, `=` as the logic operator, and [Cisco Router](#) as the data field value.

When adding conditions, you need to decide how to tie the new condition to any existing conditions. To add more condition statements to an event, you can use logical operators

AND, OR, or NOT to specify how to evaluate the condition statement that contains more than one individual condition.

Besides specifying events in a condition, you can also add filters, assets, and vulnerabilities to rules as new conditions. A filter condition monitors if an event occurs in a particular filter. If an event does occur in that filter, a correlation event is generated (see [“Specifying Rule Conditions” on page 304](#)). Asset conditions state whether your enterprise assets are targets or sources of events. An asset condition states if an event occurs and the selected asset is the source or target, generate a correlation event. Finally, you can also use an existing enterprise vulnerability to create a rule condition. A vulnerability condition states if an event occurs with the vulnerability selected, generate a correlation event. For more information on vulnerabilities, see [“Modeling Your Network and Managing Assets” on page 456](#).

In some cases, however, you may want to specify more complex rule processing to restrict the events that actually cause a rule to fire. ESM provides two additional elements you can include to specify more complex rule conditions: rule thresholds and aggregation. (See [“Specifying Rule Thresholds and Aggregation” on page 308](#).)

Rules

An ArcSight rule is a programmed procedure that attempts to correlate incoming network [Events](#) and generates new events that report on correlation when it occurs, as determined by security policy. Rules also apply [Conditions](#) and perform [Rule Actions](#).

ESM's "canned" rules can be viewed, edited, and used as templates to create your own enterprise-specific or custom rules. To see what's available, browse the description provided with each rule in the [Console](#).

Different users can simultaneously create rules from their ESM Consoles. Once created, all rules are sent to the ESM [Manager](#), which updates any other individual ESM Consoles. Updates to [Resources](#), including rules, are automatically refreshed every few seconds so that clients get the latest changes from other clients.

Information on creating, deploying, and managing rules is provided in Rule Authoring.

Rules Processing and Correlation

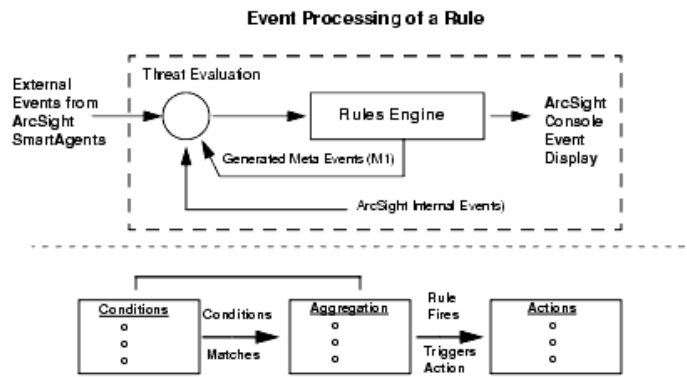
A rule has three parts, a condition, threshold and time window aggregation, and an action. The condition states [if exists](#) and [satisfies](#) expressions and the action states [do](#) expressions. A rule states [if \[one or more conditions\] exist and satisfy the rule, then do \[action expressions\]](#). A rule can have one or more rule conditions. If there is one condition, the rule acts as a filtering tool. If there is more than one condition, the rule acts as a correlation tool. A rule can be created for any incoming event from one or more event generators, with various conditions, logic statements, and threshold and time window qualification of events.

Components of a Rule



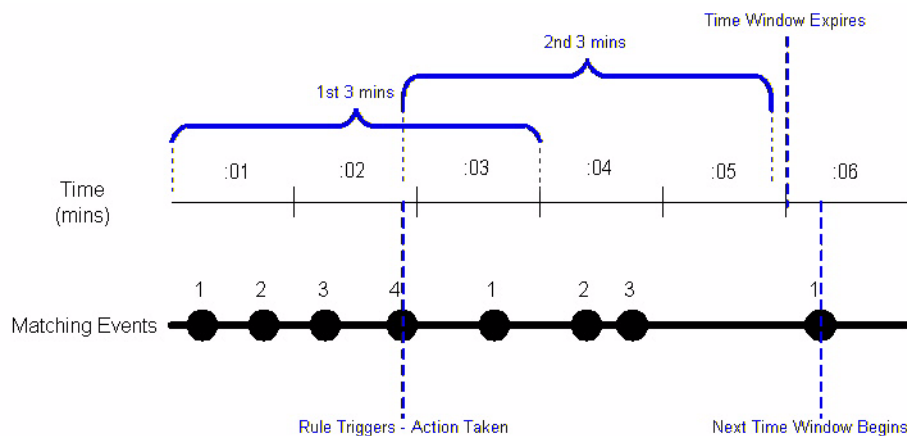
The Correlation Engine, a sub-component of the ESM Manager that handles rules, is not the same as a database query engine. For example, the Correlation Engine can perform a complex join across several events in real-time and aggregate the response to these events. In order for the Correlation Engine to do this in an efficient manner it keeps a list of

events that match each condition. These are referred to as **partial matches** because they satisfy part, but not all, of the rule's conditions. As new partial matches occur, the Correlation Engine attempts to pair them with previous partial matches in order to construct a full match. At that point the Correlation Engine may aggregate that match with others while it waits to pass some threshold (which can be either time or a target number of full matches). If the threshold is passed the Correlation Engine generates a derived event and performs the other actions associated with the rule.



It is important to note that all rules containing a specified threshold and a time window expiration follow a certain process in order to generate a derived event and perform an action. If a rule's threshold is passed, but the time window expiration has not been met, then the Correlation Engine compensates for this by generating a derived event, performing an action, and moving (or sliding) the time window until it expires. If this rule process was not in place, under certain conditions, rules would trigger on nearly every event in a short amount of time and which would cause a large amount of useless events to be displayed or actions occurred.

For example, assume that you created a rule with an event threshold of 4 and a time expiration window of 3 minutes that sends a notification every time the threshold is met. This rule's process would look like the following:



In this example, the 4th incoming event occurred before the time window expired, so the rule triggered at the 4th event and the time window shifted adding another 3 minutes. Within the 2nd 3 minutes the rule restarted its incoming event count, however a 4th event did not occur so the rule did not fire. Note that the time window did not expire until the 5th minute had passed. If a 4th event had occurred before that time then the shifting process would have begun again. If you were to show the rule chain for this example, it would display the information for incoming events 1-4 that occurred within the first 3 minutes.

Time windows expiration triggers fire at the minute boundary unless the next time window starts before the minute boundary.

The Rules resource tree in the Navigator panel offers a default collection of rules that you can use directly or as a template for creating your own custom rules.

For example, there are rules predefined to detect and perform actions based on ArcSight system rules processing and SmartConnector status. Other rule groups detect and respond to attacks and suspicious activity, specific types of attacks on various sensor types, network components, or assets, and report attack results or successes.

Rule Groups

Rules are organized into groups to store similar rules in one location. The Rules tree in the Navigator panel organizes rules into the following groups.

Rule Groups	Description
<userID>'s Rules	The user's home directory, where they have read/write permissions to author rules.
Shared Rules	Rules that establish the permissions for the current user.
Real-time Rules	Rules that are run against real-time events.
Public Rules	The rules that any user can read.
System Rules	The global rules provided by ArcSight.
Unassigned	Rules that do not belong to any directory. These can be rules that have not been inserted into any directory, or their parent directory has been deleted.

If you have Administrator access you will have another group named All Rules that contains all user rule groups and their rules.

Scheduled Rules

You can deploy scheduled rules to run at a specified time interval (such as hourly, daily, or monthly). This is a useful alternative to real-time rules in situations where you want to deploy rules that take into account historical data along with live data, or when you simply want to control when the rules are run. The scheduled rules engine can process historical data, take real actions, and generate correlated events which are the same as those generated by the real-time rules engine.

Only rule groups can be scheduled. To schedule one or more rules, you add the rule(s) to a rule group, and then edit the rule group to add a scheduled job. For more information, see [“Scheduling Rules” on page 319](#).

Rule-triggering Timing

Rule-processing sessions are associated with “Group By” tuples (e.g., a particular pairing of source and target address).

A match occurs when all the conditions of the rule are met.

The first match associated with a new tuple creates a new session. It also triggers `onFirstEvent` and an `OnEveryEvent`. The system then sets the start time for the first time window.

Subsequent matches will trigger `onSubsequentEvents` and `onEveryEvent`.

If enough matches occur to pass the threshold count **before** the time window expires (which is defined as `start time + time window > current time`), then ESM triggers `onEveryThreshold` and one of either `onFirstThreshold` or `onSubsequentThreshold` and it resets the start time for the next time window.

If a time window ends without meeting the threshold, then "final aggregation" occurs. The `onTimeWindowExpiration` option is triggered and the session is disassociated from the tuple.

The next match with the same tuple (or, in fact, any tuple, same or new) will cause the whole process to repeat.

Rule Chains

When rules are designed to trigger in a series, in order to capture or act upon correlated events within a specified interval or at a particular threshold, they are referred to as rule chains.

ArcSight Variables

You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as `$Now` and `$CurrentDateTime`. The same is true for time elements, including `s` (second), `m` (minute), `d` (date), `M` (month), `w` (week), and `y` (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign; e.g., "Source Address" would be `$sourceAddress`.

Rules Editor

The Rules Editor is a panel in the Console for creating and editing rules.

The rules you create or edit are stored in `.ARL` (ArcSight Rules Language) files.

For more information, see [Chapter 13, Rules Authoring, on page 301](#).

Scheduling Jobs

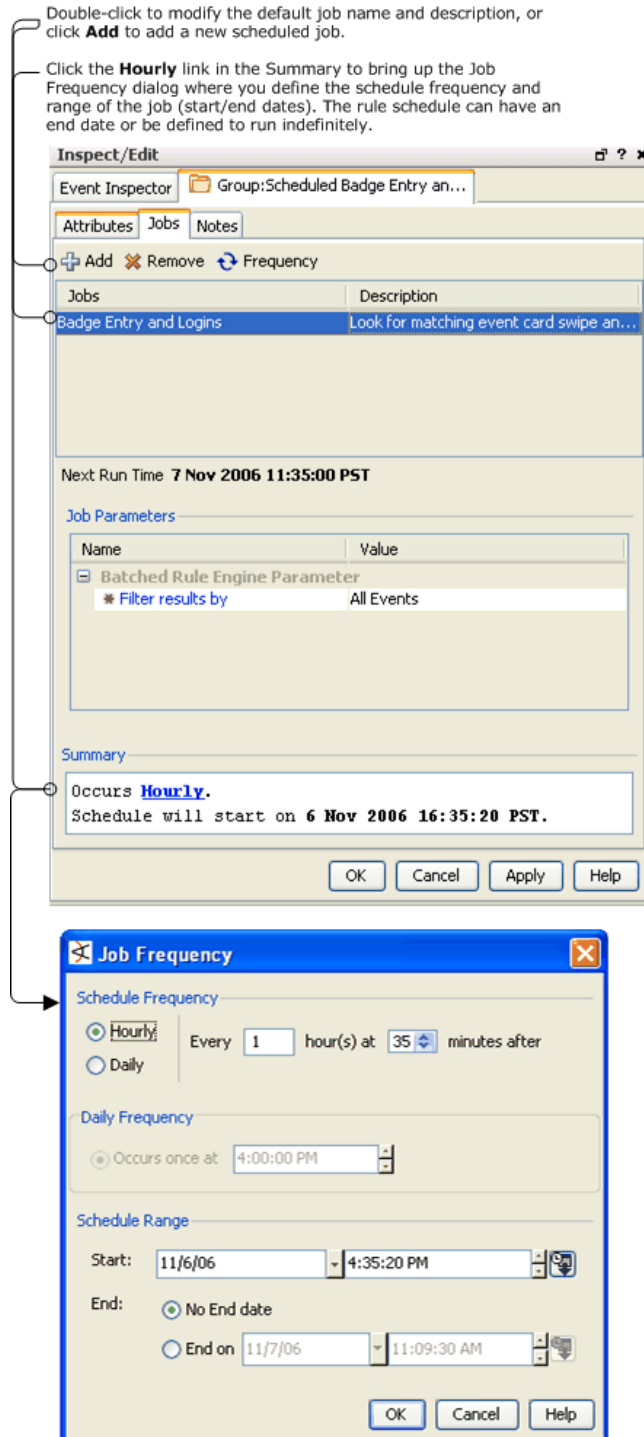
You can schedule some tasks to occur automatically. Specifically, this feature is available for the archiving and scheduling reports, pattern discovery snapshots, and rules. See these topics for information specific to scheduling jobs for particular resources:

- ["Scheduling Report Tasks" on page 297](#) for information on how to schedule reports individually or by group
- ["Scheduling Rules" on page 319](#)
- ["Scheduling a Snapshot" on page 133](#) in ["Pattern Discovery" on page 127](#)


This topic provides general information on how to schedule a job for any resource and view all scheduled jobs.

To schedule a job

- 1 Click the **Jobs** tab in the Editor for a group
- 2 Click **Add** on the Jobs tab. This brings up the Job Frequency dialog.
- 3 Define the schedule frequency and range of the job (start and end dates, or indefinite).
- 4 Click **OK** to save the task and close the dialog.



To view all scheduled jobs

Click the **Open scheduled jobs list** tool button (). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

Click a job in the list. The status of previous and pending runs for that job are shown in the "Scheduled Runs for <Task>" list on the bottom part of the Viewer panel.

Troubleshooting Tips

If the Manager system clock time is changed after jobs are scheduled (e.g., set back a week, a month or a year), some scheduled jobs might not run as expected. They might be kept in pending status in the queue temporarily, and/or synch back up on subsequent scheduled run times. Best practice is not to make dramatic adjustments to the system clock time on a Manager system on which critical jobs are already scheduled. If this problem occurs and does not correct itself soon enough, stop the Manager again and re-set the system clock to the original date/time. Or, if you need to keep the new time setting, be prepared to re-schedule the jobs.

Send Logs

ArcSight Enterprise Security Management (ESM) components output various types of information to log files. For example, the ArcSight ESM Manager logs are located in: [ARCSIGHT_HOME/logs/default/server.log](#). Various ESM Manager utilities write logging information into different sets of log files. (The archive utility writes to the [archive.log](#), the database init utility writes to the [dbwizard.log](#), and so forth). Each of those sets can consist of multiple files. The number and size of the log files are configurable on the Manager under [ARCSIGHT_HOME/config/server.properties](#). ESM Console and ArcSight Web also generate and store log files.

ArcSight Customer Support may request log files and other diagnostic information to troubleshoot problems. The **sendlogs** utility facilitates the process of sending your log files and diagnostics to ArcSight for troubleshooting.

The sendlogs utility automatically locates log files, compresses them, and (optionally) uploads them to the ArcSight Customer Support server.

Guidelines for Using the Send Logs Utility

- Although Send Logs is accessible to any user logged into an ArcSight component, only administrators have permissions to collect logs on remote systems. A non-administrative user can only collect local logs from the component on which he or she is logged in.
- SmartConnectors must be running version 4037 or newer to support remote collection of logs with Send Logs (using a Console or the Manager)
- You can only collect local logs on SmartConnectors or ArcSight Database. That is, if you run the Send Logs utility on ArcSight Database, only the database log files are gathered.
- You can run the sendlogs utility on a component even when the component service is down. If ArcSight Database is down, you can still collect its logs using this utility. If the Manager is down, you can only collect its local logs. However, if you need to collect the database logs as well, use the `arcdt` command on the Manager.

- All log files for a component are gathered and compressed. That is, you cannot select a subset of log files that the utility should process.
- The compressed file is uploaded to the ArcSight Customer Support server using SSL. Therefore, you must have either Port 443 open on your firewall or a proxy server that the ArcSight component can use to make SSL connections.
- Automatic upload of the compressed file is optional. If you do not choose to upload automatically, the `sendlogs` utility generates a compressed file on your local system that you can send to ArcSight Customer Support by e-mail. The compressed log file is created in `ARCSIGHT_HOME/tmp/logs<Filename>.zip`.
- You can review the compressed file before it is uploaded to ensure that only a desired and appropriate amount of information is sent to ArcSight support.
- You can remove or sanitize information such as IP addresses, host names, and e-mail addresses from the log files before compressing them. The options are to (a) send logs as generated, (b) remove only IP address, or (c) remove IP address, host names, and email addresses.

For full details on using the `sendlogs` utility both from the command line and through the Console, see the *ArcSight ESM Administrator's Guide*.

Options for Running Diagnostics and Sending Logs

There are two ways to launch the `sendlogs` utility:

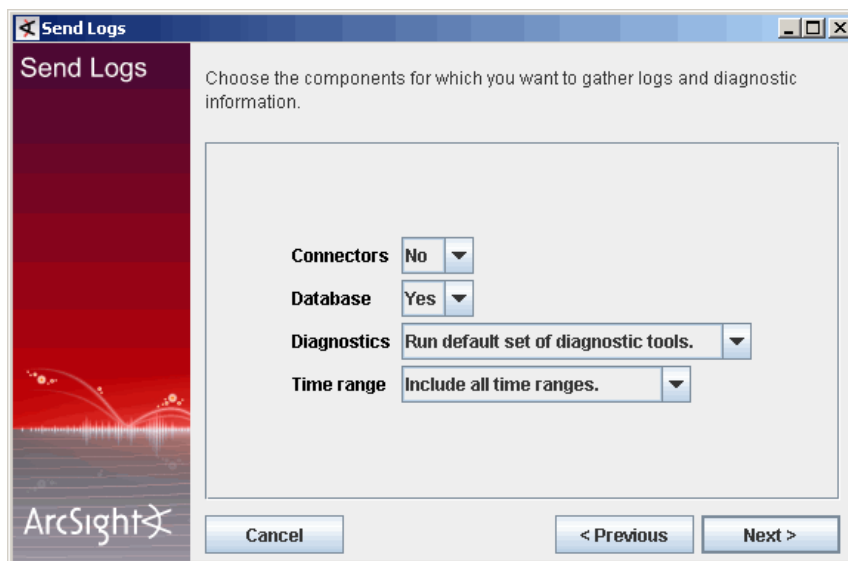
- As a wizard from the Console Tools menu. (See “Using the Network Tools” on page 72.)
- From the command-line interface of each component (via the command `arcsight sendlogs` from `ARCSIGHT_HOME/bin` on the ESM Console, Manager, or ArcSight Web)

You can also use the `arcdt` command to run specific diagnostic utilities from the Manager command line.

Starting the Send Logs Wizard on the Console

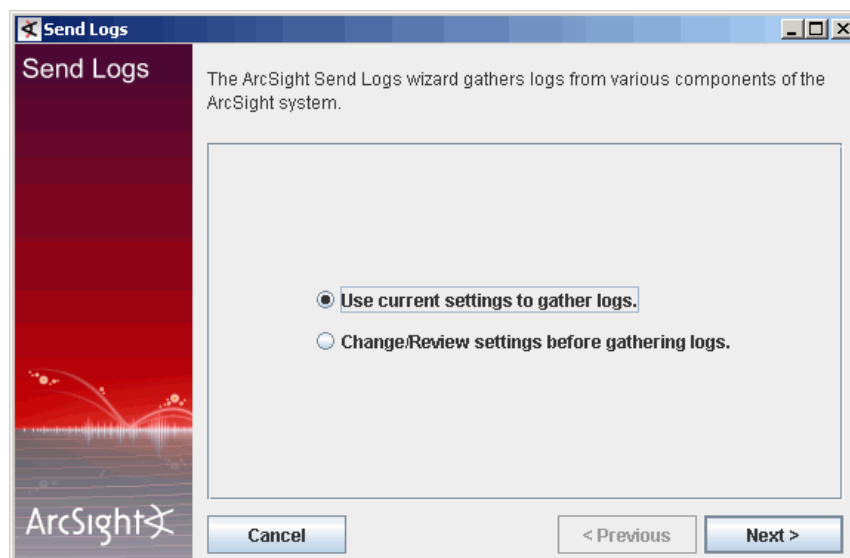
You can launch the Send Logs Wizard from the ESM Console.

Choose **Tools > SendLogs** from the ESM Console menus.



The first time the utility is run from the Console, you are prompted to select the components from which to gather logs and diagnostics. Some additional first-time settings are also required (such as notification details, time ranges, and options to gather diagnostics for session wait times, thread dumps, and database alert logs). The wizard remembers most of these, so that on subsequent runs you can choose to use to retain the original configuration.

From now on when you start the Send Logs wizard, you will get this dialog. If you want to retain your original settings, select **"Use current settings to gather logs."** If you want to re-set the configuration, select the **"Change/Review settings before gathering logs."** option.



From either of these initial dialogs, the wizard guides you through the process of collecting logs and diagnostic information and, optionally, sending them to ArcSight.

For a full description of all options and settings on the Send Logs wizard and sendlogs utility, see "Configuring ESM Manager Logging" in the *ArcSight ESM Administrator's Guide*, especially the following topics:

- Sending logs and diagnostic information to ArcSight
- Guidelines for using the sendlogs utility
- Gathering logs and diagnostic information



A complete set of documentation for ArcSight ESM is available from the Console Help menu. Select **Help > Browse ArcSight Documentation** from the Console menus. This launches the ESM Console Documentation Web page, which provides links to all books. (For example, click the ArcSight Administrator's Guide on to view that book.)

Session Correlation

ArcSight considers a session to be information about the actors behind your network traffic that applies for a limited and specific period of time. Session information can be used to answer questions such as: "Who is in the New York office?" or "How many people are in meetings?" or "Are users accessing this resource according to company policy?"

ESM session correlation is a set of tools that capture session information to not only identify the assets involved in network traffic, but also the users, or actors, behind the traffic. (See [“Understanding Session Correlation” on page 357.](#))

Session correlation makes it possible to map users to assets at specific time periods. This is especially valuable for identifying who is doing what on your network from which assets and when, especially when the asset IDs themselves may be variable (such as DHCP or VPN logins).

Why Session Correlation Matters

Monitoring traffic on your network generally means processing data about the assets involved in the network traffic. However, there are times when asset data alone is not sufficient to detect potential threats to your network.

For example, users who log into the network on VPN or DHCP connections are assigned different IP addresses every time they log in. When sensors report events to ArcSight SmartConnectors, they are only identified by their assigned IP address, which means that you may be missing a whole spectrum of activity from mobile assets, such as laptops and PDAs and remote offices.

Whether accessing your network by using assets with fixed or variable IDs, it is often the user (the “actor”) involved in the network activity whose actions you want to correlate with other event data. This enables you to track who is doing what on your network and when, and what they are doing in subsequent log-in sessions.

Capturing data about who is involved in network traffic as well as what assets are involved also adds crucial verification data to your correlation process. For example, three failed login attempts from a particular IP address can trigger a rule. But if that IP address is assigned to three different assets in the timeframe evaluated, session correlation makes it possible to clarify that the three failed login attempts were not executed by the same user.

Session Lists

Session Lists are similar to [Active Lists](#), with the following major differences:

- Session Lists always have Start Time, End Time, and Creation Time fields.
- Session Lists partition data because the lists can grow very large over a period of time.
- Session Lists do not have to fit entirely in memory.
- Session Lists are optimized for efficient time-based queries.

Session Lists can monitor activity based on any [Rules](#)-driven combination of [Events](#) attributes or set of custom fields. For example, session lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised.

While you can populate session lists “manually” (adding entries from grid views or the Session List Editor), you should use session lists in conjunction with rules specifically tailored to work with them. Rules can dynamically add and remove entries on lists, thereby making them a flexible information-gathering tool.

You can open and edit session lists in [Grid Views](#).

Session lists function differently than [Active Channels](#). Session lists are not continuously re-evaluated and are not time-window constrained. Session lists draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them.

You can use session lists as [Filters](#) in other [Resources](#) that are not based on active channels, such as [Reports](#).

In addition to their integral definitions, you can apply temporary (not saved) filters to session list grid views. Click the status description in the **Filter** line in the view header to use the [Common Conditions Editor](#).

ESM includes a set of default items in the Session Lists resource tree that you can use for templates or for operational monitoring with minor modifications. For example, use the ArcSight User Sessions list to watch activity related to ESM logins.

If you have Administrator access you will have another group named All Session Lists that contains all session list groups and lists.

See also: [“Session Correlation” on page 760](#).

SmartConnectors

ArcSight SmartConnectors are collectors of security event information generated by multi-vendor security [Devices](#) throughout your enterprise. SmartConnectors normalize and correlate this data into [Events](#), expressed as ArcSight Messages, which are forwarded to the Connector Data Manager (a component of the ESM [Manager](#)) for further processing. SmartConnectors can reside on a device, on the ESM Manager, or on a host machine. (For more information on SmartConnectors, see also [“Managing SmartConnectors” on page 498](#).)



Do not delete a Connector resource at the ESM [Console](#) unless the corresponding SmartConnector is first uninstalled from the device it is running on. If the SmartConnector running on the device has not been uninstalled, and its Connector resource is deleted, the SmartConnector will lose its connection to the ESM Manager, causing the SmartConnector to start caching events and eventually dropping them.

Note that ArcSight “agents” are referred to as “SmartConnectors” starting with ArcSight ESM v.4.0.

Operational Status

ArcSight SmartConnectors display their operating status conditions next to their names in the Connectors resource tree in the Navigator panel.

Status Condition	Description
running	The SmartConnector is operating normally.
down	The SmartConnector is not connected to the ESM Console, therefore no events are being received.
stopped	The SmartConnector is responding to commands sent from the Console, but events aren't being received.
paused	The SmartConnector is responding to commands sent from the Console, but events aren't being transferred and are remaining in the SmartConnector's cache.

Configuration

You can configure ArcSight SmartConnectors to set a specific priority level for events that match specific criteria. One of the typical applications of this is to change the default priority mapping. By default, SmartConnectors will map the device priority (which may contain multiple levels) to the standard ArcSight priority levels: **Very-High**, **High**, **Medium**, and **Low**. For example, if a device has eight priority levels (0-7) where 0 is the highest priority, then most likely 0 and 1 will be mapped to Very-High, 2 and 3 to High, 4 and 5 to Medium, and 6 and 7 to Low. You can use this feature to change this behavior and make the SmartConnector set the priority based on different parameters. For example, assume two firewalls, one of which is your production firewall and the other an internal firewall used for testing. You can configure the SmartConnectors to set the ArcSight priority to Low for all the events coming from the internal firewall and leave the rest of the events with the default priority mapping.

SmartConnectors can be configured to optimize their performance and increase their functionality. SmartConnectors can be configured to enable aggregation, batching, and time zone correction functionality. You can also send control commands from the Console to SmartConnectors to manage the flow of events.



SmartConnector configuration also affects ESM's ability to automatically create the assets that represent network devices. Each SmartConnector needs to report an IP address or hostname for its sensor so its events can be identified on the network. See the configuration guides for your SmartConnectors to ensure they are reporting this information.

For information on how to import and export SmartConnectors configurations, see ["Importing and Exporting SmartConnector Configurations" on page 527](#).



ArcSight SmartConnectors can send event information to the ESM Manager in a compressed format using HTTP compression. Using compression lowers the overall network bandwidth used by ArcSight SmartConnectors dramatically, without impacting their performance. By default, all SmartConnectors have compression enabled. You can disable compression on SmartConnectors by modifying the `ARCSIGHT_HOME/user/agent/agent.properties` file as described in "Disabling Event Compression" in *Configuring ArcSight SmartConnectors* in *SmartConnector User's Guide*.

Zones

Network zones are address-based network zone information as reported by or assigned to connectors and integrated as an asset property. You can access zone through the [Zones Tab](#) of the Assets resource trees, and the Zone Editor.

The ESM system can gather and integrate zone information by any of the methods. Only one method can apply with a given connector.

- If an AUP file (ArcSight SmartConnector [Content](#) update) is installed with an connector, the zone information, if present, provides addressed-based recognition.
- If a `defaultzones.csv` file is installed in the connector's `ARCSIGHT_HOME/system/agent/acp` directory, it overrides an AUP file if present.
- If the various zone URI values are set in the Connector Editor, in the Network section of the Networks: Content tab, they override URIs from an AUP file, a `defaultzones.csv` file, or the defaults.

In v3.0, you could further control the usage of zone URI field information with the **Address-based Zone Population Defaults Enabled** and **Address-based Zone Population** fields.

- When the first is enabled and there are values in the second, the zones entered in the second field override the defaults, though the defaults are still used for address ranges not covered by the zones entered in the second field.
- When the first is enabled and the second is blank, the defaults (AUP file or [defaultzones.csv](#) file) take effect.
- If the first field is disabled and the second is blank, this connector doesn't do any zone population.
- If the first field is disabled and the second has values, **only** those URIs will be active (the defaults are turned off).

The **Address-based Zone Population Defaults Enabled** and **Address-based Zone Population** fields are not applicable in post v3.5 versions of ArcSight ESM.

Upgrading

ArcSight Enterprise Security Management (ESM) now provides the ability to centrally manage, configure, and update SmartConnectors remotely. You can use the Upgrade SmartConnector utility on the Console to install newer versions of ArcSight SmartConnector software for managed devices, and to review which versions are currently installed. (See [“Upgrading SmartConnectors” on page 529](#).)

The connector upgrade utility is one of control commands available on SmartConnectors. (See [“Sending Control Commands to SmartConnectors” on page 517](#).)

Filtering

SmartConnectors can also act as a filtering tool between devices and the ESM Manager, using filtering conditions. Filtering conditions are set with a combination of AND or OR statements and data field values. Extraneous events are filtered out to minimize the number of events sent to the ESM Manager and analyzed in the ESM Console.



Events filtered out by ArcSight SmartConnectors are not reported to the ESM Manager, so they won't be stored in or available later from the ArcSight Database.

For information on how to import and export filters on SmartConnectors, see [“Importing and Exporting SmartConnector Configurations” on page 527](#) (especially the topic on [“SmartConnector Filters” on page 529](#)).

SMTP

SMTP is used to send e-mail. An SMTP server must be configured either at install time or through context (right-click) menu e-mail settings. For [Notifications](#), the relevant fields are "from address", which designates the e-mail address of notification e-mail sent from ESM, and the "outgoing e-mail server," which is the SMTP server ESM uses to send e-mail. It is important to ensure that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses. POP3 and IMAP can be used to check for e-mail acknowledgments.

You can specify these options at install time, or through context (right-click) menu e-mail option settings. For acknowledgements, the relevant fields are "incoming mail server,"

which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager providers with host and port information using the Context (right-click) menu Pager Settings option.



For notifications sent by pager, firewalls must be configured so that the pager can connect directly to the paging service provider. ArcSight ESM currently supports any provider that supports SNPP. For notifications sent by cell phone, any cell phone must be e-mail enabled. For notifications sent by e-mail, you need to add an address to the e-mail Address field.

Sortable Field Sets

Because ESM processes large numbers of [Data Fields](#) from many sources, it is important to carefully manage which fields are subject to the additional indexing that supports sorting.

This sorting is represented by the ascending and descending **Sort Column** and **Remove Sort** commands you can apply in the headers of grid view columns. This is also the sorting that you apply through the **Sort Fields** tab in the Active Channel Editor when creating or editing channels.

Enabling all fields for sorting, or allowing on-the-fly sort indexing for previously unindexed fields, are both impractical for real-world performance. The practical solution is to select and index the most order-significant or frequently used fields and to make these fields readily available in clearly marked sets. Therefore, field sets are available from a Navigator panel resource in Active Channels called Sortable Field Sets. (In the Navigator, choose **Active Channels**, and click the **Field Sets** tab.)

Sortable field sets are like other [Field Sets](#), except that they are composed only of fields for which sort indexing has been enabled.

Like other resources, sortable field sets are associated with user groups to control access, through the ACL Editor, which edits Access Control Lists. (See ["Editing Access Control Lists \(ACLs\)" on page 443.](#))

The selection of sortable fields and the named sets these fields are collected in are often customized during initial installation for an enterprise, and are usually tailored further after production use begins. Therefore, a reliable list can't be published in advance.

If you try to add an unsortable field to a sortable field set, or try to select sorting for an unsortable field in the **Sort Fields** tab in the Active Channel Editor, the Console alerts you about the field's status.




Notes:

- Sortable fields belong to exclusive sets. This means that if you use a sortable field from one sortable field set to control an active channel, you cannot use sortable fields from other sets as secondary sort controls.
- The field sets in the System Field Sets folder should not be edited by users. If edits do occur by mistake, the system will auto-restore those resources to their defaults in about an hour.

To change an existing non-sortable field to sortable, contact your ESM administrator.



[Variables](#) are not subject to indexing and therefore are not candidates for sortable field sets.

Using Sortable Columns in Grid Views

In grid views (including [Active Channels](#)), the names of sortable fields in column headers are indicated with a double arrow icon  and the **Sort Column** right-click command is enabled. Unsortable fields lack the icon and disable **Sort Column**.

To sort a list per a particular column, right-click over the column name and choose **Sort Column**.

If a field is already sorted, one of two additional icons is shown next to the column name indicating which direction the sort is applied.

- A down arrow  indicates a "top-down" sort is in effect on that field. (For example, when the event End Time field is sorted top-down, newer events are displayed at the top of the list and older events at the bottom. When the Priority field is sorted top-down, events are listed from higher to lower priority.)
- An up arrow  indicates the reverse ("low-to-high") sort in effect on that field. (For example, if the event End Time were sorted this way, older events show at the top of the list and newer events at the end. Similarly, a reverse sort on the Priority field would put low priority events at the top of the list.)

When **Sort Column** is chosen on a sortable field, a "low-to-high" sort is applied first (for example, show events from lowest to highest priority if the Priority field is sorted). If **Sort Column** is selected again, the sort order toggles to the reverse of the previous sort (high to low priority, per our example). The **Remove Sort** option disables the sort and returns the list to its unsorted state with regard to that particular column.

Multiple columns can be sorted simultaneously. The most recently applied sort will take precedence.

See also ["Applying a Field Set to an Active Channel" on page 94](#) and ["Sorting Events in an Active Channel" on page 93](#).

Status Monitor Events

ESM status monitor events can reveal and isolate many different quantity and time-unit issues that bear directly on performance and capacity. There are many possible applications of this system-state data, but those applications must always be interpreted within the context of your particular hardware, software, and network environment, and the deployment choices you have made for ESM and your SmartConnectors.

Compare status monitoring events, which provide information about a wide variety of *system states*, to [Audit Events](#), which report on *system activity*.

Active Channel Statistics

Active channel statistics, specifically any changes that occur in the counts they report, can indicate performance issues and the use of processing cycles. These events summarize:

- The number of currently open Active Channels

- The number of events inserted into Active Channels per second
- The number of events changed across all open Active Channels per second

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveChannels/Open	monitor:100	Open active channel count	Count, current value.
/Monitor/ActiveChannels/Events/Insertions	monitor:174	Active channel event insertions per second	Count per second, since last monitor event.
/Monitor/ActiveChannels/Events/Changes	monitor:175	Active channel event changes per second	Count per second, since last monitor event.

Active List Statistics

Active list statistics monitor the resources being used by active lists. Active lists entries use some memory and database resources, and use CPU resources when they are referenced by other parts of the system (e.g., rules, reports, and filters). While changes to these temporary lists are not persisted, they do represent some memory overhead. Note that when active lists are used by replay-with-rules, this also creates temporary lists.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveLists/ListCount	monitor:114	Open active list count	Count, current value.
/Monitor/ActiveLists/EntryCount	monitor:115	Active list entry count	Count, current value.
/Monitor/ActiveLists/EntryCapacity	monitor:116	Active list entry capacity	Count, current value.
/Monitor/ActiveLists/EntryPercentUsed	monitor:117	Active list entry usage	Percent, current value.
/Monitor/ActiveLists/TemporaryListCount	monitor:118	Temporary Active list count	Count, current value.
/Monitor/ActiveLists/TemporaryEntryCount	monitor:119	Temporary Active list entry count	Count, current value.
/Monitor/ActiveLists/TemporaryCapacity	monitor:120	Temporary Active list capacity	Count, current value.
/Monitor/ActiveLists/TemporaryPercentageUsed	monitor:121	Temporary Active list usage	Percent, current value.
/Monitor/ActiveLists/QueriesPerSecond	monitor:122	Active list queries per second	Count per second, since startup.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveLists/ChangesPerSecond	monitor:123	Active list changes per second	Count per second, since startup.

Asset Statistics

Asset statistics offer insight into performance areas that affect assets in the system and can help resolve source, destination, agent, and device asset issues for incoming events. These events summarize:

- **Asset resolutions per second** is the average number of end-points in events, that are resolved to assets in a second.
- **Asset resolutions average time** is the average time in milliseconds taken to resolve an end-point in an event to an asset.
- **Asset scanner events per second** is the number of scanner events processed in a second.
- **Asset scanner events average time** is the average time in milliseconds taken to process a scanner event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Asset/TotalCount	monitor:200	Asset total count	Count, current value.
/Monitor/Asset/Scanner/EventsPerSecond	monitor:201	Scanner events processed per second	Count per second, since last monitor event.
/Monitor/Asset/ResolutionsPerSecond	monitor:202	Asset resolutions per second	Count per second, since last monitor event.
/Monitor/Asset/Scanner/AverageTime	monitor:203	Scanner event average processing time	Count per second, since startup.
/Monitor/Asset/ResolutionsAverageTime	monitor:204	Asset resolution average time	Microseconds per count, since startup.
/Monitor/Asset/ResolutionsAverageTime/Source	monitor:205	Asset source resolution average time	Microseconds per count, since startup.
/Monitor/Asset/ResolutionsAverageTime/Destination	monitor:206	Asset destination resolution average time	Microseconds per count, since startup.
/Monitor/Asset/Size	monitor:240	Transitive closure size	Count, current value.

Data Monitor Statistics

The data monitor statistics indicate how intensively the data monitors are working, which in turn can indicate situations such as filters needing adjustment or data monitors needing restructuring. These events summarize:

- **Active probes** is the number of currently enabled data monitors.
- **Evaluations per second** is the number of events times the number of enabled data monitors per second.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/DataMonitors/ActiveProbes	monitor:101	Active data monitor probe count	Count, current value.
/Monitor/DataMonitors/EvaluationsPerSecond	monitor:124	Data monitor evaluations per second	Count per second, since last monitor event.

Event Broker Statistics

These statistics monitor reading events from, and writing events to, the database. As such, they are database health indicators. These events summarize:

- **Event count** is the number of events inserted into the database since the last monitor event.
- **Insert time** is the average time taken to insert each event into the database, in microseconds.
- **Retrieval time** is the average time taken to retrieve each event from the database in microseconds.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/EventBroker/InsertTime	monitor:102	Events insertion time per event	Microseconds per count, since last monitor event.
/Monitor/EventBroker/InsertedEventCount	monitor:103	Events processed count	Count, since last monitor event.
/Monitor/EventBroker/RetrievalTime	monitor:140	Events retrieval time per event	Microseconds per count, since last monitor event.

Filter Engine Statistics

The count of in-memory filter evaluations can serve as a broad indicator of filter performance.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Filters/EvaluationCount	monitor:161	Filter evaluation count	Count, since last monitor event.

Main Flow Statistics

These events report statistically on the overall throughput of the ESM Manager, for both incoming and internal events. This flow is the sequence of processing steps applied to each event and is a broad indicator or benchmark of system traffic. These events summarize:

- **Count** describes the number of events that have passed through the flow since the manager started.
- **Rate** describes the current event rate in events per second.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/MainFlow/EPS	monitor:230	Main flow event rate	Count per second, since last monitor event.
/Monitor/MainFlow/Events	monitor:231	Main flow event count	Count, since startup.

Notification Statistics

This group reports on notification activity, which can be of diagnostic value in detecting unusually high notifications activity.

- **New count** describes the number of new notifications since the last monitor event.
- **Escalated count** describes the number of notifications that were escalated since the last monitor event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Notification/New	monitor:180	New notification count	Count, since last monitor event.
/Monitor/Notification/Escalated	monitor:181	Escalated notification count	Count, since last monitor event.

Pattern Discovery Statistics

These events provide statistics for recent or pending pattern discovery runs. Because pattern discovery is database-intensive, these statistics can indicate or help diagnose database performance issues.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Patterns/RunCount	monitor:190	Pattern discoveries run count	Count, since last monitor event.
/Monitor/Patterns/RunsQueued	monitor:191	Pattern discoveries queued count	Count, current value.

Report Statistics

These events provide statistics about the current number of reports querying the database or being rendered. Because reports are database-intensive, these statistics can indicate or help diagnose database performance issues.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Reports/Running	monitor:130	Reports running count	Count, current value.
/Monitor/Reports/RunningQueryingDB	monitor:131	Reports querying database count	Count, current value.
/Monitor/Reports/RunningRendering	monitor:132	Reports rendering count	Count, current value.

Resource Framework Statistics

Resource-framework events report on the database activity connected with updates (reads, writes, and deletions) to system resources such as rules, assets, and filters, since the last monitor event. This data can be valuable in tracking or diagnosing performance-related issues such as automatic asset maintenance, the threat-level formula, or rule-driven usage.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Resource/Activity/Insert	monitor:171	Resources inserted per second	Count per second, since last monitor event.
/Monitor/Resource/Activity/Update	monitor:172	Resources updated per second	Count per second, since last monitor event.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Resource/Activity/Delete	monitor:173	Resources deleted per second	Count per second, since last monitor event.

Rules Engine Statistics

The statistics related to the ESM Manager's rules engine can help reveal performance issues in several areas. Please remember that information about rules activity always needs to be considered in the full content of the Manager's operations. For example, a busy Moving Average data monitor, if used inefficiently, can affect several of these statistics; a poorly written rule can inadvertently drive up the rate of actions executed.

These statistics have the following performance implications

- Count of events inserted into the rule engine: CPU.
- Rate of event insertion into the rule engine: CPU.
- Count of correlated events generated by the rule engine: CPU.
- Rate of correlated event generation by the rule engine: CPU.
- Count of events that are still present in rule engine's working memory: memory.
- Count of groupBy cells that are being used by the rule engine: memory.
- Count of rules currently active in the rule engine: comparative value only.
- Rate of actions being executed by the rule engine: CPU.
- Count of events matching any rule: CPU, memory.
- Count of events matching a rule with single alias: CPU, memory.
- Count of events matching a rule with multiple aliases: CPU, memory.
- Count of events rule matches: CPU, memory.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Rules/InsertedEventCount	monitor:151	Rules total event count	Count, since last monitor event.
/Monitor/Rules/InsertedEventRate	monitor:152	Rules inserted events per second	Count per second, since last monitor event.
/Monitor/Rules/GeneratedEventRate	monitor:153	Rules generated events per second	Count per second, since last monitor event.
/Monitor/Rules/EventsInRuleEngineMemory	monitor:155	Rules in-memory event count	Count, current value.
/Monitor/Rules/GroupByCellsSize	monitor:156	Rules group by cells size	Count, current value.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Rules/ActiveRulesCount	monitor:157	Active rules count	Count, current value.
/Monitor/Rules/ActionsTakenRate	monitor:158	Rules actions rate	Count per second, since last monitor event.
/Monitor/Rules/GeneratedEventCount	monitor:159	Rules generated event count	Count, since last monitor event.
/Monitor/Rules/EventsMatchingAnyRule	monitor:232	Events matching any rule	Count, since last monitor event.
/Monitor/Rules/EventsMatchingFilterRule	monitor:233	Events matching filter rule	Count, since last monitor event.
/Monitor/Rules/EventsMatchingJoinRule	monitor:234	Events matching join rule	Count, since last monitor event.
/Monitor/Rules/MatchCount	monitor:235	Match Count	Count, since last monitor event.

Session List Statistics

Session list statistics monitor the resources being used by session lists. Session lists entries use some memory and database resources, and use CPU resources when they are referenced by other parts of the system (e.g., rules, reports, and filters).

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SessionLists/ListCount	monitor:260	Open session list count	Count, current value.
/Monitor/SessionLists/EntryCount	monitor:261	Session list entry count	Count, current value.
/Monitor/SessionLists/EntryCapacity	monitor:262	Session list entry capacity	Count, current value.
/Monitor/SessionLists/EntryPercentUsed	monitor:263	Session list entry usage	Percent, current value.
/Monitor/SessionLists/QueriesPerSecond	monitor:264	Session list queries per second	Count per second, since startup.
/Monitor/SessionLists/ChangesPerSecond	monitor:265	Session list changes per second	Count per second, since startup.

Session Management Statistics

This statistic tracks the current number of active user sessions.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Sessions/Active/Total	monitor:160	Active session count	Count, current value.

Side Table Statistics

Side tables are ones held in-memory and in the database to retain common and relatively static information, similar to a cache. The purpose is to improve access times for inserts and queries. Side tables store event data that includes: geographical information, categorization information, agent information, device information and labels for custom strings and numbers.

- **Size** identifies how many entries are presently in the cache.
- **Insert** identifies the number of inserts in the past two hours.
- **Cache misses** identifies how many failed attempts to find entries occurred in the past two hours.
- **Cache hit rate** identifies how many successful attempts to find entries occurred in the past two hours.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SideTable/GeoInfo/HitRate	monitor:210	Geo info sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/GeoInfo/Inserts	monitor:211	Geo info sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/GeoInfo/CacheMisses	monitor:212	Geo info sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/GeoInfo/Size	monitor:213	Geo info sidetable size	Count, current value.
/Monitor/SideTable/Category/HitRate	monitor:214	Category sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Category/Inserts	monitor:215	Category sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Category/CacheMisses	monitor:216	Category sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Category/Size	monitor:217	Category sidetable size	Count, current value.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SideTable/Agent/HitRate	monitor:218	Agent sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Agent/Inserts	monitor:219	Agent sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Agent/CacheMisses	monitor:220	Agent sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Agent/Size	monitor:221	Agent sidetable size	Count, current value.
/Monitor/SideTable/Device/HitRate	monitor:222	Device sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Device/Inserts	monitor:223	Device sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Device/CacheMisses	monitor:224	Device sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Device/Size	monitor:225	Device sidetable size	Count, current value.
/Monitor/SideTable/Labels/HitRate	monitor:226	Labels sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Labels/Inserts	monitor:227	Labels sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Labels/CacheMisses	monitor:228	Labels sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Labels/Size	monitor:229	Labels sidetable size	Count, current value.

SmartConnector Flow Statistics

SmartAgent flow statistics record the event rates that occur at different stages of agent processing. "Sum of" statistics are sums of all values reported by all agents connected to the ESM Manager. All values are statistics over the past 1-minute range. These events summarize:

- **Received event rate** is the rate at which agents receive events from devices.
- **Post filter event rate** is the rate of events that passed the filter (e.g., were not filtered out).
- **Post aggregation event rate** is the rate of event aggregation.
- **Agent-to-manager event rate and count** describe how many events were actually sent to the Manager.

- **Cache size** describes the estimated size of the on-disk agent event cache.

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Agents/Events/ToManager	monitor:104	Agent to-manager event count	Count, since startup.
/Monitor/Agents/EPS/ToManager	monitor:109	Agent to-manager event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/Received	monitor:110	Agent received event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/PostFilter	monitor:111	Agent post-filter event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/PostAggregation	monitor:112	Agent post-aggregation event rate	Count per second, since last monitor event.
/Monitor/Agents/CacheSize	monitor:113	Estimated agent cache size	Count, current value.
/Monitor/Agents/Total/Events/ToManager	monitor:141	Sum of agent to-manager event counts	Count, since startup.
/Monitor/Agents/Total/EPS/ToManager	monitor:146	Sum of agent to-manager event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/EPS/Received	monitor:147	Sum of agent received event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/EPS/PostFilter	monitor:148	Sum of agent post-filter event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/EPS/PostAggregation	monitor:149	Sum of agent post-aggregation event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/CacheSize	monitor:150	Sum of estimated agent cache sizes	Count, current value.

Templates

See ["Report Templates" on page 745](#).

Threat

The means by which the potential of a threat connector to adversely affect an automated system, facility, or operation, can be manifest. A potential violation of security.

Threat Evaluation

ESM incorporates a system of security-threat evaluation that culminates in the Priority field you often see in views, reports, or event details. The Priority field uses a scale of 0-10 to rate incoming [Events](#), with 10 being the most-significant value. Naturally, you use Priority field [Threat](#)-evaluation values as a factor in many types of analyses and [Rules](#)-driven reaction or [Notifications](#) scenarios.

Evaluation Process

Threat evaluation is "always on" and applies to all the events received by the ESM Manager. The evaluation process consists of:

- 1 Identify the targeted asset.

The identification process uses (in this order) the Target Address, Target Host Name, Target MAC Address, or relevant asset address range to classify the targeted asset.

- 2 Identify the targeted vulnerabilities.

Using the targeted asset as a key, the ESM Manager looks up applicable vulnerabilities.

- 3 Match the targeted vulnerabilities with the vulnerabilities of the targeted asset.

When matches occur, one is chosen and placed in the Event Vulnerability field.

- 4 Compute the event's threat-priority value.

It is at this point that ESM performs the computation involving model confidence, relevance, criticality and severity (in this specific order), as described further in the section below.

Evaluation Definitions

The Priority field is a calculated value. It uses a formula that processes the contents of certain [Prioritization Fields](#) that help assess the potential security impact of an event. These fields use information about specific [Assets](#) and [Vulnerabilities](#) to establish models, and a confidence factor concerning the appropriateness of those models. Given confidence about a particular asset/vulnerability model, events directed at that asset can then be evaluated against a combination of factors that include relevance, criticality, and severity.

An event has **relevance** as a threat if it contains an [Attack](#) signature that is genuinely applicable to the targeted [Device](#), and the device is in a posture that would permit a successful attack. For example, is the event aimed at a valid port, and when the port was checked, was it open?

An asset's degree of **criticality** is based on the way it serves your enterprise, as seen from the perspective of the network's asset categories. For example, a server could be

categorized among your "Very High Criticality Assets" because it handles customer financial transactions.

An event has **severity** if the targeted device is of a more sensitive type that is known to be subject to compromise, and the source of the event has been identified as a hostile or suspicious entity. Specifically, this is the value found in the Device Severity field. For example, did the event originate from an arch competitor on your Hostile List and was it aimed at a router on your Compromised List?

These three factors, when enabled by a suitable model confidence value, are averaged to produce the value that appears in the Priority field. If a suitable model confidence value isn't present, then severity and criticality are averaged to produce a value for Priority. The exploited vulnerability is also recorded in the event's vulnerability field. (See ["Investigating Views" on page 98.](#))

The exact numeric weight applied to each possible relevance, severity, or criticality state (such as unknown, low, medium, high, very high) is set through a configuration file named `ThreatLevelFormula.xml`. This file is usually configured prior to deployment, using your enterprise policies to guide relative value choices.

Maintaining Model Confidence

The asset/vulnerability model confidence for various network devices is based on correlations between the asset and vulnerability resources you can see in the resource trees of the Console's Navigator panel. Fresh vulnerability information that correlates well with a particular asset's identification results in greater model confidence.

Stated more directly, the model is the sum of the resources that describe the protected and external networks: assets, asset ranges, asset categories, network zones, and certain active lists.

While asset and vulnerability information can be updated manually, it is more practical to refresh this information by automated means such as vulnerability scanners (i.e., network vulnerability assessment scanners). (See ["Managing Vulnerabilities" on page 476.](#)) ESM can automatically import vulnerability information from certain scanner products. Information drawn successively from the same scanner product is overwritten when duplicative; information from different products is additive. Information about new assets or vulnerabilities generates new resource references, and the ESM Manager automatically matches the new references to their opposites, whether new or old.

It should also be noted that asset resources can be updated in bulk using XML files.

Using Threat Evaluation Information

While the Priority field has many obvious uses, starting with simply sorting the events in grid views, there are other ways to put this and its underlying information to work.

Rules, reports, filters, and any place you can apply logic can use the threat-evaluation operators described in ["Priority Calculations and Ratings" on page 737.](#) You can also use the values described in ["Prioritization Fields" on page 736](#) to perform many threat-related functions.

Limitations and Workarounds

Because it is dependent upon a certain amount and type of event data, threat evaluation can be inhibited by these factors:

- A correlation event, produced by a rule or a data monitor, may not be populated with enough information. Only fields used to 'group by' will be populated in correlated events. Without enough information (such as targeted asset or severity) the threat evaluation will not be able to make a sound decision on the event's priority.
- Over-population of correlated events can also inhibit results. Some ArcSight rules are only used to maintain active lists. These rules do not generate useful new information, but the "group by" they need to use in order to collect the information for an active list may give them the appearance of a seriously offensive event.
- Rules offer the option to set your own priority. If a rule populates the priority attribute, then a threat model component will not change that value.

To compensate, you can use these techniques:

- Use the Priority field's value to control when you do and don't notify.
- If a rule is inferring some new piece of information (such as the classic Brute Force Login Attempt), then make sure that you "group by" sufficient information to be able to characterize the threat later. In the BFLA case, that would mean using the source and target addresses from the base events and setting the severity attribute to, for example, "Low"; the BFL Success rule, on the other hand, would set severity to "Very High".
- If the rule is a bookkeeping rule, try to copy as little information forward as you can, set the severity to low, and set the category to "/informational".

Thresholds

There are two types of thresholds: rule thresholds and event thresholds.

A rule threshold is the point at which a rule is triggered and a correlation event generated.

An event threshold is the number of times the event must occur before triggering the rule threshold.

A rule can have a threshold that states when the rule is triggered and also specify a threshold for each rule event. For example, thresholds can be created so that a rule is triggered only after all the events in the rule have occurred a set number of times.

See also, ["Rules" on page 753](#) and ["Events" on page 722](#).

Time Error Correction

In the context of the ESM [Console](#), time error correction means the synchronization of time between a network [Device](#), its ArcSight SmartConnector and the ESM [Manager](#).

See also, ["SmartConnectors" on page 762](#).

Timestamps

See also ["Timestamp Variables" on page 780](#).

Because timestamps are a key element in network security analysis, it is important to clarify the location, source, and context of the timestamps seen in or processed by ESM.

Security Events

Multiple timestamps are applied to events in the course of processing.

Timestamp	Context
Device Receipt Time	The timestamp applied by the source sensor device upon receipt of the event.
Connector Receipt Time	The timestamp applied by the ArcSight SmartConnector's JVM (Java Virtual Machine) when the event is received from the originating sensor device.
Manager Receipt Time	The timestamp applied by the ESM Manager's JVM (Java Virtual Machine) when the event is received from the ArcSight SmartConnector.
Start Time	The time at which the event actually began, as recorded by the source sensor device or, possibly, a secondary source monitored by that device.
End Time	The time at which the event actually ended, as recorded by the source sensor device or, possibly, a secondary source monitored by that device.

Resources

Timestamps are also applied to the ArcSight resources you see in the Navigator panel.

Timestamp	Context
Resource Created	This timestamp is applied by the ESM Manager's JVM (Java Virtual Machine) when a resource is created.
Resource Modified	This timestamp is applied by the ESM Manager's JVM (Java Virtual Machine) when a resource is changed.

General Information

All timestamps are stored as Coordinated Universal Time (**UTC**) times.

The Console presents timestamps in the local time zone of the host computer using the Java Locale facility.

Log timestamps are produced by the local JVM for that component and are written using the Java Locale facility.

Timestamp Variables

See also ["Variables" on page 784](#), especially the subtopic on ["Timestamps" on page 785](#).

For date and time data fields, such as Detect Time, you can type an actual date value, such as `10/12/2002 8:54:00 AM`, or can use special system variables such as:

- `$CurrentDateTime`: for the date and time the report is run; the system variable is replaced by the current date and time value.
- `$CurrentDate`: for the date the report is run; the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run.

You can also specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: `$CurrentDate - 7d` for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or `$CurrentDateTime - 12h`, which evaluates to the current date time minus 12 hours.

The time and date editing window you access through the **Detect Time** and **Detect Time Offset** fields of the Console's Report Editor can accept month (uppercase "M"), minute (lowercase "m"), and current week (uppercase "W") parameters.

Use spaces to separate these special system variables or parameters from other operators when including them in a condition statement.

Inclusive Timestamps

The Detect Time timestamps reported for **correlated** events include the timestamps of the **base** events that initiated them. The timestamp is that of the most recent base event in the series of base events that caused the correlated event.

For example, an event's Detect Time field in the Event Inspector might now show `22 Sep 2003 18:18:24 PDT` instead of `22 Sep 2003 16:10:29 PDT`, with the difference being that the earlier timestamp represents the last base event rather than a later correlated event.

This refinement helps you interpret correlated events more readily, without the need to trace back through detailed rule chains.



You can also inspect the Connector Time parameter to find out just when a rule triggered (the time that was recorded as the Detect Time in prior releases.)

Time Zone Correction

The "correction" of a local time zone is the number of hours of offset to apply in order to adjust local time to another clock (often UTC or GMT) to synchronize device-time queries, correlation, and filters.

Trends

A trend is an ArcSight resource that defines how and over what time period data will be aggregated and evaluated for trends. A trend executes a specified query on a defined schedule and time duration.

Building trends is a component of ESM Reporting resource tools. Be sure to see [Chapter 11, Building Reports, on page 205](#) for an overview of all reporting tasks and tools, and ["Understanding Reporting Workflow" on page 205](#) to see how Trends fit in to the process of creating a report.

Understanding Trends and Queries

A base trend is made up of one query. Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.

The ArcSight Enterprise Security Management (ESM) system evaluates source data for trends based on event conditions (such as number of worm outbreaks, incident time-to-close, or number of cases closed) or common network elements (such as operating system, business role, or regulatory compliance relevance).

This provides a means of querying not just the current model of the network but to build reports on queries of historical data, scheduled queries, and snapshot trends. Using queries in trends allows you to evaluate, for example, trending statistics on vulnerabilities and incident metrics over time to determine whether your vulnerability posture or incident closing rate is getting better or worse.

ESM provides generic trend reporting and a set of specific reports to show trends on current data. For example, you can evaluate trends by operating system, by role, by compliance requirement, time to close on cases, and number closed.

You can provide a trend on a selected period of time, and pull reports that generate aggregated data. Trends can include case metrics such as time to close, open and time open, number closed, which allows for trending reports on incidents.

For more information, see [“Query-Trend Relationships in Reporting” on page 242](#) in [“Building Trends” on page 241](#).

Building Trends

You can access trends and associated editors in the Reports resource in the ESM Console.

See [“Building a Trend” on page 243](#) for information on how to navigate to and use the Trend Editor for [Defining Trend Settings](#).

Upgrade SmartConnectors

See [“Upgrading SmartConnectors” on page 529](#).

User Groups

User groups are named and organized collections of ESM [Users](#). You can create groups based on departments, permission levels, work shifts, or whatever structure best supports your enterprise.

All users within a group inherit the group's permissions. If permissions are given to or taken from a group, all users within that group gain or lose those permissions. When users belong to more than one group, they receive permissions from all their groups. For example, if a user is in a group that has inspect permissions to all rules and is in another group with inspect permissions to all reports, the user will be able to inspect both rules and reports.

ESM provides these pre-defined groups to help you manage your users:

- **Users:** Lists the current logged-in user and grants permission to inspect and edit their own information.
- **Shared:** Lists groups and users that the logged in user has permissions to.
- **All Users:** Lists all groups and users, only Administrators have permission to this group.

Groups created from the All Users group inherit permissions to only a few ArcSight resources. You can either edit the group ACL to add or remove permissions or create

groups beneath one of the pre-existing groups to inherit a pre-configured set of permissions.

- **Default User Groups:** Lists groups and users with default permissions to all ArcSight resources. For more information on ArcSight resources, see [“Editing Access Control Lists \(ACLs\)” on page 443](#).
- **Administrators:** Lists groups and users with full rights and access to manage all groups and users



Do not delete the Administrators group. ESM relies on the Administrators group to grant administrative access. The Administrators group contains at least one user account. This user account is created during installation.

- **Live Rules Editors:** Lists groups and users with permissions to inspect and edit rules
- **Reports Editors:** Lists groups and user with permissions to inspect and edit reports
- **Unassigned:** Lists users who do not belong to a group

Users

ESM users are individuals who are assigned login names, passwords, and privileges to access and perform operations using the ESM [Console](#) or [ArcSight Web](#) clients. For details on using the Console for various tasks on dealing with users as an administrator, see [Chapter 20, Managing Resources \(for Administrators\), on page 437](#).

You manage ESM users by storing user information, setting passwords, enabling or disabling login functionality, and organizing them into groups. When you create a new user account, a temporary password must be created for the user to login to the ESM Console. The user should change their password during their initial ESM session. For more information on changing passwords, see [“Changing User Preferences” on page 556](#).

As an added security feature, user logins can be disabled. This feature may be used when the user is on an extended leave of absence, if the user ID and password have been compromised, or for any reason the user ID and password should not be used to access the ESM Console.

When ESM users are deleted, they are removed from the Users resource tree but not the ArcSight Database. The deleted user ID is stored in the database for future offline processing and user activity auditing. If the user belongs to more than one group, the user account is deleted from all groups automatically.

User Types

ESM user accounts serve several purposes. To enable giving all users only the minimum set of privileges that are needed for them to fulfill their duties, user accounts have a “user type”. The user type specifies, at a high level, which ESM features a user may access. This mechanism is complementary but does not replace permissions specified by access control lists (ACLs), which allow administrators to control access to ESM resources such as assets, rules, and filters. User types are used primarily to control access to ESM Manager services such as archiving and other management tools.

Most often, user types are used to limit the risk resulting from the fact that user name and password combinations are stored on disk for components that require unattended startup but have to authenticate to the ESM Manager. For example, the ForwardingConnector needs to authenticate to the ESM Manager in order to obtain events, but does not need

access to any of the resource management functionality provided by archive and other management tools.

The currently supported user types are:

- **Normal User:** Has full privileges to use the ArcSight Console or ArcSight Web client, and all tools. Only apply this user type to accounts that actually need access to the ArcSight Manager.
- **Management Tool:** Has only the privileges needed to run certain management tools used in conjunction with network management products.
- **Forwarding Connector:** Has only the privileges needed by the ForwardingConnector.
- **Archive Utility:** Has only the privileges needed to run the archive utility. Access to specific resources is controlled through ACLs.
- **Connector Installer:** A specialized identity used only to add SmartConnectors to the system.
- **Web User:** Has privileges to use the ArcSight Web client only (not the ArcSight Console or other tools).



Only Normal User accounts can log in to the Console or an ArcSight Web client.

Unassigned users are those that do not belong to a group.

Variables

Variables are data **derived** from "hard" event data, or are **associated** data maintained by ESM. Derived variable data is [Timestamps](#)-oriented. For example, an event's timestamp can produce a day-of-the-week value (e.g., 2 for Tuesday). Associated variable data concerns [Assets](#) and [Categories Resources](#). For example, a useful asset-category Base Group could be [/All Asset Categories/System Asset Categories/Criticality/Medium](#), which would include any medium-criticality system assets in its scope.

In ESM release v4.0 and newer versions, you can right-click a variable and choose **Copy**, then **Paste** it to another variable tab to avoid re-typing.

You can use variables as another way to tune [Active Channels](#), [Filters](#), [Reports](#), [Rules](#), [Field Sets](#), and [Data Monitors](#), or to expose more information, such as in report or grid view columns. The editors for these tools each include a **Variables** tab you click to add, edit, or remove variables. Note that the variables you create are each local to the resource for which you create them.

Once created, variables appear in the [Common Conditions Editor](#) as additional fields on the Filters or Conditions tabs, or as Group By arguments for data monitors and rules. In the Field Set Editor, variables are an additional category that appears once variables are defined.

Variables are especially useful for situational-awareness applications such as reporting on attacks by division, or for compliance monitoring as in reporting the number of compromise events directed at Sarbanes-Oxley related devices.

Asset-category variables are based on the relevant ESM resource ID of the modeled network asset (device). Timestamp variables are based on the start, end, or receipt times recorded by SmartConnectors, Managers, or devices.



Variables do increase processing overhead and can affect report-generation performance. Consider the performance sensitivity of a report before adding variables.

When you click **Add** in a Variables tab, the Add Variable dialog box can present several fields, depending on the function to be used. All field values can be edited later except the choice of function. To change a Variable from one function to another, create a new Variable and delete the old Variable.

Variables Fields

Variable Field	Description
Name	A name for the variable that is unique to the associated resource.
Function	Each variable implements a single function. Functions are grouped into the following types: <ul style="list-style-type: none"> • Timestamps • String Functions • Group Functions • Type Conversion Functions • Arithmetic Functions • IP Address Functions • List Functions • Conditional Functions
Arguments	The contents of the Arguments section vary based on the Function selected. Functions require one, two, or three data fields as input arguments. The event data field list is filtered to show only fields of the required argument type. For example, the GetMonth function requires a single argument of type timestamp, so the list only shows Agent Receipt Time, Device Custom Date 1, Device Custom Date 2, Device Receipt Time, End Time, Event Annotation Modification Time, and so on.

Timestamps

See also the [“Arithmetic Functions” on page 790](#).

Timestamp variables can use different Time Zones. To see the Time Zone field, click **More Options**. The choices for Time Zone are:

Time Zone	Description
Default Time Zone	The ESM Manager time zone
Agent Time Zone	The time zone of the Connector which sent the event
Original Agent Time Zone	The time zone of the first Connector in a possible chain of connectors which sent the event.
Device Time Zone	The time zone of the originally-reporting device.

Time Zone	Description
Final Device Time Zone	The time zone of the device which reported to the original Connector.

Function Field	Description
Get Day of Month (GetDayOfMonth)	Returns an integer from 1 to 31 to represent the day of the month, based on the selected timestamp.
Get Day of Week (GetDayOfWeek)	<p>Returns an integer from 0 to 6 (0 is Sunday) to represent the day of the week, based on the selected timestamp. The associated day of the week (for example "Sunday") is displayed on the Console UI.</p> <p>You can test the value returned by this function using numeric operations like <code>></code> , <code><</code> , <code>>=</code> , <code><=</code> , <code>=</code> .</p> <p>For example, for a variable called "day" that contains the value returned by the GetDayOfWeek function, you can create an AND logical operator that checks for a weekday with these conditions:</p> <ul style="list-style-type: none"> <code>day >= Monday</code> <code>day <= Friday</code>
Get Hour of Day (GetHour)	Returns an integer from 0 to 23 to represent the hour of the day, based on the selected timestamp.
Get Minute of Hour (GetMinute)	Returns an integer from 0 to 59 to represent the minute of the hour, based on the selected timestamp.
Get Month of Year (GetMonth)	Returns an integer from 1 to 12 to represent the month of the year, based on the selected timestamp.

String Functions

Function	Description
Concatenate	Returns the string result of joining the two string arguments. For example, Concatenate("Arc", "Sight") returns "ArcSight".
Evaluate Velocity Template	Advanced: Evaluates the <i>velocity template</i> argument and returns the result. This function is not available in a Query or Active Channel, and Filters which use this function cannot be used in a Query or Active Channel. For information on how to use Velocity Templates, please see "Velocity Templates" on page 793 .
IndexOf	Returns the integer offset into the first string argument that is the location of the second string argument. For example, <code>IndexOf("Twas the night before Christmas", "night")</code> returns 9. If the second string argument is not found in the first string argument, IndexOf returns -1.
LastIndexOf	<p>Returns the index (position) of the last (rightmost) occurrence of the second argument (the substring) within the first string argument (the source). If the substring is not found in the source, the function returns -1. The first position is index 0, as in the indexOf function.</p> <p>Examples:</p> <pre>lastIndexOf("abc/def/xyz", "/") returns 7 lastIndexOf("abc/def/xyz", "abc") returns 0 lastIndexOf("abc/def/xyz", "klm") returns -1</pre>

Function	Description
LengthOf	Returns the number of characters in the string argument. For example, <code>LengthOf("Twas the night before Christmas")</code> returns 31. <code>LengthOf("")</code> is 0.
Substring	Returns a portion of the first string argument, starting with the position specified in the second, numeric, argument and including the number of characters specified in the third, numeric, argument. For example, <code>Substring("Twas the night", 5, 3)</code> returns "the".
ToLower	Returns the string argument converted to all lowercase. For example, <code>ToLower("Inline Filter")</code> returns "inline filter". Numbers and other non-alphabetic characters are not affected.
ToUpper	Returns the string argument converted to all uppercase. For example, <code>ToUpper("Inline Filter")</code> returns "INLINE FILTER". Numbers and other non-alphabetic characters are not affected.

Group Functions

Name	Description
Format Asset Groups (FormatGroupsOfAsset)	Returns a human-readable list of asset-category URIs unexclusively, meaning that all matching and related categories are included. This variable mainly formats and displays asset category-groups. It is best used with the contents of fieldsets, reports, and data monitor fields. Avoid using this variable in conditions because result order cannot be assured for multi-item groups; instead, use the "get groups" functions for superior ordering and consistency.
Format Network Zone Groups (FormatGroupsOfNetworkZone)	Returns a human-readable list of network-zone URIs unexclusively, meaning that all matching and related zones are included. This variable mainly formats and displays asset zone-resource groups. It is best used with the contents of fieldsets, reports, and data monitor fields. Avoid using this variable in conditions because result order cannot be assured for multi-item groups; instead, use the "get groups" functions for superior ordering and consistency.
Get Group of Asset (GetGroupOfAsset)	Returns a single Asset Category or Asset Category Group, given a Base Field and Base Group. If there is more than one matching category or group, a single URI is chosen at random. Related categories are not included. Output is optimized for correlation operations. The "get groups" (plural) functions return lists of asset categories, therefore their results cannot be used in inGroup conditions. This "get group" (singular) function makes it possible to select one result at random, provided the variable is defined to produce a single result.
Get Zone Group (GetGroupOfNetworkZone)	Return a single zone category. If multiple matches occur, a single URI is chosen at random. Related categories are not included. The "get groups" (plural) functions return lists of zones, therefore their results cannot be used in inGroup conditions. This "get group" (singular) function makes it possible to select one result at random, provided the variable is defined to produce a single result.

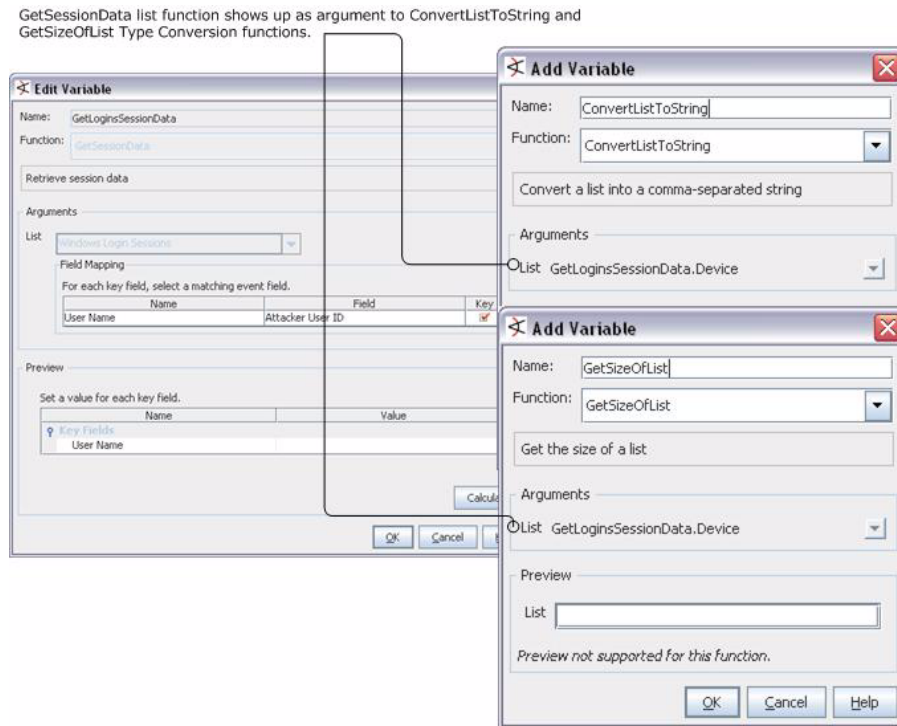
Name	Description
Get Asset Groups (GetGroupsOfAsset)	Returns a list of Asset Categories or Asset Category Groups, given a Base Field and Base Group. In rule and data monitor aggregations this should produce multiple sets. In reports, this produces a comma-separated list of asset-category names. No related categories are excluded. Output is optimized for correlation operations. This function complements the "format groups" functions. It simply shows XML representations of asset categories. Use this function in conditions and in "group by" elements of rules or reports because its output is both well-ordered and consistent.
Get Network Zone Groups (GetGroupsOfNetworkZone)	Returns a list of Network Zone Groups or Asset Category Groups, given a Base Field and Base Group. This function complements the "format groups" functions. It simply shows XML representations of group resources. Use this function in conditions and in "group by" elements of rules or reports because its output is both well-ordered and consistent.

Type Conversion Functions

Function	Description
ConvertListToString	<p>Takes as an argument the value of a multi-valued session list entry and returns it as a comma-separated string (with each entry in the same format as displayed in a channel).</p> <p>For example, suppose you have a session list set up to show user names and IP addresses associated with login sessions. You could get user names from the session list via the <code>GetSessionData</code> variable. If there are three user names on the list (e.g., darren, samantha, and endora), the <code>ConvertListToString</code> variable will return the three names (e.g., <code>[darren, samantha, endora]</code>). You could do the same with the IP addresses.</p> <p>To use this variable, first add a <code>GetSessionData</code> variable. The nested fields that show up in the field selector (<code><VariableNameFromSessionList>.<FieldName></code>) can then be selected as arguments to this function. See Figure 22-8.</p> <p>For more about session lists, see "Identity Correlation" on page 357 and Chapter 16, List Authoring, on page 385.</p> <p>Notes:</p> <ul style="list-style-type: none"> For ESMv.4.5 SP1, this will only work for multi-valued session lists with overlapping entries. The <code>ConvertListToString</code> variable is held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. It cannot be used in resources like Reports, which rely on persisted data. (ESM provides a set of velocity references specifically for use in Reports. Please see "Velocity References for Reports" on page 796 for more information.) More list functions are shown in "List Functions" on page 792.

Function	Description
GetSizeOfList	<p>Takes as an argument the value of a multi-valued session list entry and returns the size of the list.</p> <p>For example, suppose you have a session list set up to show user names and IP addresses associated with login sessions. You could get user names from the session list via the <code>GetSessionData</code> variable. If there are three user names on the list (e.g., darren, samantha, and endora), the <code>GetSizeOfList</code> variable will return the number of names on the list (e.g., <code>[3]</code>). You could do the same with the IP addresses.</p> <p>To use this variable, first add a GetSessionData variable. The nested fields that show up in the field selector (<code><VariableNameFromSessionList>.<FieldName></code>) can then be selected as arguments to this function. See Figure 22-8.</p> <p>For more about session lists, see "Identity Correlation" on page 357 and Chapter 16, List Authoring, on page 385.</p> <p>Note:</p> <ul style="list-style-type: none"> For ESMv.4.5 SP1, this will only work for multi-valued session lists with overlapping entries. The <code>GetSizeOfList</code> variable is held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. It cannot be used in resources like Reports, which rely on persisted data. (ESM provides a set of velocity references specifically for use in Reports. Please see "Velocity References for Reports" on page 796 for more information.) More list functions are shown in "List Functions" on page 792.
ConvertStringToInteger	Returns an integer based on the selected string.
ConvertNumberToString	Returns an integer from 1 to 31 to represent the day of the month, based on the selected timestamp.
ConvertStringToDouble	Returns a double (floating point number) based on the selected string. For example, if a character string event field contained <code>"3.19"</code> , <code>ConvertStringToDouble</code> would return a numeric value of <code>3.19</code> .
ConvertStringToLong	Returns a long (very large integer) based on the selected string.

Figure 22-8 Using Results of GetSessionData for List-related Type Conversion Functions. To use ConvertListToString and GetSizeOfList variables, first create a GetSessionData variable, then you can select fields from that variable as arguments in these Type Conversion Functions.



Arithmetic Functions



The result of any arithmetic function (e.g., Add) is a Long type, even if the original operands are other types (e.g., Integers).

If you want to compare an Integer type field with a Long type field, you can convert the Integer to a Long by using the Add function. For example, suppose you want to compare Bytes In (which is an Integer field) to a custom variable "BytesOut" defined as: `Bytes Out + 100`. Since the variable uses the "Add" function, it will automatically convert to a Long. You cannot compare values whose data types are different. So, create *another* variable for Bytes In (e.g., "BytesIn") defined as: `Bytes In + 0`, which will also convert to a Long. Now you can compare these two variables.

Function	Description
Absolute	Returns the absolute value (its numerical value without regard to its sign) of the numeric argument. The argument may be integer, long integer, or double.
Add	Returns the result of adding the two numeric arguments together. The arguments may be integer, long integer, or double types.
Ceil	Returns the smallest integer value that is not less than the numeric argument. The argument may be integer, long integer, or double.
Divide	Returns the result of dividing the first numeric argument by the second numeric argument. The arguments may be integer, long integer, or double types, but the second argument may not evaluate to 0.
Floor	Returns the largest integer value that is not greater than the numeric argument. The argument may be integer, long integer, or double.

Function	Description
Java Mathematical Expression	<p>(Advanced User Feature) Returns the result of the evaluation of the specified Java expression.</p> <p>Note: ArcSight ESM does not provide error checking and messaging with regard to your JEP expressions. Please refer to the Java Math Expressions Parser web pages at http://www.singularsys.com/jep/ (and other links provided below) for more information on writing these expressions.</p> <p>Supported Expressions: ESM supports use of a subset of Java Mathematical Expressions (JEP), which are written like standard mathematical expressions. A JEP expression has three basic components; operator, function, and value, as described below.</p> <ul style="list-style-type: none"> Operator - Examples of operators are +, -, /, *. JEP operators are documented in the table on this Web site: http://www.singularsys.com/jep/doc/html/operators.html Function - The available functions are listed here: http://www.singularsys.com/jep/doc/html/functions.html <p>ArcSight ESM supports only the following subset of functions listed on the referenced Web site:</p> <p><i>Supported Trigonometric Functions:</i> Sine - $\sin(x)$, Cosine - $\cos(x)$, Arc Sine² - $\text{asin}(x)$, Arc Cosine² - $\text{acos}(x)$, Arc Tangent - $\text{atan}(x)$, Arc Tan with 2 parameters - $\text{atan2}(y, x)$, Hyperbolic Sine - $\sinh(x)$, Hyperbolic Cosine - $\cosh(x)$, Hyperbolic Tangent - $\tanh(x)$, Inverse Hyperbolic Sine - $\text{asinh}(x)$, Inverse Hyperbolic Cosine¹ - $\text{acosh}(x)$, Inverse Hyperbolic Tangent¹ - $\text{atanh}(x)$</p> <p><i>Supported Log and Exponential Functions:</i> Natural Logarithm¹ - $\ln(x)$, Logarithm base 10¹ - $\log(x)$, Exponential (e^x) - $\exp(x)$</p> <p><i>Miscellaneous Functions:</i> Random number (between 0 and 1) - $\text{rand}()$, Modulus - $\text{mod}(x,y) = x \% y$ Square Root¹ - $\text{sqrt}(x)$, Absolute Value / Magnitude - $\text{abs}(x)$</p> <ul style="list-style-type: none"> Value - The values are either constants of numeric type or ArcSight fields, which are referenced by the camel hump notation just like the velocity references, but without the leading '\$'. <p>For information on how to reference ArcSight fields, refer to the "Script Alias" names in "Data Fields" on page 633. For information on velocity references, see "Velocity Templates" on page 793</p> <p>Examples</p> <ul style="list-style-type: none"> The expression "<code>round((bytesIn^2)/1000)</code>" squares the byteIn value of an event, divides the result by 1000, then rounds the result to an integer. To determine if the ratio of "Bytes In" and "Bytes Out" for events is greater than 0.5, use this expression: <code>bytesIn / bytes_out > 0.5</code> (The expression will return "0" if True and "1" if False.) <p>Notes:</p> <ul style="list-style-type: none"> Unlike velocity references, JEP expressions do not use the "\$" in front of ArcSight (ArcField) Data Fields. Be sure that variables used in JME expressions do not include mathematical operator characters or JME function names <i>as a part of the variable name</i>. If a variable name contains any mathematical operator characters (e.g., '+' or '-'), the JME parser will interpret those characters as operators and produce unexpected results. Variable names that match JME function names (e.g., <code>sqrt</code>) will cause similar problems. Some expressions may not be valid and will not produce results. This function is not available in queries or active channels, and filters that use this function cannot be used in queries or active channels. JME variables are held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. JME variables cannot be used in resources like Reports, which rely on persisted data. (ESM provides a set of velocity references specifically for use in Reports. Please see "Velocity References for Reports" on page 796 for more information.)

Function	Description
Multiply	Returns the product of multiplying the two numeric arguments together. The arguments may be integer, long integer, or double types.
Round	Returns the closest integer to the numeric argument. The argument may be integer, long integer, or double.
Subtract	Returns the result of subtracting the second numeric argument from the first numeric argument. The arguments may be integer, long integer, or double types.
Time Difference	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in a human-readable format.
Time Difference in days	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in days.
Time Difference in hours	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in hours.
Time Difference in minutes	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in minutes.
Time Difference in seconds	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in seconds.

IP Address Functions

Function	Description
ParseIPAddress	Returns an integer from 0 to 255 to represent the value of one octet of the specified IP address. For example, <code>ParseAddress(216.109.112.135, 1)</code> would return 216. <code>ParseAddress(216.109.112.135, 4)</code> would return 135.

List Functions



See also [ConvertListToString](#) and [GetSizeOfList](#) shown under “Type Conversion Functions” on page 788.

Function	Description
GetActiveListValue	Returns the value associated with a specific field of the specified Active List.
GetSessionData	Returns the value associated with a specific field of the specified Session List.

Conditional Functions

Function	Description
ConditionalEvaluation	The ConditionalEvaluation function takes three arguments: a Filter which acts as a conditional expression, a value to return if the expression evaluates to True, and a value to return if the expression evaluates to False.

Velocity Templates

ArcSight ESM supports the use of *velocity templates* or scripts as defined by The Apache Velocity Project (<http://velocity.apache.org/>). Velocity templates are a means of specifying dynamic or variable inputs to, or outputs from, underlying Java code.

In ESM, there are a number of places where a person familiar with Velocity templates can specify inputs using Velocity, instead of a literal value, to greatly enhance the results.



(Advanced User Feature)

- Because Velocity templates do have such wide-ranging and sophisticated possibilities, and mis-application or inappropriate application is entirely possible, ArcSight ESM cannot assume responsibility for adverse results caused by user-supplied Velocity templates.
- ArcSight ESM does not provide error checking and messaging with regard to your velocity expressions. Please refer to the Apache Velocity Project web page at <http://velocity.apache.org/> for more information on using velocity templates.
- Velocity template based variables are held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. Velocity template based variables cannot be used in resources like Reports, which rely on persisted data. (ESM provides a set of velocity references specifically for use in Reports. Please see "[Velocity References for Reports](#)" on page 796 for more information.)

Velocity Application Points

Velocity template support appears both in the ESM user interfaces and in certain configuration files. The designated Velocity access points are described below.

Stated briefly, Velocity templates can be applied in most places where a literal string might be enhanced by a conditional or variable string. Common examples are formatting time expressions or condensing fine units into more meaningful groupings.

Application Point	Description
Rules Action Parameters	You can use Velocity templates in Add Action dialog boxes to create or edit fired-rule behavior. You get to these from the Actions tab or the Rules Editor. The Command and Parameters fields for Execute Command actions are Velocity candidates, as is the message-subject text in the Message field of Send Notification actions.
Custom Columns	Velocity templates are also applicable in the Cell Format and ToolTip Format panels of the Custom Columns Editor, which are described in " Customizing Grid Columns " on page 111.
SmartConnector Configuration	The URI strings in the Default Content tab of the Connector Editor can accept Velocity templates.
Case Audit Events	ArcSight audit events concerning cases can also be customized with Velocity templates, through properties files. In the case.default.properties or case.properties files (which overrides the former file), found at \$ARCSIGHT_HOME/config/audit, you can replace the expression in a key-value pair with a template variable or specify an additional field.

Application Point	Description
Notification Messages	In addition to using the Message field of Send Notification actions in the Add Action dialog box, you can also add Velocity templates to the destination-oriented notification configuration files located with the ArcSight Manager at \$ARCSIGHT_HOME/config/notification. This text controls message content (in contrast to the subject line).
Reports Text Fields	You can use a specific set of Velocity references for Report parameters when creating, editing, scheduling or running Reports and Focused Reports. Velocity references for Reports are covered in detail in “Velocity References for Reports” on page 796 .

Using Velocity Expressions in Rule Actions to Retrieve Values from Event Fields or Variables

You can use velocity expressions in rule actions to retrieve the value of an event field or variable. These expressions can be used in commands or notification messages in rule actions.

Retrieving Values from Event Fields

To retrieve the value of an event field, use the field name in "camel notation" without any spaces, preceded by a dollar sign (\$):

```
$<fieldNameInCamelNotation>
```

For example, to retrieve the value of the "Attacker Address" field, use:

```
$attackerAddress
```

For more information on event fields, see [“Data Fields” on page 633](#).

Variables

To retrieve the value of a variable, use the variable name preceded by a dollar sign (\$) without dots: `$<dvName>`

For example, to retrieve the value of the variable `dhcp.Hostname`, use: `$dhcpHostname`

For more information on variables, see [“Variables” on page 784](#).

Example of Rule Action that Uses Velocity Expressions to Retrieve Values

Following is an example of using both types of velocity expressions in a rule action to retrieve values from an event field (`Attacker Address`) and a variable (`dhcp.Hostname`):

- 1 In the Navigator panel, choose **Rules** from the drop-down menu.
- 2 Create or edit a rule.
- 3 Click the **Actions** tab.
- 4 Right-click on a rule action and choose the **Send Notification** rule action.

The notification subject can be constructed as follows:

```
"Brute force login attempt from IP Address: $attackerAddress
Hostname: $dhcpHostname"
```

- 5 Click **OK** or **Apply** to save the rule.

When the rule action is triggered, the notification message will replace the event field velocity expression "`$attackerAddress`" with the value of the Attacker Address field, and the variable velocity expression "`$dhcpHostname`" for the value of `dhcp.Hostname`.

Examples

You might use a Velocity template in a Zone URI field in an Connector Configuration Editor to specify a conditional target, as in:

```
#if($deviceHostName.equals("foobar")) /All Customers/SuperCustomer #end
```

If you are setting up zones based on customers and you want to populate those values dynamically, you could use the following statement to populate fields based on host names, etc. For example, if you have one connector that collects events from devices monitoring different customers networks, you may want to set the customer name based on the device hostname.

```
device hostname = companyx.arcsight.com
```

The following sets the customer name to "arcsight.com":

```
CustomerURI=/All
Customers/$deviceHostName.substring($deviceHostName.indexOf("."))
```

You can set the customer field from the SmartConnector as well, so events from a particular SmartConnector or device can be tagged as "customer xyz" (provided that Customer URI does exist on the Manager) and you can make ACLs limiting the customers' event privileges so they see only events tagged as "customer xyz". If you have one SmartConnector that monitors devices reporting from multiple customers, you can dynamically set the customer name to be based on the device hostname. For example, if you have a customer named "arcsight" and the device hostname is "device1.arcsight.com", the following template returns "arcsight" as the customer name:

```
CustomerURI=/All
Customers/$deviceHostName.substring($deviceHostName.indexOf("."),$
deviceHostName.lastIndexOf(".")).substring(1)
```

The result would be the URI: `/All Customers/arcsight`

For a case audit event in case.default.properties, a template could consist of:

```
deviceCustomString3=$history
```

Usage Tips

- ArcSight Variables. You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as `$Now` and `$CurrentDateTime`. The same is true for time elements, including `s` (second), `m` (minute), `d` (date), `M` (month), `w` (week), and `y` (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign. For example, "Source Address" would be `$sourceAddress`.
- Use of regular expressions is not tested or supported.
- Velocity templates apply **only** to fields that contain string or numeric values.

- You can conveniently test Velocity templates by trying them first in a customField of an active channel.

Velocity References for Reports

The following Velocity references are available for use in [Reports](#) anywhere where Text is used. These references pick up, contain, display, and print the given values. Generally, Velocity references in Reports are used for display and print purposes when creating, editing, scheduling or running Reports and Focused Reports. In some cases, they are used for more than that. For example in archived reports, [\\$Archive_Report_Folder](#) and [\\$Archive_Report_Name](#) determine the location where reports will be stored.



The following table shows the complete set of applicable references for use with Reports. Other types of references (such as those discussed in the previous sections of this topic) do not apply to Reports. However, most of the [Usage Tips](#) detailed above also do apply to Velocity Templates for Reports.

Category	Reference	Description
Report	\$ReportName	Prints the name of the report, as specified in the Name field on the Attributes tab of the Report Editor.
	\$AccessDisclaimer	Prints a disclaimer statement regarding the user permissions with which the report was run. The disclaimer statement is a read-only string which is generated when report data has been filtered due to limited access privileges of the user Reports are generated only with data for which the current user has access privileges. Depending on user permissions for the user running a given report, access to some types of events or data may be curtailed. In such cases, the report is generated with all the information for which the user has access privileges. Events and data requiring higher-level access privileges are not included in the report. The access disclaimer statement is a standard explanation of the limitations of such a report.
	\$CurrentPageNumber	Prints the current page number of the report.
	\$TotalPageNumber	Prints the total number of pages in the report.

Category	Reference	Description
Time	\$CurrentDateTime	Prints the current date and time. (Same as \$Now) Example output: 12-06-2006-15:32:19. Tip: Formats for dates and times depend on your Console preference settings. To change the way dates and times are displayed throughout the Console, choose Edit > Preferences , then click the Date & Time button. For more information, see "Changing User Preferences" on page 556 .
	\$CurrentDate	Prints the current date per your format preferences. Example output: 12-06-2006.
	\$CurrentMonth	Prints the current month. Example output: 12-2006.
	\$CurrentWeek	Prints the current week. Example output: 49-2006 (for December of 2006).
	\$Now	Prints the current date and time. (Same as \$CurrentDateTime) Example output: 12-06-2006-15:33:00.
	\$Today	Prints today's date. Example output: 12-06-2006-00:00:00.
	\$CurrentDateTime-<Number>d	Prints the current date and time minus the number of days you specify. For example, if you ran the report on 12-06-2006 at 15:33:00 and specified the current date and time minus 1 day (\$CurrentDateTime-1d), this reference would output 12-05-2006-15:33:00. If, on the same day, you specified the current date and time minus 3 days (\$CurrentDateTime-3d), this reference would output 12-03-2006-15:33:00

Category	Reference	Description
Parameters	\$Report_Format	<p>Prints the name of the report format that is configured as the default. Output formats are:</p> <ul style="list-style-type: none"> • pdf - Adobe PDF file. • xls - Microsoft Excel file for tables and charts • rtf - Rich-text format document • csv - Tabular data as a list of comma-separated values • html - Web page displayed by the default web browser <p>If the default output format for the report is set to html, then \$Report_Format reference simply will print the word "html".</p> <p>See "Report Parameters" on page 267 in Creating Reports for information on how to set the default output formats for reports.</p>
	\$Page_Size	<p>Prints the page size of the report.</p> <p>Example output: Letter [8.5x11 in]</p>
	\$Run_as_User	<p>Prints the user name specified, if any, for the "Run as User" parameter in the report.</p>
	\$Email_to	<p>Prints the email address specified, if any, for the "Email to" parameter in the report.</p>
	\$Email_Format	<p>Prints the email format specified, if any, for the "Email Format " parameter in the report. For example, "Send URL" or "Attach Report".</p>
	\$Filter_by	<p>Prints the filter(s) used by the referenced query for this report.</p>
	\$Archive_Report_Folder	<p>Prints the folder location where the archived report is stored.</p>
	\$Archive_Report_Name	<p>Prints the name of the archived report.</p>
	\$Archive_Report_Expiration_Time	<p>Prints the expiration time for an archived report.</p>

Category	Reference	Description
	<code>\$<ComponentID>.Row_Limit</code>	<p>Prints the row limit for the specified component.</p> <p>Tip: <code><ComponentID></code> refers to the data components or building blocks of a report. To view the components of a given report, right-click on the report in the Navigator panel, choose Edit Report, and click on the Data tab for the report.</p> <p>For example, if the report contains a component called Table, you can display related information by using the Velocity reference <code>\$Table.Row_Limit</code>, <code>\$Table.Time_Zone</code>, and so forth.</p> <p>Similarly, if the report, contains components called Chart1, Chart2, and Chart3; you can display related information on each of the charts by using references such as <code>Chart1.Time_Zone</code>, <code>Chart2.Start_Time</code>, and so forth.</p>
	<code>\$<ComponentID>.Time_Zone</code>	<p>Prints the time zone for the specified component.</p> <p>For example, <code>Table.Time_Zone</code> would output the time zone used for the data in a component called Table in your report.</p> <p>Example output: America/Los_Angeles</p>
	<code>\$<ComponentID>.Start_Time</code>	<p>Prints the start time for the specified component.</p> <p>For example, <code>Table.Start_Time</code> would output the start time used for the data in a component called Table in your report. (Start Time is a report parameter that can be configured on a per-component basis.)</p> <p>Example output: 12/05/2006 17:46:50.406-0800</p>
	<code>\$<ComponentID>.End_Time</code>	<p>Prints the end time for the specified component.</p> <p>For example, <code>Table.End_Time</code> would output the end time used for the data in a component called Table in your report. (End Time is a report parameter which can be configured on a per-component basis.)</p> <p>Example output: 12/05/2006 18:00:21.140-0800</p>
	<code>\$<ComponentID>.<Parameter_name></code>	<p>Prints the value of the specified component parameter.</p>
	<code>\$Custom.<Parameter_name></code>	<p>Prints the value a custom component parameter.</p>

Views

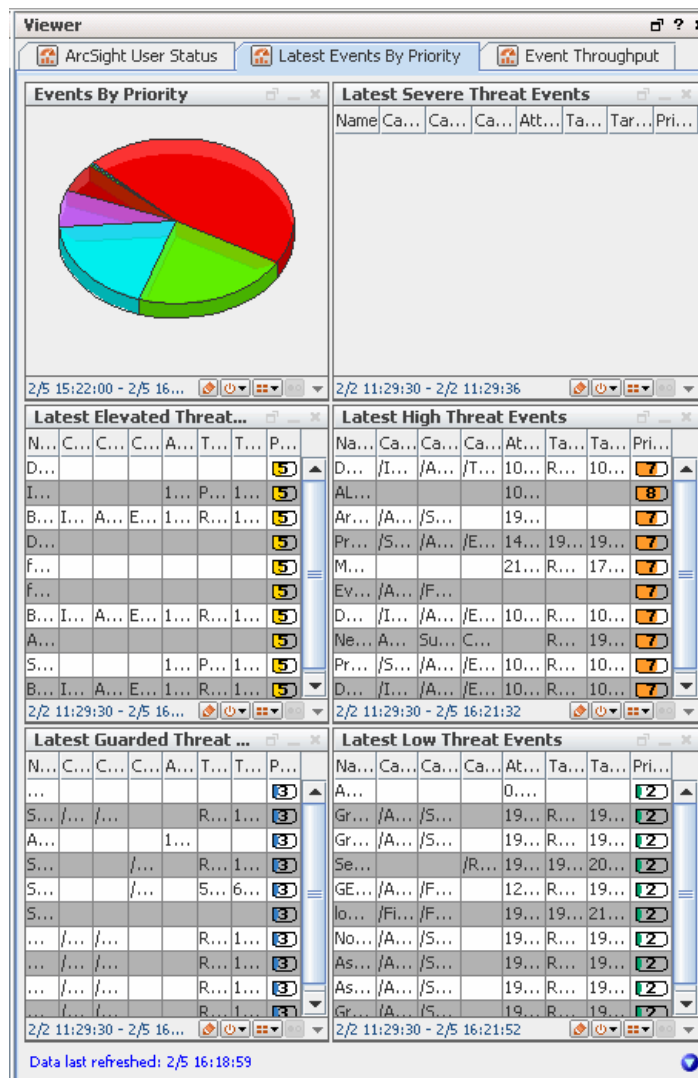
"Views" is a collective term for all the different options you have for seeing raw and processed [Events](#) information in the ESM [Console's](#) Viewer panel.

The Console's Viewer panel can display event information in several formats and is readily customizable. Views may be customized to best reflect an enterprise and can be organized in a hierarchical structure with drill-down functionality. ESM provides a list of chart-format views in addition to grids, maps, and dashboards.

See also ["Viewing" on page 63](#) and ["Monitoring Active Channels" on page 91](#).

View Types

Each view type represented by a tab at the **top** of the Viewer panel serves as a container for all individual instances of that type of view. For example, all data monitors opened in a dashboard remain part of it, and also inherit any visual choices you make for that view. Using the **View Layout** icon at the lower-right corner of the Viewer panel you can choose to tile or tab the individual views. When you tab the views, you select them using the tabs at the **bottom** of the panel.



ESM views give you the flexibility to monitor an enterprise from various perspectives. Views can be customized to best capture and reflect an enterprise's network infrastructure and can also be organized in a hierarchical structure with drill-down functionality. Views can vary in scope and scale, from broad to detailed, depending on how the enterprise is monitored and organized.

The Console provides a number of different views in which you can display event data in the Viewer panel. You can select which views to display by selecting options from the Views menu.

Other Views

The Viewer panel also automatically shows basic HTML-based information such as reports, reference pages, results for the Web Search tool, and notifications in its Web Viewer tabs (as described in [“Viewing” on page 63](#).) The Viewer panel is also where you use the Find Resource query editor and result details display. (See also, [“Finding Resources” on page 534](#).)

Dashboards

Dashboards provide a more customized view of data, letting you create individual “instrument panels”, each of which can display results based on different event data and filter conditions, and in different formats.

From the Viewer panel, you can change the view type or format of individual tabs from grid to line chart, bar chart, pie chart, or graphic. In addition, you can **float** the display of individual sub-view tabs, dashboards, and individual data monitors into separate windows to expand or resize individual displays.

While chart views display a summary of events, grid views display each event. Grid views display events organized in rows and columns. As new events occur, they are inserted at the top of the grid as a new row. Rows contain events while columns contain data fields.

Vulnerabilities

A vulnerability is a hardware, firmware, or software state that leaves an automated information system (AIS) open for potential exploitation. It could be due to anything, including circumstance, configuration, design, or implementation. A vulnerability can also be described as a weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerabilities are discovered using scanners and their associated ArcSight SmartConnectors. ESM imports the output from vulnerability scanners, recording them as items in the Vulnerabilities resource tree, in the Assets section of the Navigator panel. Vulnerabilities are mapped to their associated devices. Vulnerabilities describe asset threats and exposures and provide more information with a link to Knowledge Base articles or notes.

Vulnerability Groups

Vulnerability groups are created to store similar groups of vulnerabilities in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's permissions. If a group

is deleted, the vulnerabilities within that group are also deleted. ESM provides the following groups:

- **Shared:** vulnerabilities to which logged-in users have permission.
- **Unassigned:** vulnerabilities that are not assigned to a group.

If you have Administrator access you will have another group named All Vulnerabilities that contains all vulnerability groups and vulnerabilities.

Standardized Vulnerability Tracking

In the Vulnerabilities tab of the Assets resource tree, ESM includes a branch for using the MITRE Corporation's CVE (Common Vulnerabilities and Exposures) standardized vulnerability naming and reference system.

CVE is a list (dictionary) of standardized names for vulnerabilities and other information security exposures. CVE seeks to standardize the names for all publicly known vulnerabilities and security exposures.

ESM can map CVE as one of its vulnerability reference authorities, within its Navigator panel resource tree. This information can serve, for example, to determine the significance of IDS events. The goal of CVE is to provide a common naming scheme, shared by vulnerability scanners and other security devices to link real-time events to asset vulnerabilities.

With v3.5, ESM gains the ability to search its CVE-related Navigator panel resources by CVE name, and to include CVE names in its Console or report output.

ESM fulfills all the requirements for CVE compatibility through its capacity to analyze event streams utilizing CVE names, generate reports for CVE-related vulnerabilities, map events to asset vulnerabilities, and the existence of documentation for CVE-related functionality.

Index

A

- access control lists
 - for editing user group permissions 447
 - for event permissions 448
 - for operations permissions 446
 - for resource permissions 444
 - for sortable field set permissions 450
 - glossary definition 571
- ACLs, *see access control lists*
- action permissions. *See operations.*
- actions 572
- active channels 572
 - active lists and 574
 - applying resources as filters 155
 - audit events 584
 - charts 103
 - collaborating on events 141
 - field sets 101
 - modifying with filters 159
 - replay-with-rules 326
 - report from grid view 291
 - variables 784
 - view panel 63
 - viewing and using 92
- Active Lists
 - General Configuration 18
- active lists 574
 - audit events for 751
 - automating with rule actions 751
 - case-insensitive 386
 - for identity correlation 375
 - general configuration 24, 26
 - rules for add, remove items to 315
 - using, monitoring 124
- administrator 580
 - certification subjects 53
 - tasks, management 437
 - tasks, permissions and resources 443
 - tasks, send logs to support 758
 - users 443
- agents
 - see SmartConnectors*
- aggregation 580
- alias 552
- arb file
 - see packages*
- archive
 - partitions 548
 - partitions, deactivating 550
 - partitions, reactivating 549
 - partitions, reactivating zipped or large 549
- archive, *see packages*
- ArcSight Console, *see Console*
- ArcSight Express
 - Device list 37
- ArcSight Manager, *see Manager*
- ArcSight Web 580
- Asset Auto-Creation Filters
 - Connector 41
 - Device 42
- Asset Categories 459
 - Criticality 17
- Asset Category Count Data Monitor 692
- asset groups
 - creating 474
- Asset Modeling
 - Protected Network 16, 39
- asset ranges
 - CSV file 466
 - populating using wizard 466
- Assets 457
- assets 581
 - asset tab 581
 - auto-zoning 474
 - categories tab 582
 - creating 470
 - CSV file 464
 - deleting 473
 - editing 473
 - finding 475
 - location tab 583
 - moving or copying 473
 - networks tab 582
 - populating using wizard 464
 - retrieving vulnerable 477
 - scalability 475
 - showing in a channel 473
 - vulnerabilities tab 583
 - zones tab 582
- assets groups
 - deleting 475
 - editing 474
 - moving or copying 475
 - renaming 474
- attack 583
- attributes, common 552
- audit events 583
- auto-zone 474
 - Network Model wizard 468

B

- baselines
 - adding to query viewers 177
- batching 600
- behavior category 607

C

- case editor tab fields 600
- cases
 - attachments 400
 - creating 397
 - creating channels from 401
 - deleting 401
 - editing 399
 - exporting 401
 - finding by ID 399
 - glossary definition 605
 - properties 398
 - queries against 403
 - stages 143
- categories
 - behavior 607
 - custom 614
 - device group 607
 - grouping assets in 470
 - managing as assets 581
 - object 607
 - outcome 607
 - overview 606
 - significance 607
 - tab 582
 - technique 607
- changing a filter 148
- channels, see *active channels*
- charts
 - in channels and data monitors 103
- collaboration 615
- commands
 - integration 405
- common conditions editor 616
- conditions
 - CCE 616
 - common conditions editor 616
 - editor 616
 - glossary definition 626
 - statements 625
- Configuration
 - Active Lists 18
 - Connector Asset Auto-Creation Filter 41
 - Device Asset Auto-Creation Filter 42
 - integration commands 423
 - schedule reports 47
 - set up connectors and model the network 36
- configuration
 - active lists 24, 26
 - Asset Auto-Creation Filters 18
 - Connector Asset Auto-Creation Filter 19
 - Device Asset Auto-Creation Filter 21
 - SNMP Trap Forwarding Filter 22
- connectors
 - see *SmartConnectors* 762

Console

- glossary definition 628
- menus 77
- content 628
- correlation
 - Event Reconciliation Data Monitor 697
 - glossary definition 629
 - rule 629
 - session 760

CounterACT

- integration commands 406

customers

- creating 551
- deleting 551
- editing 551
- managing as a resource 551
- resource 630

D

dashboards

- adding data monitors to 115
- adding query viewers 174
- creating 114
- deleting 115
- editing 115
- glossary definition 630

data fields 633

- derived (shown in italics) 102
- exporting to CSV file 139

data monitors

- adding to dashboards 115
- charts 103
- controlling user permissions to deploy 452
- creating 117
- deleting 118
- deploying, undeploying 118
- editing 118
- enabling, disabling 118
- expressions 720
- glossary definition 692
- overriding last state 120
- permissions to deploy 452
- types 692

database 631

dependencies

- managing in reports 209

deprecated 553

derived fields 102

device 721

device group category 607

Device List

- Standard Content 15

E

editor

- rules 302

editors

- common conditions 616
- image 552
- queries 230
- reports 253
- trends 245

Event Correlation Data Monitor 693
 Event Graph Data Monitor 694
 Event Reconciliation Data Monitor 695
 events
 aliases in rule conditions 752
 audit 583
 categories 606
 categorization, custom 614
 collaborating on 141
 context report 291
 correlation data monitor 693
 data monitors 692
 filtering 147
 glossary definition 722
 graph data monitor 694
 grid views 139
 hierarchy map data monitor 699
 hourly counts data monitor 707
 inspector 721
 last *n* events data monitor 708
 last state data monitor 709
 monitoring 91
 moving average data monitor 710
 payloads 145
 prioritization fields 736
 reconciliation data monitor 695
 status monitor 766
 using attributes to show filtered views 157
 viewing in inspect/edit panel 726
 visualizing 125
 exporting
 cases to external systems 401
 data fields to CSV file 139
 events to a file from grid view 107
 see also *importing and exporting* 107

F

field sets
 creating 101
 editing 102
 glossary definition 723
 see also *data fields* 633
 sharing 103
 sortable 765

fields
 derived (shown in *italics*) 102
 prioritization 736
 see also *data fields* 633
 see also *field sets* 101

files
 adding to packages 490
 as attachments to cases 399
 creating as resources 488
 deleting 490
 downloading 490
 editing resource attributes 490
 finding 491
 managing as resources 488
 replacing 490
 uploading 488
 viewing 490

filter groups
 creating 481
 deleting 482

 editing 482
 moving or copying 482
 renaming 481

filters
 adding an event attribute 158
 adding to resources 155
 creating for SmartConnectors 515
 creating inline 148
 creating new 148
 debugging to match events 151
 deleting 481
 editing 480
 exporting, see *packages*
 filtering out ArcSight events 157
 for showing exploited vulnerabilities 159
 for showing targeted assets 159
 glossary definition 724
 importing, see *packages*
 modifying a view 160
 modifying an active channel 159
 moving or copying 481
 on active channels 155
 on patterns 137
 refining with an event attribute 157
 removing a filter condition 155
 removing a resource 155
 SmartConnectors 516

finding
 resources in the Console 534

Foundations 10

G

graphs
 creating to visualize resources 537
 using 537

grid view
 reports from 291

grid views
 exporting events from 107
 for resources 540
 glossary definition 725

groups
 assets 474
 filters 481
 notifications 483
 reports 293
 rules 303
 SmartConnectors 525
 users 782
 vulnerabilities 478

H

Help
 back, next keyboard commands xxxv
 how to use Console Online Help xxxv
 PDF view, print, or download xxxv
 setting Web display preference 559

Hierarchy Map Data Monitor 699
 hotkeys 563
 Hourly Counts Data Monitor 707
 HTML
 report format 268
 see also *Web*

I**ID**

- external 552
- resource 552
- version 553

iDefense 726

identity correlation, see *session correlation*

image editor 552**importing and exporting**

- active lists 390, 391
- cases to external systems 401
- data fields to CSV file 139
- events to a file from grid view 107
- filters 481
- reports 292
- rules 319
- SmartConnector configurations 527

inline filters

- creating 148
- modify view inline 159
- undoing 159

inspect/edit panel 726

invalid resource
troubleshooting 543

invalid resources

- fixing 541
- overview 540

italics

- on derived fields 102

J

job scheduler 756

K**keys**

- shortcut 563

knowledge base 727

- article groups 435
- associating articles 436
- creating articles for 433
- getting articles 146
- getting updates 436
- managing articles 433

L

Last N Events Data Monitor 708

Last State Data Monitor 709

latitude

- preference setting for locations 561

learning paths 51

lists

- active 574
- session 761

locations

- describing as assets 470
- editor 471
- latitude, longitude format for 561
- managing as assets 581
- tab 583

logical operators 727

logs

- sending to ArcSight 758

longitude

- preference setting for locations 561

M

Managed Security Service Providers, see *MSSPs*

Manager

- glossary definition 728
- performance related to custom rules 330
- reconnecting 63

master use cases 334

menus 77

- Console 77
- Edit 78
- File 77
- Help 81
- System 81
- Tools 80
- Views 78
- Window 79

model confidence

- in prioritization fields 736
- in priority calculations 737
- maintaining by threat evaluation 777

model mappings

- sending to SmartConnectors 517

Moving Average Data Monitor 710

MSSPs

- customer resources for 630
- glossary definition 728
- useful query-trend reporting features for 243

myArcSight

- see ArcSight Web 580

N

navigating resource types 58

navigator panel 729

Network Model wizard

- asset CSV file 464
- asset ranges CSV file 466
- auto-zone 468
- column types 460
- using 459
- zone CSV file 462

Network Modeling

- ArcSight Express 36
- Asset Categories 459
- Assets 457
- auto zone 468
- batch loading 459
- bulk loading 459
- Networks 459
- What is 16
- wizard 459
- Zones 458

network tools

- as integration commands 431
- standard 72

Networks 459**networks**

- describing as assets 470
- editor 472
- managing as assets 581
- sending model mappings to SmartConnectors 517

- tab 582
- notes
 - tabs in resources 76
- notifications
 - acknowledging, managing received 482
 - audit events 591
 - categories 482
 - destinations 484
 - e-mail settings 486
 - glossary definition 729
 - groups and levels 483
 - inbound 482
 - managing 482
 - messages and velocity templates 794
 - pager services 486
 - popup preferences 556
 - rule trigger 315
 - testing groups and destinations 487
 - using 76
 - wait time settings 487
- nslookup
 - integration command 432
 - standard 73

O

- object category 607
- Online Help
 - see *Help*
- operations
 - permissions on 446
 - permissions to deploy data monitors 452
 - setting permissions on 446
- operators
 - logical 727
- outcome category 607

P

- packages
 - adding files to 490
 - adding resources to 496
 - and archive command 498
 - arb import bundles 494
 - creating 492
 - deleting 496
 - editor 492
 - exporting 495
 - glossary definition 731
 - importing 494
 - installing 495
 - managing 491
 - pre-v4.x content 498
 - removing resources from 496
 - resolving conflicts 497
 - uninstalling 495
- panel, navigator 729
- parent groups 553
- partitions
 - archiving 548
 - deactivating archives 550
 - getting information on 548
 - glossary definition 731

- managing 547
- properties 550
- reactivating archives 549
- reactivating zipped or large archives 549
- schedules 548
- schedules, overriding to run tasks now 550
- passwords
 - changing for user 440, 557
 - changing yours 557
- pattern discovery
 - creating profiles 128
 - deleting patterns 137
 - glossary definition 732
 - inspecting patterns 135
 - snapshot 131
 - using 127
 - viewing patterns 137
- payload 736
- payloads
 - for events 145
- PDF
 - getting Console Help as a PDF xxxv
- permissions
 - managing users, user groups 443
- ping
 - integration command 432
 - standard 73
- portinfo
 - integration command 432
 - standard 73
- prioritization fields 736
- priority
 - calculations 737
 - color code 740
- Priority Formula
 - Criticality Asset Categories 17
- profile
 - creating for pattern discovery 128
 - pattern discovery properties 130
- Protected Network
 - How ArcSight determines 39

Q

- queries
 - and trends in reports 242
 - attributes for 230
 - creating 230
 - editing 241
 - editor 230
 - for finding resources in Console 535
 - for reports, glossary definition 741
 - overview 228
 - see also *query viewers* 161
- query viewers
 - adding to dashboards 174
 - baselines in 177
 - custom 164
 - generating reports for 176
 - overview 161
 - pre-built 163
 - see also *queries* in Reporting topics 228
 - using 164

R

- radar display
 - active channel headers 95
 - area in charts 104
 - example, operation in channel headers 574
- reference pages 742
- relevance
 - of events based on priority 736
 - of threats 777
- replay-with-rules channels 326
- Reports
 - scheduling 47
- reports
 - advanced example 276
 - archiving 294
 - beginner example 273
 - copying 293
 - creating 251
 - CSV format 268
 - editor 253
 - end-to-end examples 272
 - exporting 293
 - glossary definition 742
 - groups 293
 - HTML format 268
 - importing 293
 - managing dependencies 209
 - moving 293
 - on query viewers 176
 - on vulnerable assets 479
 - parameterized entries 296
 - PDF format 268
 - queries 228
 - RTF format 268
 - running delta 290
 - running from grid view 291
 - running new or archived 287
 - scheduling 297
 - stopping 60
 - templates 209
 - trends 241
 - variables 784
 - velocity references for 796
 - wizard 273
 - workflow 205
- reports templates
 - creating new 212
 - designer 211
 - designer UI tour 212
 - designing custom 211
 - editing 211
 - glossary definition 745
 - navigating to 209
 - overview 209
 - using pre-built 210
- Resources
 - Shared Resources 12
- resources 746
 - access control lists (ACLs) 571
 - adding filters to 155
 - attributes, common 749
 - attributes, common, in editors 552
 - customers 551, 630

- deprecated 553
- finding 534
- fixing 541
- graphs 537
- graphs, configuring 539
- navigating 58
- notes 76
- printing and saving definitions 83
- saving copies 552
- selecting 533
- sharing 451
- system core content 454
- troubleshooting invalid 543
- validating 540
- viewing in grids 540
- visualizing 537

- rules
 - actions 310, 751
 - aggregate thresholds 308
 - authoring 301
 - automatic disabling 330
 - chains 313, 756
 - conditions 304, 752
 - correlation 629
 - creating 303
 - custom rules and Manager performance 330
 - data monitor, partial match 713
 - deploying real-time 329
 - editor 756
 - enabling, disabling 317
 - errors 324
 - glossary definition 753
 - groups 303
 - importing and exporting 319
 - load and performance 330
 - managing 302
 - pattern discovery action triggers 129
 - replaying events with 326
 - scheduling 319
 - testing 324
 - testing against events 326
 - thresholds and aggregation 308
 - triggering with actions 315
 - variables 784
 - verify with events 326
 - verifying with events 326

Rules Partial Match Data Monitor 713

S

- saving
 - copies of resources 552
- schedules
 - for partitions 548
 - overriding to run partition tasks now 550
- scheduling
 - jobs 756
 - rules 319
- searching
 - for resources 534
 - query options to find resources 535
- send logs 758
 - toolbar command 73

- SendLogs 73
- session correlation 760
- session lists 761
- severity
 - of threats 777
 - setting levels 516
- sharing
 - resources 451
- shortcut keys 563
- significance category 607
- SmartConnector groups 525
 - creating 526
 - deleting 526, 527
 - editing 526
 - moving or copying 526
 - renaming 526
- SmartConnectors
 - adding filter conditions 516
 - commands 517
 - configuration fields 500
 - configuring 498
 - default Content tab configuration fields 501
 - deleting filter conditions 516
 - editor option tabs 499
 - event severity levels 516
 - exporting configurations 528
 - filters 529
 - filters, creating 515
 - flow-control commands 518
 - for ArcSight Express content 37
 - For Standard Content 15
 - getting status 518
 - glossary definition 762
 - importing configurations 527
 - network model mappings 517
 - processing categories 514
 - rollback to previous version 532
 - time interval options 515
 - turbo mode 509
 - upgrading 529
- SmartFolders 60
- SMTP 764
- snapshots
 - pattern discovery 131
- sortable field sets 765
- stages
 - creating for cases 143
 - editing for cases 144
- Standard Content
 - Device List 15
 - Foundations 10
- Statistics Data Monitor 715
- status monitor events 766
- System Content 11
- System Monitor Attribute Data Monitor 718
- System Monitor Data Monitor 717

T

- targets
 - integration commands 426
- technique category 607
- templates
 - reports, see report templates
 - velocity 793

- threat
 - evaluation 777
 - glossary definition 777
- thresholds 779
- time
 - error correction 779
 - timestamp variables 780
 - timestamps 779
 - UTC times 780
 - zone correction 781
- time zone correction 781
- toolbars 70
- tools
 - network 72
- Top Value Counts Data Monitor 718
- traceroute
 - integration command 432
 - standard 73
- Trends
 - About 26
 - Enabling and Disabling 29
- trends
 - and queries in reports 242
 - creating 243
 - editing or viewing definition 251
 - editor 245
 - glossary definition 781
 - interval 242
 - overview 241
 - refreshing data 250
 - snapshot 242
 - testing 249
 - using in queries 251
 - using in reports 251
 - viewing data 249
- TRM
 - integration commands 406
- turbo mode
 - on SmartConnectors 509

U

- Unlocking a User-locked Resource 455
- uploading files 488
- use cases 333
 - applying settings 342
 - categorizing assets/zones 344
 - installing 335
 - master 334
 - navigating to 336
 - opening 336
 - overview 333
 - scheduling daily report 350
 - scheduling monthly report 353
 - scheduling weekly report 351
 - scheduling yearly report 355
 - summary 342
 - wizard 338
- user
 - user-created content 454
- user groups 782
 - ACL edit permissions, deleting 447
 - ACL edit permissions, adding 447
 - creating 442
 - data monitor deploy permissions 452

- deleting 442
- editing 442
- event permissions, adding 448
- event permissions, deleting 448
- moving or linking 442
- operations permissions, adding 446
- operations permissions, deleting 446
- renaming 442
- resource permissions, adding 444
- resource permissions, deleting 444
- setting startup views 443
- sortable field set permissions, adding 450
- sortable field set permissions, deleting 450

users

- access control lists (ACLs) 443
- administrator 580
- creating 438
- deleting 440
- editing 440
- glossary definition 783
- groups, see user groups 782
- moving or linking 440
- passwords 438
- roles and learning paths 51
- types 783

UTC times 780

V

validating resources

- automatic or manual 546
- overview 540
- requirements 543

variables 784

- field sets and 101
- timestamp 780

velocity templates

- overview 793
- references for reports 796
- rules example 794
- usage tips 795

VeriSign iDefense 726

views

- glossary definition 800
- graph 537
- grid 725
- investigating 98
- modifying with filters 160
- Web 64

vulnerabilities

- describing as assets 470

vulnerabilities

- adding an asset to 478
- creating 476
- CVE and 802
- deleting 478
- deleting an asset from 478
- editing 477
- editor 472
- glossary definition 801
- managing as assets 581
- moving or copying 477
- tab 583

vulnerability groups

- creating 478
- deleting 479
- editing 478
- moving or copying 479
- renaming 478

W

Web

- saving, printing resource definitions as HTML 86
- see also ArcSight Web
- setting preference for Online Help display 559
- setting preferred Web browser 557
- viewer panel 64
- viewing Online Help in Web browser xxxv
- WebSearch network tool 72

WebSearch

- integration command 432
- standard 73

whois

- integration command 432
- standard 73

wizards

- Network Model 459
- Use Case 338

Z

Zones 458

zones

- CSV file 462
- describing as assets 470
- editor 471
- managing as assets 581
- populating using wizard 462
- tab 582