
Micro Focus Security ArcSight ArcSight

Software Version: 8.2.0

Configuration Guide for Windows Event Native Smart Connector

Document Release Date: May 2021

Software Release Date: May 2021



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Contents

Configuration Guide for SmartConnector for Microsoft Windows Event Log - Native	36
Product Overview	37
SmartConnector Features	38
Custom Log Support	38
Event Filtering	39
Globally Unique Identifier (GUID)	39
Host Browsing	39
IPv6	39
Localization	39
Collect Forwarded Events	40
Configuring Windows	40
Enabling Microsoft Windows Event Log Audit Policies	40
Enabling an Auditing Policy on a Local System	41
Setting Up an Audit Policy Within a Domain	42
Setting Up an Audit Policy for a Domain	43
Setting Up Standard User Accounts	43
Standard Domain User Account from Windows Server Domain Controllers	44
Standard Domain User Account from Domain Members	44
Standard Local User Account from Windows Workgroup Hosts	45
Add Security Certifications when Using SSL	45
Example: Windows Server 2012	46
Installing the SmartConnector	49
Installation Prerequisites	49
Supported Operating Systems for Installation	49
System Requirements	49
.NET Requirements	49
Supported Operating Systems for Event Collection	49
Supported Log Parsers	50
Supported Applications	50
Supported System Events	50
Supported Events	50
Use of Active Directory Query for Hosts	51
SmartConnector Setup Scenarios	52

Before you Begin	52
Installation Notes	53
Enabling FIPS at the OS Level	53
Installing and Configuring the SmartConnector	53
Using SSL for Connection (optional)	60
Installing and Configuring Multiple Connector Instances	61
Log sources and Event Mappings	62
Microsoft ADFS	62
Supported Versions	63
Configuring Microsoft ADFS Logs	63
Event Mappings for Microsoft ADFS	63
General	63
Event 299	63
Event 300	64
Event 307	64
Event 403	65
Event 404	66
Event 405	66
Event 406 - Windows Server 2016	67
Event 406 - Windows Server 2019	67
Event 410	68
Event 411	68
Event 412	69
Event 413	69
Event 418	70
Event 420	70
Event 424	70
Event 431	71
Event 512	71
Event 513	72
Event 515	72
Event 516	73
Event 1102	73
Event 1200	74
Event 1201	74
Event 1202	74
Event 1203	74

Event 1204	74
Event 1205	74
Event 1206	74
Event 1210	75
Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210	75
Active Directory	77
Audit Active Directory Objects in Windows	77
Configure an Audit Policy Setting for a Domain Controller	77
Configure Auditing for Specific Active Directory Objects	78
Active Directory Event Mappings	80
General Mappings	80
NTDS Database Mappings	81
Event 1000	81
Event 1394	81
Event 1404	81
Event 1844	81
Event 2064	82
Event 2065	82
Event 2886	82
Windows 2008 NTDS Database Mappings	83
General	83
Event 1000	83
Event 1394	83
Event 1404	83
Event 1844	84
Event 2064	84
Event 2065	84
Event 2886	85
General NTDS Mappings	85
Event 1000	85
Event 1004	85
Event 1104	86

Event 1126	86
Event 1308	86
Event 1394	87
Event 1463	87
Event 1844	87
Event 1863	88
Event 1864	88
Event 1869	88
Event 1898	89
Event 1925	89
Event 1926	89
Event 2013	90
Event 2014	90
Event 2041	90
Event 2064	90
Event 2087	91
Event 2088	91
Event 2092	92
Event 2886	92
Windows 2008 General NTDS Mappings	93
Event 1000	93
Event 1004	93
Event 1104	93
Event 1126	94
Event 1308	94
Event 1394	94
Event 1463	95
Event 1844	95
Event 1863	95
Event 1864	96

Event 1869	96
Event 1898	96
Event 1925	97
Event 1926	97
Event 2013	97
Event 2014	98
Event 2041	98
Event 2064	98
Event 2087	99
Event 2088	99
Event 2092	100
Event 2886	100
NTDS ISAM Mappings	101
Event 102	101
Event 103	101
Event 300	101
Event 301	101
Event 302	102
Event 609	102
Event 611	102
Event 612	102
Event 614	103
Event 626	103
Event 700	103
Event 701	103
Event 702	104
Event 703	104
Event 704	104
Windows 2008 NTDS ISAM Mappings	104
Event 102	104

Event 103	105
Event 300	105
Event 301	105
Event 302	105
Event 609	106
Event 611	106
Event 612	106
Event 614	107
Event 626	107
Event 700	107
Event 701	107
Event 702	108
Event 703	108
Event 704	108
NTDS KCC Mappings	108
Event 1104	108
Event 1128	109
Event 1308	109
Event 1926	110
Windows 2008 NTDS KCC Mappings	110
Event 1104	110
Event 1128	110
Event 1308	111
Event 1926	111
Windows 2008 NTDS LDAP Mappings	112
Event 1000	112
Event 1004	112
Event 1126	112
Event 1220	112
Event 1308	113

Event 1394	113
Event 1869	113
Event 2087	114
Event 2088	114
Event 2886	115
Event 2887	116
NTDS Replication Mappings	116
Event 1188	116
Event 1232	117
Event 1863	117
Event 2087	118
Event 2092	118
Event 2887	119
Windows 2008 NTDS Replication Mappings	119
Event 1188	119
Event 1232	120
Event 1863	120
Event 2087	121
Event 2092	121
Event 2887	122
NTDS LDAP Mappings	122
1000	122
1004	122
1126	123
1138	123
1139	123
1213	123
1215	124
1216	124
1220	124

1308	124
1317	125
1394	125
1535	125
1655	126
1869	126
2041	126
2087	127
2088	127
2089	128
2886	129
2887	130
2889	130
Windows 2012/Windows 8 NTDS LDAP Mappings	131
General	131
1000	131
1004	131
1126	131
1138	132
1139	132
1213	132
1215	132
1216	133
1220	133
1308	133
1317	134
1394	134
1535	134
1655	134
1869	135

2041	135
2087	135
2088	136
2089	136
2886	137
2887	138
2889	138
Local Administrator Password Solution	139
Supported Versions	139
Configuring MS Local Administrator Password Solution	139
Mappings for Microsoft Local Administrator Password Solution	140
Event 5	140
Event 10	140
Event 11	140
Event 12	140
Event 13	141
Event 14	141
Event 15	141
Event 16	141
Microsoft Antimalware Logs	142
Supported Versions	142
Mappings for Antimalware	142
Event 1000	142
Event 1001	143
Event 1002	143
Event 1005	144
Event 1011	144
Event 1013	145
Event 1116	145
Event 1117	146
Event 1150	148
Event 2000	148
Event 2001	149
Event 2002	149
Event 2010	150
Event 2011	150

Event 3002	151
Event 5000	151
Event 5001	151
Event 5004	151
Event 5007	152
Event 5010	152
Event 5012	152
Microsoft Windows Defender AntiVirus	152
Supported Versions	152
Microsoft Windows Defender AntiVirus	153
Mappings for Microsoft Windows Defender AntiVirus	153
Event 1000	153
Event 1001	154
Event 1002	154
Event 1009	155
Event 1011	156
Event 1013	156
Event 1015	157
Event 1116	158
Event 1117	159
Event 1150	161
Event 1151	161
Event 2000	162
Event 2001	163
Event 2002	163
Event 2010	164
Event 2011	164
Event 2030	165
Event 3002	165
Event 5000	166
Event 5001	166
Event 5004	166
Event 5007	166
Event 5010	166
Event 5012	166
Microsoft DNS Server Analytics	167
Supported Versions	167
Configuring Microsoft DNS Server Analytic Logs	167

Mappings for Windows 2008 R2	167
General	167
Event 20088	167
Event 20106	168
Event 20184	168
Event 20249	168
Event 20252	169
Event 20255	169
Event 20258	169
Event 20266	170
Event 20271	170
Event 20272	170
Event 20274	171
Event 20275	171
Microsoft Exchange Mailbox Access Auditing	172
Configuring Mailbox Access Auditing	172
Enabling Mailbox Access Auditing	172
Accessing the Audited Information	175
Changing Default Log Storage location	175
Excluding Service Accounts	176
Device Event Mapping to ArcSight Fields	176
Exchange Events 10100, 10101 Mappings	176
Exchange Event 10102 Mappings	177
Exchange Events 10104, 10106 Mappings	178
Exchange Online Message Tracking	179
Device Event Mapping to ArcSight Fields	179
Microsoft Exchange Mailbox Store	181
Configuring Mailbox Store Auditing	182
Enabling Mailbox Store	182
Accessing the Audited Information	183
Changing Default Log Storage location	184
Excluding Service Accounts	185
Device Event Mapping to ArcSight Fields	186
General Exchange Events Mappings	186
Exchange Events 1016 Mappings	186
Microsoft Forefront Protection 2010	187
Configuring Forefront Protection	187
Device Event Mapping to ArcSight Fields	188

Windows 2008	188
General	188
Event ID 7000	188
Event ID 7001	188
Event ID 7002	189
Event ID 7003	189
Event ID 7004	189
Event ID 7005	189
Event ID 7006	189
Event ID 7007	190
Event ID 7008	190
Event ID 7010	190
Event ID 7012	190
Event ID 7015	190
Event ID 7018	190
Event ID 7021	191
Event ID 7024	191
Event ID 7025	191
Event ID 7026	191
Event ID 7028	191
Event ID 7033	192
Event ID 7035	192
Event ID 7040	192
Event ID 7044	192
Event ID 7046	192
Event ID 7048	192
Event ID 7051	193
Event ID 7064	193
FSC Controller	193
Event ID 1000	193
Event ID 1001	193
Event ID 1020	193
Event ID 1021	194
Event ID 1022	194
Event ID 1023	194
Event ID 1024	194
Event ID 1025	194
Event ID 1026	195

Event ID 1028	195
Event ID 1037	195
Event ID 1041	195
Event ID 1043	195
Event ID 1044	195
Event ID 2102	196
Event ID 5167	196
Event ID 5183	196
Event ID 8046	196
Event ID 8055	196
FSC Eventing	196
Event ID 1075	196
Event ID 1076	197
FSC Manual Scanner	197
Event ID 1045	197
Event ID 1048	197
Event ID 1052	197
FSC Scheduled Scanner	197
Event ID 2080	197
Event ID 2081	198
Event ID 3009	198
FSC Realtime Scanner	198
Event ID 2000	198
Event ID 2001	198
FSC Transport Scanner	198
Event ID 2007	198
Event ID 2008	199
Event ID 3002	199
FSC Monitor	199
Event ID 1007	199
Event ID 1008	199
Event ID 1013	199
Event ID 1014	200
FSE On Demand Nav	200
Event ID 1049	200
Event ID 1050	200
FSE Mail Pickup	200
Event ID 1029	200

Event ID 1030	200
FSE IMC	201
Event ID 1002	201
Event ID 1003	201
FSE VS API	201
Event ID 5066	201
FSC VSS Writer	201
Event ID 1094	201
Event ID 1095	201
Get Engine Files	202
Event ID 2011	202
Event ID 2012	202
Event ID 2017	202
Event ID 2034	202
Event ID 2109	203
Event ID 6012	203
Event ID 6014	203
Event ID 6019	204
Event ID 6020	204
Microsoft Netlogon	205
Supported Versions	205
Configuring Microsoft Netlogon Logs	205
Mappings for Microsoft Netlogon	205
General	205
Event 5827	206
Event 5828	206
Event 5829	207
Event 5830	207
Event 5831	208
Microsoft Network Policy Server	209
Supported Versions	209
Configuring NPS Logging	209
Mappings for Network Policy Server	210
Mappings for Windows 2016, 2012, and 8	210
General	210
Event 13	210
Event 25	211
Event 4400	211

Event 4402	211
Event 4405	211
Mappings for Windows 2008 R2	212
General	212
Event 13	212
Event 4400	212
Event 4402	212
Event 4405	213
Microsoft Service Control Manager	214
Supported versions	214
Mappings for Windows 2016, 2012, 8, and 10	214
General	214
7000	214
7001	215
7002	215
7003	215
7005	216
7006	216
7007	216
7008	216
7009	216
7010	216
7011	217
7012	217
7015	217
7016	217
7017	217
7018	217
7019	218
7020	218
7021	218
7022	218
7023	218
7024	219
7025	219
7026	219
7027	219
7028	219

7030	220
7031	220
7032	220
7033	220
7034	221
7035	221
7036	221
7037	221
7038	222
7039	222
7040	222
7041	223
7042	223
7043	223
7045	224
Microsoft SQL Server Audit	225
Supported Versions	225
Configuring SQL Server Audit	225
Customizing Event Source Mapping	226
Microsoft SQL Server Audit Application Event Log Mappings	226
General	226
Event 615	226
Event 849	226
Event 852	226
Event 919	227
Event 958	227
Event 1486	227
Event 1814	227
Event 1945	228
Event 2007	228
Event 2812	228
Event 3406	229
Event 3407	229
Event 3408	229
Event 3421	229
Event 3454	230
Event 5084	230
Event 5579	230

Event 5701	231
Event 5703	231
Event 6253	231
Event 6527	231
Event 8128	232
Event 9013	232
Event 9666	232
Event 9688	232
Event 9689	232
Event 10981	233
Event 12288	233
Event 12291	233
Event 15268	233
Event 15457	233
Event 15477	234
Event 17069	234
Event 17101	234
Event 17103	234
Event 17104	234
Event 17107	235
Event 17108	235
Event 17110	235
Event 17111	235
Event 17115	235
Event 17125	236
Event 17126	236
Event 17136	236
Event 17137	236
Event 17147	237
Event 17148	237
Event 17152	237
Event 17162	237
Event 17164	238
Event 17176	238
Event 17177	238
Event 17199	239
Event 17201	239
Event 17550	239

Event 17551	239
Event 17561	240
Event 17656	240
Event 17658	240
Event 17663	240
Event 17811	240
Event 18453	241
Event 18454	241
Event 18456	241
Event 18488	242
Event 18496	242
Event 19030	242
Event 19031	242
Event 19032	243
Event 26018	243
Event 26022	243
Event 26037	243
Event 26048	244
Event 26067	244
Event 26076	244
Event 30090	245
Event 33090	245
Event 33204	245
Event 33205	245
Event 33217	246
Event 33218	247
Event 49903	247
Event 49904	247
Event 49910	247
Event 49916	247
Event 49917	248
Microsoft Sysmon	249
Supported Versions	249
Configuring Microsoft Sysmon Logs	249
Mappings for Microsoft Sysmon Logs	250
General	250
Event 1	250
Event 2	251

Event 3	251
Event 4	252
Event 5	252
Event 6	253
Event 7	253
Event 8	254
Event 9	254
Event 10	254
Event 11	255
Event 12	255
Event 13	256
Event 14	256
Event 15	257
Event 16	257
Event 17	258
Event 18	258
Event 19	258
Event 20	259
Event 21	259
Event 22	260
Event 23	260
Event 255	261
User 32 Service	262
Supported Versions	262
Configuring Remote Access	262
Mappings for Windows 2008 R2	262
General	262
Event 1074	263
Microsoft Windows AppLocker	264
Supported Versions	264
Configuring Microsoft Windows AppLocker	264
Mappings for Microsoft Windows AppLocker	264
Event 8001	264
Event 8002	265
Event 8003	265
Event 8004	266
Event 8005	266
Event 8006	267

Event 8007	267
Microsoft Windows ESENT	268
Supported Versions	268
Mappings for Microsoft Windows ESENT Logs	268
General	268
Event Id 102	268
Event Id 103	269
Event Id 105	269
Event Id 224	269
Event Id 225	269
Event Id 300	270
Event Id 301	270
Event Id 302	270
Event Id 325	270
Event Id 326	271
Event Id 327	271
Event Id 330	271
Event Id 335	272
Event Id 455	272
Event Id 641	272
Microsoft Windows BITS Client Logs	273
Supported Versions	273
Mappings for Microsoft Windows BITS Client	273
General	273
Event ID 3	273
Event ID 4	274
Event ID 59	274
Event ID 60	275
Event ID 61	276
Microsoft Windows Event	277
Supported Versions	277
Configuring Windows Update Client	277
Windows Update Client	278
Supported Versions	278
Configuring Windows Update Client	278
Mappings for Windows-WindowsUpdateClient	279
General	279
Event 16	279

Event 17	279
Event 18	279
Event 19	280
Event 20	280
Event 21	280
Event 22	281
Event 27	281
Event 28	281
Event 43	281
Event 44	281
Microsoft Windows WMI Activity Trace	283
Supported Versions	283
Mappings for Microsoft Windows WMI Activity Trace	283
Event 11	283
Microsoft Windows WMI Analytic and Operational	285
Supported Versions	285
Mappings for WMI Analytics Operations	285
Mappings for Microsoft Windows WinRM Analytic	285
Event 788	285
Event 789	286
Event 1050	286
Event 1295	286
Mappings for Microsoft Windows WinRM Operational	286
Event 6	286
Event 11	287
Event 15	287
Event 142	287
Event 161	287
Event 162	288
Event 169	288
Event 81	288
Event 82	288
Microsoft WINS Server	289
Supported versions	289
Configuring WINS	289
Windows 2016, 2012, and 8	290
General	290
4097	290

4098	290
4119	290
4143	291
4178	291
4179	291
4180	291
4181	291
4224	292
4252	292
4253	292
4309	292
4318	292
4325	292
4326	293
4329	293
4330	293
4337	293
5001	293
5002	293
Oracle Audit	294
Configuring Auditing	294
Enabling Auditing	294
Auditing Administrative Users	294
Device Event Mapping to ArcSight Fields	295
Oracle Windows Event Log Mappings to ArcSight ESM Fields	295
Event ID 4	295
Event ID 5	295
Event ID 8	295
Event ID 12	296
Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields	296
Event ID 34	296
Oracle Audit Trail Event Mappings to ArcSight ESM Fields	297
Event ID 34	297
Oracle Unified Audit Trail Event Mappings to ArcSight ESM Fields	298
Event ID 36	298
Powershell	299
Configuring Auditing for Specific Powershell Objects	299
Mappings for PowerShell Events	301

General Mappings	301
Windows PowerShell Mappings	301
Event 400, 403	301
Event 500, 501	302
Event 600	302
Event 800	303
Windows Microsoft-Windows-PowerShell/Operational Mappings	304
Event 4100	304
Event 4103	304
Event 4104	305
Event 4105	305
Event 8193	306
Event 8194	306
Event 8195	306
Event 8196, 12039	306
Event 8197	307
Event 24577	307
Event 24579	307
Event 24580	307
Event 24581	307
Event 24582	308
Event 24583	308
Event 24584	308
Event 24592	308
Event 24593	308
Event 24594	308
Event 24595	309
Event 24596	309
Event 24597	309
Event 24598	309
Event 24599	310
Event 40961	310
Event 40962	310
Event 53249	310
Event 53250	310
Event 53504	311
Remote Access	312
Supported Versions	312

Configuring Remote Access	312
Mappings for Remote Access Events	312
Mappings for Windows 2016, 2012, 2012 R2, 8, and 10	313
General	313
20088	313
20106	313
20169	313
20184	314
20249	314
20252	314
20255	315
20258	315
20266	315
20271	316
20272	316
20274	317
20275	317
Mappings for Windows 2008 R2	318
General	318
Event 20088	318
Event 20106	318
Event 20184	318
Event 20249	319
Event 20252	319
Event 20255	319
Event 20258	320
Event 20266	320
Event 20271	320
Event 20272	321
Event 20274	321
Event 20275	322
Collecting Forwarded Events	322
Event Collector for Windows Event Forwarding	323
Source Hosts Windows OS Version	323
Additional Connector Configurations	324
Configuring Custom Logs and Filtering	325
Configuring Filter	326

Specifying Custom Log Names	327
Configuring the Host Browsing Thread Sleep Time	328
Creating a Source Hosts File	329
Collecting Events from the Event Log	329
Configure Advanced Options	330
Access Advanced Parameters	330
Advanced Container Configuration Properties	331
Advanced Common Configuration Parameters	332
Advanced Configuration Parameters per Host	333
Advanced Configuration Parameters for SID and GUID Translation	333
Customizing Event Source Mapping	333
Creating an Override Map File	334
Customizing Event Parsing in a Clustered Environment	334
Creating Custom Parsers for System and Application Events	335
Before Creating a Parser	335
Creating and Deploying Your Own Parser	336
Customizing Localization Support for the Native Connector	340
Troubleshooting	343
Parameters not functioning as expected	343
Log message for resource adjustment	343
A Non-administrator User Is Unable to Run Windows Native Connector and the Log File Has Permission Error	343
Windows Common Security Mappings	344
Specific Windows Security Event Mappings	346
Event Id 1100	346
Event Id 1101	346
Event Id 1102	346
Event Id 1104	346
Event Id 1105	347
Event Id 1074	347
Event Id 4608	347
Event Id 4609	347
Event Id 4610	348
Event Id 4611	348
Event Id 4612	348
Event Id 4614	349
Event Id 4615	349

Event Id 4616	349
Event Id 4618	350
Event Id 4621	350
Event Id 4622	351
Event Id 4624	351
Event Id 4625	352
Event Id 4626	353
Event Id 4627	354
Event Id 4634	355
Event Id 4646	355
Event Id 4647	356
Event Id 4648	356
Event Id 4757	394
Event Id 4758	395
Event Id 4759	395
Event Id 4760	396
Event ID 4761	396
Event ID 4762	397
Event ID 4763	397
Event ID 4764	398
Event ID 4765	398
Event ID 4766	399
Event ID 4767	399
Event ID 4867	420
Event Id 4868	420
Event Id 4869	420
Event Id 4870	421
Event Id 4871	421
Event Id 4872	421
Event Id 4873	421
Event Id 4874	422
Event Id 4875	422
Event Id 4876	422
Event Id 4877	423
Event Id 4878	423
Event Id 4879	423
Event Id 4880	423
Event Id 4881	423

Event Id 4882	424
Event Id 4883	424
Event Id 4884	424
Event Id 4885	424
Event Id 4886	425
Event Id 4887	425
Event Id 4888	425
Event Id 4889	425
Event Id 4890	425
Event Id 4891	426
Event Id 4892	426
Event Id 4893	426
Event Id 4894	426
Event Id 4895	426
Event Id 4896	427
Event Id 4897	427
Event Id 4898	427
Event Id 4899	427
Event Id 4900	427
Event Id 4902	428
Event Id 4904	428
Event Id 4905	428
Event Id 4906	429
Event Id 4907	429
Event Id 4908	429
Event Id 4909	430
Event Id 4910	430
Event Id 4911	430
Event Id 4912	430
Event Id 4913	431
Event Id 4928	431
Event Id 4929	431
Event Id 4930	431
Event Id 4931	432
Event Id 4932	432
Event Id 4933	432
Event Id 4934	432
Event Id 4935	432

Event Id 4936	432
Event Id 4937	433
Event Id 4944	433
Event Id 4945	433
Event Id 4946	433
Event Id 4947	433
Event Id 4948	433
Event Id 4949	434
Event Id 4950	434
Event Id 4951	434
Event Id 4952	434
Event Id 4953	434
Event Id 4954	435
Event Id 4956	435
Event Id 4957	435
Event Id 4958	435
Event Id 4960	435
Event Id 4961	436
Event Id 4962	436
Event Id 4963	436
Event Id 4964	436
Event Id 4965	437
Event Id 4976	437
Event Id 4977	437
Event Id 4978	437
Event Id 4979	438
Event Id 4980	438
Event Id 4981	438
Event Id 4982	438
Event Id 4983	439
Event Id 4984	439
Event Id 4985	439
Event Id 5024	440
Event Id 5025	440
Event Id 5027	440
Event Id 5028	440
Event Id 5029	440
Event Id 5030	441

Event Id 5031	441
Event Id 5032	441
Event Id 5033	441
Event Id 5034	441
Event Id 5035	441
Event Id 5037	442
Event Id 5038	442
Event Id 5039	442
Event Id 5040	442
Event Id 5041	442
Event Id 5042	443
Event Id 5043	443
Event Id 5044	443
Event Id 5045	443
Event Id 5046	443
Event Id 5047	443
Event Id 5048	444
Event Id 5049	444
Event Id 5050	444
Event Id 5051	444
Event Id 5056	445
Event Id 5057	445
Event Id 5058	445
Event Id 5059	446
Event Id 5060	446
Event Id 5061	447
Event Id 5062	447
Event Id 5063	447
Event Id 5064	447
Event Id 5065	448
Event Id 5066	448
Event Id 5067	448
Event Id 5068	448
Event Id 5069	449
Event Id 5070	449
Event Id 5071	449
Event Id 5120	450
Event Id 5121	450

Event Id 5122	450
Event Id 5123	450
Event Id 5124	450
Event Id 5125	451
Event Id 5126	451
Event Id 5127	451
Event Id 5136	451
Event Id 5137	451
Event Id 5138	452
Event Id 5139	452
Event Id 5140	453
Event Id 5141	453
Event Id 5142	454
Event Id 5143	454
Event Id 5144	454
Event Id 5145	455
Event Id 5146	455
Event Id 5147	456
Event Id 5152	456
Event Id 5153	457
Event Id 5154	457
Event Id 5155	457
Event Id 5156	458
Event Id 5157	458
Event Id 5158	458
Event Id 5159	459
Event Id 5168	459
Event Id 5376	460
Event Id 5377	460
Event Id 5378	461
Event Id 5379	461
Event Id 5380	462
Event Id 5381	462
Event Id 5382	462
Event Id 5440	463
Event Id 5441	463
Event Id 5442	463
Event Id 5443	463

Event Id 5444	463
Event Id 5446	464
Event Id 5447	464
Event Id 5448	464
Event Id 5449	464
Event Id 5450	464
Event Id 5451	465
Event Id 5452	465
Event Id 5453	465
Event Id 5456	465
Event Id 5457	466
Event Id 5458	466
Event Id 5459	466
Event Id 5460	466
Event Id 5461	466
Event Id 5462	467
Event Id 5463	467
Event Id 5464	467
Event Id 5465	467
Event Id 5466	467
Event Id 5467	468
Event Id 5468	468
Event Id 5471	468
Event Id 5472	468
Event Id 5473	468
Event Id 5474	469
Event Id 5477	469
Event Id 5478	469
Event Id 5479	469
Event Id 5480	469
Event Id 5483	470
Event Id 5484	470
Event Id 5632	470
Event Id 5633	470
Event Id 5712	471
Event Id 5888	471
Event Id 5889	471
Event Id 5890	472

Event Id 6144	472
Event Id 6145	472
Event Id 6272	472
Event Id 6273	473
Event Id 6274	474
Event Id 6275	474
Event Id 6276	474
Event Id 6277	474
Event Id 6278	474
Event Id 6279	475
Event Id 6280	475
Event Id 6281	476
Event Id 6409	476
Event Id 6410	476
Event Id 6416	476
Event Id 8191	477
Mappings for Microsoft OAlerts	477
Event Id 300	477
Mappings for DNS Client Operational	477
Event Id 1015	477
Event Id 1016	478
Event Id 1017	478
Event Id 3006	478
Event Id 3008	478
Event Id 3009	479
Event Id 3010	479
Event Id 3011	479
Event Id 3012	480
Event Id 3013	480
Event Id 3014	480
Event Id 3016	480
Event Id 3018	481
Event Id 3019	481
Event Id 3020	481
Windows Event Log Event Descriptions by Category	482
Appendix A. Types of Internal Events	505
Specific Windows Security Event Mappings	505

General	505
104	505
1100	506
1101	506
1102	506
1104	506
1105	506
Collector Connected	507
Collector Disconnected	507
Collector Down	508
Collector Configuration Accepted	508
Collector Status for “Collector Configuration Accepted”	508
Host Status for “Collector Configuration Accepted”	509
Event Log Status for “Collector Configuration Accepted”	509
Collector Status Updated	510
Collector Status for “Collector Status Updated”	510
Host Status for “Collector Status Updated”	510
Event Log Status for “Collector Status Updated”	511
Collector Event Collection Started	511
Collector Status for “Collector Collection Started”	511
Host Status for “Collector Collection Started”	512
Event Log Status for “Collector Collection Started”	512
Collector Up	513
Appendix B. Microsoft Windows Event Log Native Connector and Unified	
Features Comparison	514
Windows Event Log - Native and Unified Connector Features	514
SmartConnector for Windows Event Log - Native Limitations	515
Send Documentation Feedback	516

Configuration Guide for SmartConnector for Microsoft Windows Event Log - Native

ArcSight SmartConnectors intelligently collect a large amount of heterogeneous raw event data from security devices in an enterprise network, process the data into ArcSight security events, and transport data to destination devices.

ArcSight SmartConnector for Windows Event Log - Native supports event collection from log sources such as Sysmon, Powershell etc.,

This guide provides a high level overview of ArcSight SmartConnector for Windows Event Log - Native.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microsoft.com.

For specific product issues, contact [Micro Focus Customer Care](#).

Product Overview

The SmartConnector for Microsoft Windows Event Log – Native can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs. It can collect events from

ArcSightSmartConnectors provide easy, scalable, audit-quality collection of all logs from all event-generating sources across the enterprise for real-time and forensic analysis. The ArcSight is optimized for a large number of hosts.

The infrastructure provided with the SmartConnector for Microsoft Windows Event Log – Native (Windows Event Log – Native) has been improved to deliver critical features such as Operational Windows Event Logs and event collection and event filtering from IPv6 hosts. It leverages the native technology on the Microsoft platform and provides the best support for Windows event features and capabilities (including collection for all log types).

The Security events are not audited by default. You must specify the type of security events to be audited.

There are following types for default Windows event logs:

- Application log (tracks events that occur in a registered application)
- Security log (tracks security changes and possible breaches in security)
- System log (tracks system events)

The connector consists of the following major components:

- SmartConnector framework-based event processor
- The Windows API application, which collects events from Microsoft Windows Event Logs
- A Message Queue that facilitates communication between the previous two components

The Windows API event collection and the Message Queue are started by the connector at the time of connector setup and at the start of the connector process.

For SmartConnector security event mappings to ArcSight data fields, see *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings*.

SmartConnector Features

SmartConnector capabilities include real-time event collection and processing, as well as data enrichment (normalization, categorization, Common Event Format (CEF), aggregation, and filtering) and efficiency (caching, batching, compression, and bandwidth management). For more information about SmartConnector capabilities in general, see [SmartConnector Features](#). Specific features of the Windows Event Log – Native connector are described in the following sections.

Custom Log Support

Event collection from non-administrative, operational, or custom logs is provided.

Event Filtering

Filters that apply at the time of event collection from the event source to the connector are supported. With this support, events in which you have no interest can be filtered out, making better use of resources.

Globally Unique Identifier (GUID)

Supports translation and mapping of the GUID (also known as UUID) within a forest (A forest is a complete instance of Active Directory). The connector can perform GUID translation for GUIDs within a forest by querying the Global Catalog Server. The Active Directory parameters are used for Global Catalog Server. The connector is not configured to translate GUIDs by default. See “[Advanced Configuration Parameters for SID and GUID Translation](#)” for more information about enabling GUID translation. Global Catalog and Active Directory must be on the same machine.

Host Browsing

Host browsing is used when hosts are added during installation using Active Directory. Notification is sent to a destination when a new host is added to Active Directory.

IPv6

Supports event collection from IPv6 hosts and parsing of IPv6 events.

Localization

The Windows Event Log – Native connector supports security event localization for the following languages:

Language	Locale	Encoding
French	fr_CA	UTF-8
Japanese	ja_JP	Shift_JIS
Chinese Simplified	zh_CN	GB2312
Chinese Traditional	zh_TW	Big5

The locale and encoding can be specified for the event.name field during SmartConnector installation. See [Configuring Multiple Host Parameters](#). For localization of other languages, see [Customizing Localization Support for the Native Connector](#).

Collect Forwarded Events

The connector has the ability to read events forwarded to a Windows Event Collector host. Windows Event Collection is a Microsoft capability that lets a Windows host collect events from multiple sources. Collecting forwarded events is different than the traditional event collection because the events are collected from multiple sources.

With Microsoft Windows Event Collector (WEC), you can subscribe to receive and store events on a local computer (event collector) that are forwarded from any number of remote computers (event sources). Before using this feature, refer to Microsoft Windows documentation, to know more about Windows Event Collector functionality. To configure the connector to collect forwarded events, see [Collecting Forwarded Events](#).

Configuring Windows

You must enable the appropriate auditing policies on Windows servers from which the connector collects information and also setup standard user accounts. This section has the following information:

Enabling Microsoft Windows Event Log Audit Policies

Because event information generated by Windows servers is based on the auditing policies that are enabled, make sure that appropriate auditing policies are enabled on Windows servers from which the connector collect information. By default, none of the Windows auditing features are enabled.

Auditing events consumes system resources such as memory, processing power, and disk space. Auditing an excessive number of events can dramatically slow down your servers.



Note: You must be logged on as an administrator or a member of the Administrators group to set up audit policies. If your computer is connected to a network, network policy settings might also prevent you from setting up audit policies.

The method used to create an audit policy varies depending on whether the policy is being created on a member server, a domain controller, or a stand-alone server.

- To configure a domain controller, member server, or workstation, use **Active Directory Users and Computers**.

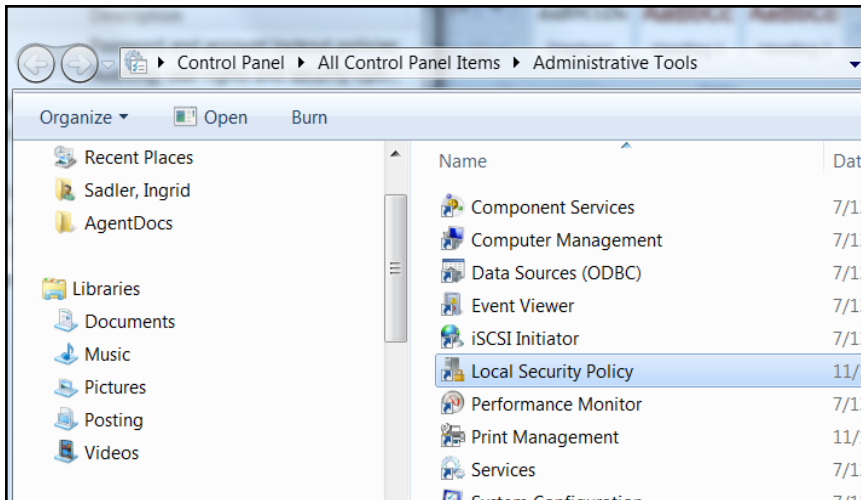
- To configure a system that does not participate in a domain, use **Local Security Settings**.

This section has the following information:

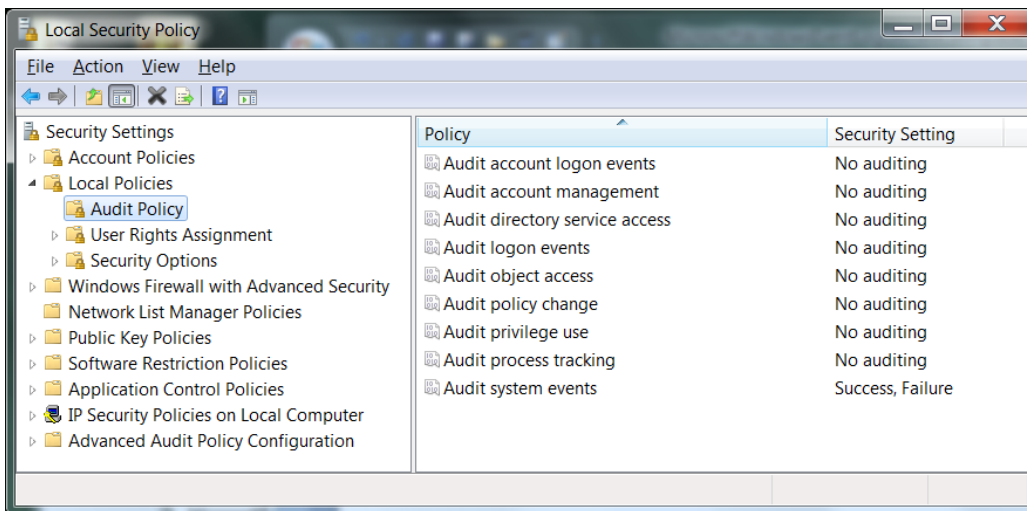
Enabling an Auditing Policy on a Local System

To establish an audit policy on a local system:

1. Select **Start > Control Panel > Administrative Tools > Local Security Policy**.

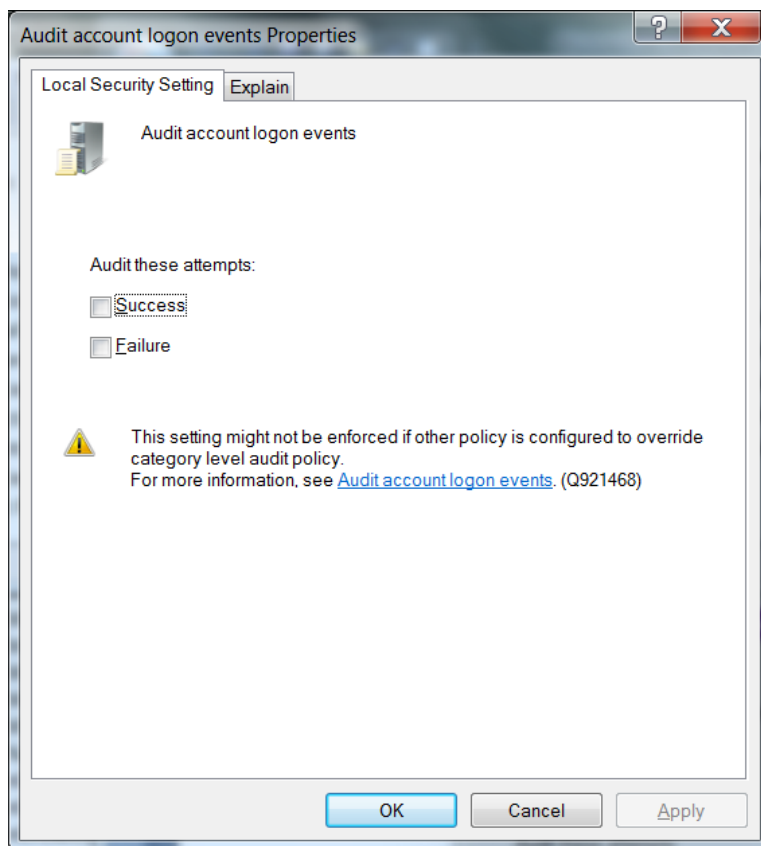


2. Double-click on **Local Policy** in the **Security Settings** tree to expand it.
3. Select **Audit Policy** from the tree. Doing so reveals the auditing information for that system.



4. To enable auditing for any of the areas, double-click on the type of audit. A dialog box similar to the following is displayed, letting you choose to perform a **Success** or a

Failure audit (or both) on that type of event.



Note: To audit objects such as the Registry, printers, files, or folders, select the Object Access option. Otherwise, when you attempt to enable auditing for these objects, an error is displayed instructing you to make the necessary adjustments to the local audit policy (or, in the case of a domain environment, to the domain audit policy).

After you have enabled auditing, go through the system and fine-tune the type of events that will be audited in each category.

Setting Up an Audit Policy Within a Domain

To set up an audit policy for a domain controller:

1. Choose **Start > Programs > Administrative Tools > Active Directory Users and Computers**.
2. Navigate through the console tree to the domain you want to work with. Expand the domain.
3. Beneath the domain, you will see a **Computers** object and a **Domain Controllers** object. Select the appropriate object for your system and right-click on **Domain**

Controllers. The Domain Controller's properties sheet is displayed.

4. Select the **Group Policy** tab. Select the group policy to which you want to apply the audit policy and click **Edit**.
5. Navigate through the tree to **Default Domain Controllers Policy > Computer Configuration > Windows Settings > Security Settings Local Policies > Audit Policy**.
6. When you select **Audit Policy**, a list of audit events is displayed in the right pane. To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable **Success**, **Failure**, or both audits for that group of events.

After enabling auditing for a group of events, fine-tune the exact events you want to audit.

Setting Up an Audit Policy for a Domain

To set up auditing for all computers under a domain:

1. Click **Start > Administrative Tools > Domain Security Policy**.
2. Open **Default Domain Security Settings**.
3. Expand **Security Settings** if it is not already open.
4. Expand **Local Policy** and double-click on **Audit Policy**. A list of audit events is displayed in the right pane.
5. To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable **Success**, **Failure**, or both audits for that group of events.

Setting Up Standard User Accounts

The connector does not require domain administrator privileges to collect Security events from Windows hosts. Event Log Reader privilege is required for system and custom application event collection including Forwarded Events Collection.

To configure the SmartConnector for Microsoft Windows Event Log – Native to use a Standard User account to collect Security events only from the target hosts, follow the steps provided in the following sections.

These steps describe how to configure and assign the privileges by creating a single user account such as **arcsight**. You can also create a group of users instead and follow the same steps provided for the configuration, assigning all the minimum privileges to the user group instead of the single user.



Note: Sometimes, although we have assigned appropriate privileges to the standard user, there could be other policies in your environment preventing the user account from accessing the security event logs. You can start identifying this problem by checking **Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security** options. There are many security policies defined that would require investigation; however, one policy to check right away is the **Network Access: Sharing and security model for local accounts**. Make sure this is set to **Classic – local users authenticate as themselves**.

Standard Domain User Account from Windows Server Domain Controllers

On the Windows Server Domain Controller:

1. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Users**.
2. Create a new **Domain User**, such as arcsight.
3. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Builtin**.
4. Open the properties of the security principal **Event Log Readers**.
5. From the **Members** tab, add the new Domain User arcsight to this security principal.
6. This Group Policy can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

```
GPUpdate /Force
```

This command will update any modifications you have made to any group policy, not just this one.

Standard Domain User Account from Domain Members

On the Windows Server Domain Controller:

1. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Users**.
2. Create a new Domain User, such as arcsight.

3. Go to **Settings > Control Panel > Administrative Tools > Group Policy Management > Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
4. Open the **Manage auditing and security log** policy.
5. Enable **Define these Policy Settings** and add this new Domain User arcsight to this policy.
6. This Group Policy can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

```
GPUpdate /Force
```



Note: This command will update modifications to any group policy you have made, not just this one

Standard Local User Account from Windows Workgroup Hosts

On the Windows Workgroup host:

1. Go to **Settings > Control Panel > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Users**.
2. Create a new **Local User**, such as arcsight.
3. Go to **Settings > Control Panel > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Groups**.
4. Open the **Event Log Readers** group and add this new Local User arcsight to this group.
5. Go to **Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**.
6. Open the **Network access: Sharing and security model** for local accounts policy.
7. Set this policy to the option: **Classic – local users authenticate as themselves**.

Add Security Certifications when Using SSL

If you choose to use SSL as the connection protocol, security certificates for both the Windows Domain Controller Service and for the Active Directory Server are required. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic.

The certificates will be imported to the connector's certificate store during the connector installation process. See **step 3** of the installation procedure for instructions.

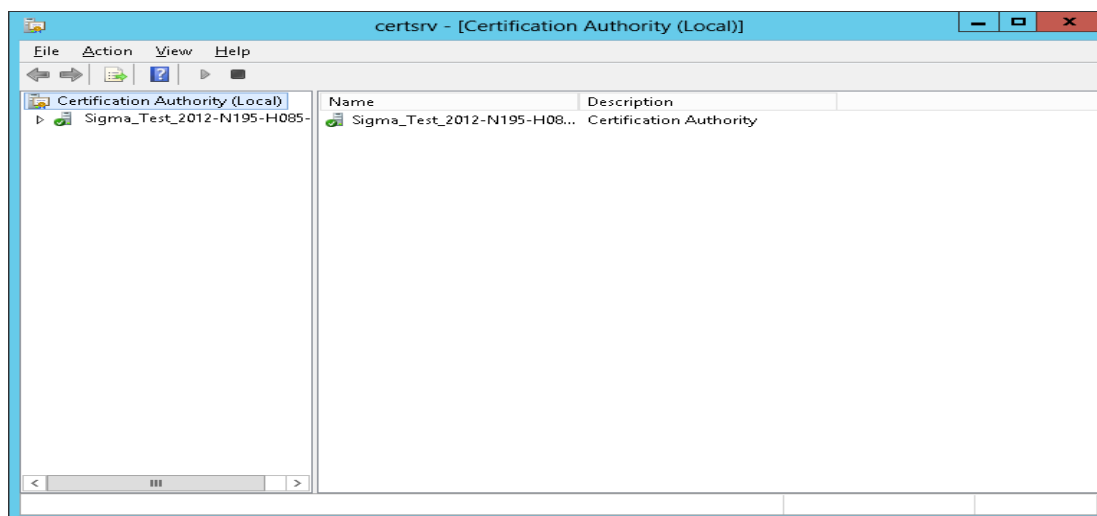
Procedures for Windows 2012 are shown; steps could vary with different Windows versions. For other Windows versions, see Microsoft's documentation for complete information.

Example: Windows Server 2012

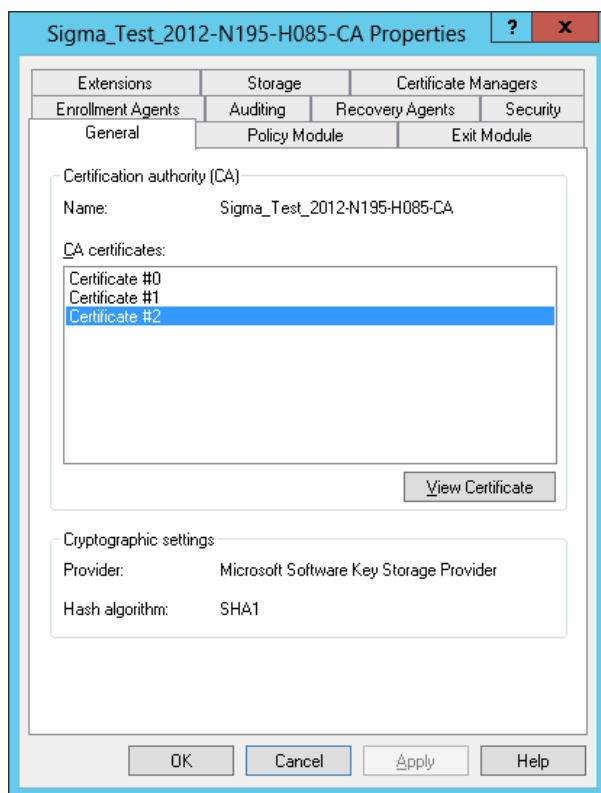
The following steps assume Windows Server 2012 as the operating system

To export the certificates:

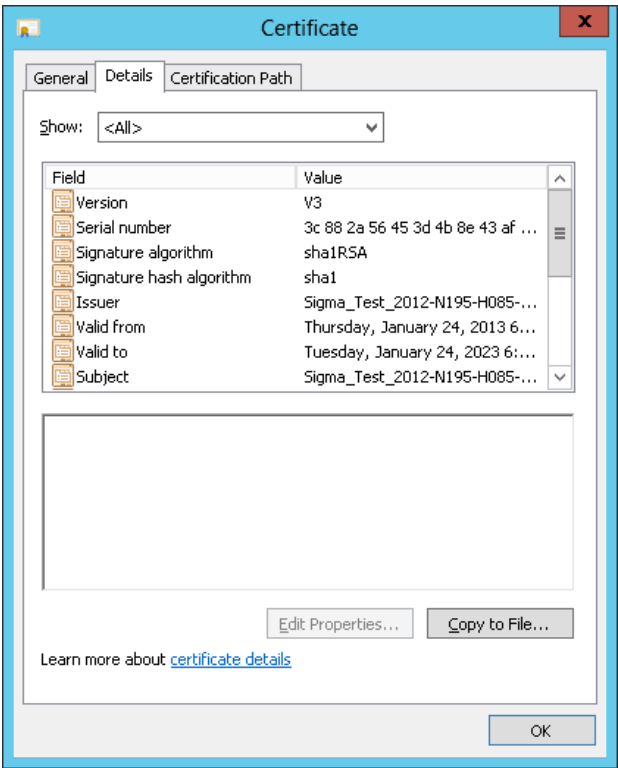
1. From the Windows **Start** menu, select **Administrative Tools**.
2. Select and double-click **Certification Authority**; one or more Domain Certificate Authority servers are shown.



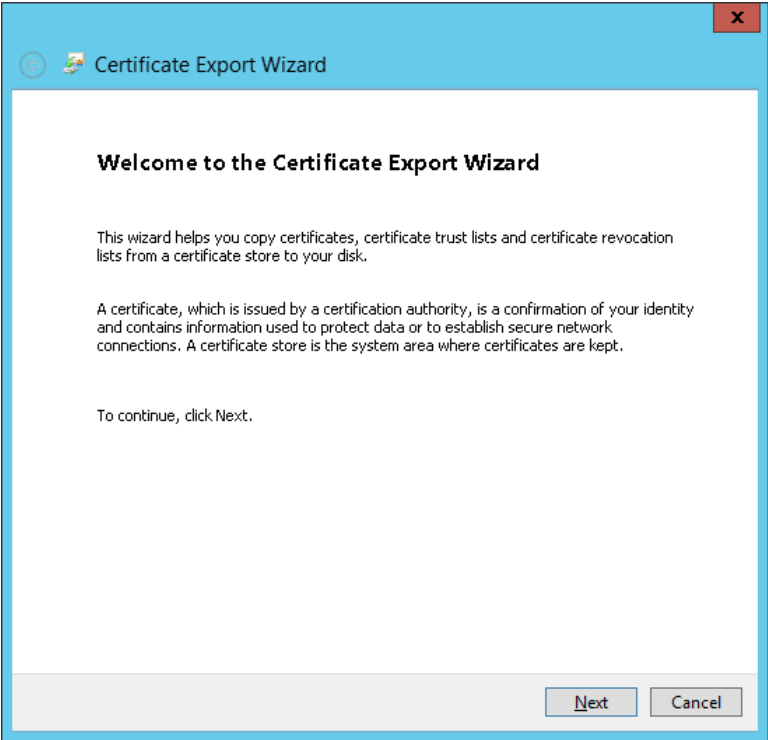
3. Select the Domain Certificate Authority server for the domain to which the Active Directory server belongs, right-click, and select **Properties** to open the **Properties** window.



4. Click **View Certificate**.
5. Click the **Details** tab, and **Copy to File...**



6. Follow the steps in the **Certificate Export Wizard** to complete the export.



Installing the SmartConnector

This section has the following information:

Installation Prerequisites

Supported Operating Systems for Installation

System Requirements

This connector can be installed on only one of the following supported Microsoft Windows 64-bit platforms:

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2 Standard
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)
- Microsoft Windows 10

.NET Requirements

- .NET 4.5.2, 4.6, 4.6.1 or 4.7.2.

Supported Operating Systems for Event Collection

ArcSight supports Windows Event Log Security, System, and Application event collection from hosts running the following Microsoft OS versions.

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)
- Microsoft Windows 10

It also supports events forwarded from source hosts to a Windows Event Collector (WEC).

Supported Log Parsers

The SmartConnector supports parsing for the following logs:

- Security
- System
- Application (event header)
- Forwarded Events (for forwarded security, system, and application (event Header) events)

Supported Applications

Parser support for the following application events is provided:

- Microsoft Active Directory
- Microsoft Exchange Access Auditing
- Microsoft SQL Server Audit
- Microsoft Local Administrator Password Solution (LAPS)
- Microsoft Windows Powershell
- Microsoft Windows BITS Client
- Microsoft Windows ESENT
- Oracle Audit
- Symantec Mail Security for Exchange

Supported System Events

Parser support for the following system events is provided:

- Microsoft Network Policy Server
- Microsoft Remote Access
- Microsoft Service Control Manager
- Microsoft WINS Server
- Microsoft Windows WindowsUpdateClient

Supported Events

Windows Event Log supports parsing for:

Event Type	Event Header	Event Description
Security	yes	yes
Application	yes	no*
System (Service Control Manager and WINS event sources)	yes	yes
Other System events (including Remote Access and NPS)	yes	no*
<p>* Support is provided for a Flex-Connector-like framework that lets you create and deploy your own parsers to parse the event description for all system and application events. See “Create and Deploy Parsers for System and Application Events” for more information. See “Log Parser Support” for application and system events already supported.</p>		

Use of Active Directory Query for Hosts

An Active Directory query can be used to populate or update collection end points, or specify the Windows OS version of source hosts for forwarded events if collected from the Windows Event Collector. The connector discovers and retrieves information about the hosts registered in an Active Directory. The host information includes the DNS name along with its operating system version. When new hosts are registered in an Active Directory while the connector is running, it sends an internal event notifying the user of the newly discovered host.

SmartConnector Setup Scenarios

The following examples describe some typical setup scenarios. For configuration details, see [“Configure the Connector”](#)

- **Scenario 1 - Collect Application, Security, and System Logs for the Local Host:** You select local host logs on the first configuration window with no remote hosts, no custom logs or event filters, and no Windows Event Forwarding configuration. Locale and encoding of the local host are automatically detected and configured by the connector; therefore, configuration of these values for the local host is not necessary.
- **Scenario 2 - Collect Application, Security, and System Logs from Remote Hosts, from One Domain, and Enter the Hosts Manually:** In this scenario, you can collect logs from remote hosts and add the host entries manually. You can either add a table parameter in the entry window that is displayed or import a csv file containing host information. However, when importing, make sure your local host is in the csv file if you intend to collect events from the local host, as the content from the imported file replaces the existing host information.
- **Scenario 3 - Collect Application, Security, and System logs from Hosts Recorded in Active Directory:** Collect logs from a host recorded in Active Directory. The table parameter entry window is then displayed, where you can make configuration selections for each host.
- **Scenario 4 - Collect Forwarded Events or Other WEC Logs from Local Or Remote Hosts:** With any of the previous scenarios, to collect Forwarded Events or other WEC logs from the local host (or remote hosts); a window is displayed where you can specify the name of a csv file containing the source hosts names and Windows OS versions for the hosts after making configuration selections for your hosts on the table parameter entry window.

Before you Begin

The following items are required when installing this SmartConnector :

- Local access to the machine where the SmartConnector will be installed.
- Administrator passwords to the machine.

Installation Notes

- Install this SmartConnector only on 64-bit Windows platforms. See [“Operating Systems Support for Event Collection.”](#)
- It is not possible to upgrade from the Microsoft Windows Event Log -- Unified connector to the Microsoft Windows Event Log -- Native connector.
- Parser overrides that exist for the Windows Event Log – Unified connector must be modified for use with the Windows Event Log – Native connector.
- If you use Forwarded Event Collection, the full computer name and OS version of source hosts must be available for use either through Active Directory or a source hosts file in csv format.

Enabling FIPS at the OS Level

1. From the Windows **Start** menu, select **Run**.
2. Enter `gpedit.msc`.
3. In the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
4. In the right pane, locate and click the “System cryptography: Use FIPS compliant5 algorithms for encryption, hashing, and signing” setting.
5. Set to **Enabled** and click **OK**.
6. Restart the computer.

Installing and Configuring the SmartConnector

For additional information about installing the SmartConnectors, see the [ArcSight SmartConnector Installation and User Guide](#).

To install and configure the Windows Event Log - Native SmartConnector:

1. Start the installation process.
2. Follow the instructions to add the required details to complete the installation of core software.
3. After the installation completes, to configure the connector, you can either click **Next** or run the `<ArcSightSmartConnectors_installDirectory>\current\bin\runagentsetup.bat` file.
4. Select the relevant [Global Parameters](#), then click **Next**.

5. From the **Type** drop-down, select **Microsoft Windows Event Log - Native** as the type of connector, then click **Next**.
6. In the **Configure Parameters** window, specify the following information:
 - a. Select logs for event collection:
 - The **Security log**, **System log**, and **Application log** options are selected by default. See “[Log Parser Support](#)” for a list of supported application and system events. For more information about the type of logs to select for different log sources, see [Selecting the Type of Logs for Event Collection](#).
 - **Custom Log**: Select this option to collect custom logs. For more information, see [Configuring Custom Logs and Filtering](#)
 - **ForwardedEvents Log**: If you select this option, you can collect events forwarded from a source host to any log type on the collector machine to which the connector has access.

Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types.
 - b. If you selected the **ForwardedEvents Log** option, the Windows OS version of the event source host is not populated automatically in the normalized events. To populate this value, you must either provide the Windows OS version or configure the Active Directory. If both Active Directory and Windows OS version is available from the source host file , then value from Active Directory takes precedence. Select any of the following options to specify the Windows OS version for the hosts from which you want to collect events:
 - **Use file for OS version**: Select this option to supply the name of the source hosts in a file. If you select this option, you will be prompted to specify the file details.
 - **Use Active Directory for OS version**: Select this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information. Newly discovered hosts are [added to the lookup automatically](#) without having to reconfigure the connector itself.

 For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it must be placed within the same forest as the Active Directory.

 If you select this option, you will be prompted to enter your domain credentials and Active Directory parameter information in the next screen.

- **Do not use any source for Windows OS version:** Select this option to not provide an Active Directory query or a CSV file to list all hosts involved in events forwarding along with their Windows OS version. If you select this option, no Windows OS version will be displayed in the event headers from the forwarding host.
- c. Select one or many of the following parameters to add hosts for event collection:
- **Use Common Domain Credentials:** Select this option to specify common domain credentials.
 - **Use Active Directory:** Select this option to use the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information.
 - **Enter Manually:** Select this option to manually specify all the host details.
7. Click **Next**.
8. One or more of the following screens will be displayed depending on your selections in the previous window:
- a. **WEF Source Hosts File Name:** If you selected **ForwardedEvents log** or **Use file for OS version** options in the previous window, then you are prompted to enter the name of the file that contains the source host information. This window is also displayed if you have selected **Is WEC** for any hosts in the table parameter window. For forwarded event collection, specify only the Event Collector hosts.
 - b. **Device Details Collection:** The first row displays selections from the initial parameter entry window for the local host. Click **Add** to manually add a host, or click **Import** to select a .csv file to import host information. Make sure that there is a carriage return (only one CR) at the last entry in the .csv file. Else the import fails.

If you have added hosts for which you decide not to collect events, you can use the checkbox in the leftmost column to deselect rows in the table.

Parameter	Description
Host Name	Host name or IP address of the target Windows host.
Domain Name	Name of the domain to which the host belongs. If you are using a Domain User account for a target host or using Active Directory, fill in the Domain Name field. This must be a name, not an IP address, for the OS version to be resolved.

Parameter	Description
User Name	Name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain.
Password	Password for the user specified in User Name .
Windows Version	Select the Microsoft Operating System version this host is running.
Is WEC	If you selected Indicates that this is a WEC server on the initial configuration page, this selection is already checked for the local host.
Security	Select for security events to be collected from this host. This log is automatically selected for all hosts.
System	Select for system events to be collected from this host.
Application	Select for application events to be collected from the Common Application Event Log of this host.
ForwardedEvents	Select for events to be collected from the ForwardedEvents log of this host.
Custom Event Logs	Specify the custom application log names, separated by a comma (such as "Exchange Auditing, Directory Service"). For Windows Event Collector servers, use HardwareEvents . See "Installing and Configuring the SmartConnector" on page 53 for more information.

Parameter	Description
Filter	This is a filter you can get from the Microsoft event viewer when you want to collect particular events. You can copy the filter text to this field. For more information, see “Configure a Filter.”
Locale	<p>Enter the value for your locale or accept the United States English default, en_US. Leave this field blank if you want the connector for the local host to automatically determine the correct Locale value.</p> <p>Values are:</p> <ul style="list-style-type: none"> ■ French Canadian: fr_CA ■ Japanese: ja_JP ■ Simplified Chinese: zh_CN ■ Traditional Chinese: zh_TW ■ United States English (the default): en_US <p>For localization of other languages, see “Customize Localization Support for the Native Connector” on page 39.</p>
Encoding	<p>Enter the encoding value for the language used to send localized log events, or accept the United States English default, en_US. This value cannot be determined automatically. Select from the following values:</p> <ul style="list-style-type: none"> ■ French Canadian: fr_CA ■ Japanese: Shift_JIS ■ Simplified Chinese: GB2312 ■ Traditional Chinese: zh_TW ■ United States English (the default): UTF-8 <p>For localization of other languages, see “Customize Localization Support for the Native Connector” on page 39.</p>

- c. **Domain Credentials:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:

**Note:**

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.

Parameter	Description
Domain Name	Enter the name of the domain to which the host belongs. Work group hosts and stand-alone hosts can be added manually on the table parameters entry window.
Domain User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Domain User Password	Enter the password for the user specified in the Domain User Name field.

- d. **Active Directory Parameters:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:

**Note:**

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.
- If GUID translation is enabled, then the Active Directory Domain and credentials are used. You must provide the complete domain name, including any qualifiers, such as .com.

Parameter	Description
Active Directory Domain	Enter the name of the Active Directory domain to which the host belongs.
Active Directory User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Active Directory User Password	Enter the password for the user specified in the Active Directory User Name field.
Active Directory Server	Enter the Active Directory Host Name or IP address required for authentication to the Microsoft Active Directory for the host browsing feature.

Parameter	Description
Active Directory Filter	<p>Enter the Active Directory Filter required for automatic host browsing to filter hosts by name, operating system, and creation time.</p> <p>The query can contain attributes for Common Names (cn), Operating System (operatingsystem) and Creation Time (whencreated) in 'YYMMDDHHmmSS' format, where YY=Last two digits of the year, MM=Month, DD=Date, HH=Hours, mm=Minutes, SS=Seconds in 24-hour format.</p> <p>The query can also contain wildcard characters (*) to match the attributes to different values.</p> <p>Active Directory Filter examples</p> <p>To create hosts after and inclusive of a particular time point, set filter to: <code>(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSSZ))</code></p> <p>To create hosts between and inclusive of two time points, set filter to: <code>(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSS)(whencreated<=YYMMDDHHmmSS))</code></p>
Active Directory Protocol	<p>Select whether the protocol to be used is non_ssl (the default value) or SSL. For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector.</p>

Parameter	Description
Use Active Directory host results for	<p>For WEF Only: If you selected “Use Active Directory for OSVersion” on the initial configuration window, the list of hosts retrieved from Active Directory is used to determine the Windows OS version for the WEF source hosts. When For WEF Only is selected, the result of the query will not populate the table of hosts on the table parameter entry window.</p> <p>For initial installation, Merge Hosts and Replace Hosts act the same because only the local host is present and preserved. If you selected Use Active Directory on the initial configuration screen under Parameters to add hosts for event collection, or you are modifying parameters to add hosts, the following applies.</p> <p>When Merge Hosts is selected, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding if WEC servers are present and Use file for OS is not selected on the initial configuration screen). The original host is not replaced and all other preconfigured hosts are preserved. Hosts are added from the list retrieved from Active Directory with Security events selected by default. If duplicates are found, the existing host entry is not overwritten.</p> <p>When Replace Hosts is chosen, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding when WEC servers are present and Use file for OS is not selected on the initial configuration screen). The local host is not replaced, but all other hosts preconfigured are replaced with those retrieved from Active Directory, with Security events selected by default.</p>

9. Select a destination, then configure the destination parameters.
10. Specify a name for the connector.
11. Select whether you want to run the connector as a service or in the standalone mode.
12. Complete the installation process.

Using SSL for Connection (optional)

If you are using SSL for connector connection, follow these steps.

To import the certificates to the connector’s certificate store, click **Cancel** to exit the wizard:

1. From \$ARCSIGHT_HOME\current\bin, execute the **keytool** application to import the two certificates (see “[Add Security Certifications when Using SSL](#)” earlier in this guide).

```
arcsight agent keytoolgui
```

The graphical interface asks you to open a keystore

2. Select `jre/lib/security/cacerts`, then select **import cert** to import your certificate. Verify that the correct certificate has been imported.
 3. When prompted **Trust this certificate?**, click **Yes**.
- Repeat this process for the second certificate.

4. Save the keystore.
5. Verify the imported certificates by entering this command from `$ARCSIGHT_HOME\current\bin`:

```
arcsight agent keytool -list -store clientcerts
```

The new certificates are listed.

6. Return to the configuration wizard by entering the following command from `$ARCSIGHT_HOME\current\bin`:

```
runagentsetup
```

Installing and Configuring Multiple Connector Instances

Follow these steps to install and run another instance of the connector on the source host.

1. Install the core connector software, then exit the wizard.
2. Go to the installation directory. For example:
`$ARCSIGHT_HOME\ArcSightSmartConnectors\current\`
3. From the `$ARCSIGHT_HOME\current\user\agent` directory, edit the `agent.properties` file.
4. Select a valid TCP port value for the `mq.server.listener.port` property. The value cannot be used by another instance of the connector. Range can be a value from 1 to 65535; the default value is 61616.
5. Add the parameter and value for the `mq.server.listener.port` property.
6. In the `$ARCSIGHT_HOME\current\user\agent\winc` directory, create a `config.ini` file with the following contents:

```
mq.server.hostname=localhost  
mq.protocol=tcp  
mq.server.port=<valid tcp port>
```

The `mq.server.port` value in this file should match the one configured in `agent.properties`.

7. Launch the setup wizard by running **runagentsetup** from the `$ARCSIGHT_HOME\current\bin` directory.

Notes:

- When running the configuration wizard, the following warning message might be logged as the event listener starts to send the heartbeat before it is assigned to `RemoteAgentId`:

```
[updateHeartbeat]RemoteAgentId unspecified. Ignoring the heartbeat.
```

- The connector *will not run* if the value of `mq.server.port` is not unique for each instance of the Native Windows Event Log installed on the same box. It will indicate that the port is already in use.
- Resource consumption increases as the number of connector instances increase, so this constraint may limit the number of instances you use in your enterprise.

Log sources and Event Mappings

This section provides information about the following supported log sources and Event Mappings to ArcSight fields:

Microsoft ADFS

Active Directory Federation Service (ADFS) is a software component in Windows Server 2012, Windows Server 2016, and Windows Server 2019. It contains Active Directory, Federation Server, Federation Server Proxy, and ADFS Web Server.

ADFS provides the following services:

- **Single Sign-On (SSO):** ADFS provides SSO authorization to users who want to access applications in different networks or organizations. It provides SSO access to internet-facing applications or services.

- **Identity Federation (Identity Management):** This provides the digital identity to the users and allows to centralize it. This helps to maintain security and rights across security and enterprise boundaries.

Supported Versions

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides main mappings for the Windows Event Log SmartConnectors. The field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft ADFS Logs

For information about configuring Microsoft ADFS events logs, see <https://adfshelp.microsoft.com/AdfsEventViewer/GetAdfsEventList> in the Microsoft TechNet Library.

Event Mappings for Microsoft ADFS

General

ArcSight Field	Vendor Field
Device Product	'ADFS Auditing'
Device Vendor	'Microsoft'

Event 299

ArcSight Field	Vendor Field
Destination DNS Domain	%3 (Relying Party)
Device Custom String 1	%2 (Activity ID)
Device Custom String 1 Label	"Activity ID"

ArcSight Field	Vendor Field
Device Custom String 4	%1 (Instance ID)
Device Custom String 4 Label	"Instance ID"
Message	__concatenate("A token was successfully issued for the relying party", %3)
Name	"A token was successfully issued for relying party"

Event 300

ArcSight Field	Vendor Field
Device Custom String 1	%1 (Activity ID)
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%2 (Request type)
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%3 (Exception details)
Device Custom String 6 Label	"Exception details"
Message	"The Federation Service failed to issue a token as a result of an error during processing of the WS-Trust request"
Name	"Federation Service failed to issue a token as a result of an error"
Source Nt Domain	__extractNTDomain(%3)
Source User Name	__extractNTUser(%3)

Event 307

ArcSight Field	Vendor Field
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Name	"Federation service configuration was changed"
Source Nt Domain	__extractNTDomain(%3)
Source User Name	__extractNTUser(%3)

Event 403

ArcSight Field	Vendor Field
Destination Address	%9 (Local IP)
Destination Dns Domain	%14
Destination Port	%8 (Local Port)
Device Custom Date 1	%3
Device Custom Date 1 Label	"Request Time"
Device Custom Number 1	%11
Device Custom Number 1 Label	"Content Length"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%16
Device Custom String 6 Label	"Proxy DNS name"
End Time	%3
Name	"An HTTP request was received"
Old File Hash	__concatenate("Through Proxy:",%15)
Old File Id	__concatenate("Caller Identity:",%12)
Old File Type	__concatenate("Certificate Identity:",%13)
Request Client Application	%10 (User Agent)
Request Method	%5 (HTTP Method)
Request Url File Name	%6 (Url Absolute Path)
Request Url Query	%7 (Query string)
Source Address	%4
Start Time	%3

Event 404

ArcSight Field	Vendor Field
Device Custom Date 1	%3
Device Custom Date 1 Label	"Response Time"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 5	%5
Device Custom String 5 Label	"Status Description"
End Time	%3
Event Outcome	%4
Name	"An HTTP response was dispatched"

Event 405

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	__concatenate("Password change succeeded for following user: ",%2)
Name	"Password change succeeded"
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 406 - Windows Server 2016

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	__concatenate("Password change failed for following user:",%2)
Name	"Password change failed"
Reason	%4
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 406 - Windows Server 2019

ArcSight Field	Vendor Field
Destination Host Name	%4
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%3
Device Custom String 4 Label	"Device Certificate"
Message	__concatenate("Password change failed for following user:",%2)
Name	"Password change failed"
Reason	%5
Source Address	%6
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 410

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%3
Device Custom String 4 Label	"Client Application"
Device Custom String 5	%13
Device Custom String 5 Label	"Proxy"
Device Custom String 6	%11
Device Custom String 6 Label	"Forwarded Client IP"
Name	"Following request context headers present"
Old File Id	__concatenate(%6,":",%7)
Request Client Application	%5
Request Url File Name	%9
Source Address	%15
Source Translated Address	__regexToken(%11)

Event 411

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%2
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%3
Device Custom String 5 Label	"Error message"
Device Custom String 6	%4
Device Custom String 6 Label	"Exception details"
Name	"Token validation failed"

ArcSight Field	Vendor Field
Reason	__regexToken(%3)
Request Url	%2
Source Address	%5
Source User Name	__regexToken(%3)

Event 412

ArcSight Field	Vendor Field
Destination Dns Domain	%4
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%3
Device Custom String 6 Label	"Token type"
Message	__concatenate("A token of type ",%3," for relying party ",%4," was successfully authenticated")
Name	"A token for relying party was successfully authenticated"

Event 413

ArcSight Field	Vendor Field
Destination Dns Domain	%5
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"An error occurred during processing of a token request"
Old File Hash	__concatenate("Caller:",%2)
Old File Id	__concatenate("Device identity:",%6)
Old File Name	__concatenate("Act as User:",%4)
Source Address	%7
Source User Name	__extractNTUser(%3)

Event 418

ArcSight Field	Vendor Field
File Hash	%4
File Name	%2
Name	"Trust between federation server proxy and service was successfully renewed"
Old File Hash	%3
Source Address	%1

Event 420

ArcSight Field	Vendor Field
File Hash	%4
File Name	%3
Name	"Trust between federation server proxy and service was successfully established"
Source Address	%2
Source User Name	__extractNTUser(%1)
Source Nt Domain	__extractNTDomain(%1)

Event 424

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%5
Device Custom String 6 Label	"Inner exception"
File Hash	%2

ArcSight Field	Vendor Field
File Name	%3
Name	"The federation server proxy was not able to authenticate the client certificate presented in the request"
Source Address	%4

Event 431

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%5
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%4
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%6
Device Custom String 6 Label	"Signature Algorithm"
File Size	%2
File Type	%3
Name	"An active request was received at STS with RST"

Event 512

ArcSight Field	Vendor Field
Device Custom Date 1	__concatenate(%5,"",%6)
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"

ArcSight Field	Vendor Field
Message	__concatenate("The account for the following user ",%2," is locked out. A login attempt is being allowed due to the system configuration")
Name	"The account for the following user is locked out"
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 513

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%4
Device Custom String 6 Label	"Exception details"
Name	"The Artifact REST service failed to return an artifact as a result of an error during processing"
Request Url	%3
Source Address	%2

Event 515

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Event Outcome	"This account may be compromised"
Message	__concatenate("The following user ",%2," account was in a locked out state and the correct password was just provided. This account may be compromised")
Name	"The following user account was in a locked out state and the correct password was just provided"

ArcSight Field	Vendor Field
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 516

ArcSight Field	Vendor Field
Device Custom Date 1	__concatenate(%5," ",%6)
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"The following user account has been locked out due to too many bad password attempts"
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 1102

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%4
Device Custom String 5 Label	"Additional details"
Name	"The Federation Service authorized a request to one of the REST endpoints"
Request Url	%3
Source Address	%2

Event 1200

ArcSight Field	Vendor Field
Name	"The Federation Service issued a valid token"

Event 1201

ArcSight Field	Vendor Field
Name	"The Federation Service failed to issue a valid token"

Event 1202

ArcSight Field	Vendor Field
Name	"The Federation Service validated a new credential"

Event 1203

ArcSight Field	Vendor Field
Name	"The Federation Service failed to validate a new credential"

Event 1204

ArcSight Field	Vendor Field
Name	"A password was changed"

Event 1205

ArcSight Field	Vendor Field
Name	"A password change was attempted, but failed"

Event 1206

ArcSight Field	Vendor Field
Name	"A Sign Out request was successfully processed"

Event 1210

ArcSight Field	Vendor Field
Name	"An extranet lockout event has occurred"

Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210

ArcSight Field	Vendor Field
Application Protocol	AuthProtocol
Destination Dns Domain	RelyingParty
Destination Host Name	__regexToken(Server)
Destination Service Name	__regexToken(Server)
Device Custom Date 1	LastBadAttempt
Device Custom Date 1 Label	"Last Bad Attempt"
Device Custom Number 1	__oneOfLong(CurrentBadPasswordCount)
Device Custom Number 1 Label	"Current Bad Password Count"
Device Custom Number 2	__oneOfLong(ConfigBadPasswordCount)
Device Custom Number 2 Label	"Config Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	ForwardedIpAddress
Device Custom String 5 Label	"Forwarded Ip Address"
Device Custom String 6	AuditType
Device Custom String 6 Label	"Audit Type"
Device Domain	NetworkLocation
Device External Id	DeviceId
Device Process Name	ClaimsProvider
Event Outcome	AuditResult

ArcSight Field	Vendor Field
Old File Hash	__concatenate("SSO Binding Validation Level:",SSOBindingValidationLevel)
Old File Name	__concatenate("Device Auth:",DeviceAuth)
Old File Path	__concatenate("Primary Auth:",PrimaryAuth)
Old File Type	__concatenate("Failure Type:",FailureType)
Reason	ErrorCode
Request Client Application	UserAgentString
Source Address	IpAddress
Source Nt Domain	__extractNTDomain(UserId)
Source Translated Address	__regexToken(ForwardedIpAddress)
Source User Name	__extractNTUser(UserId)

Active Directory

Active Directory, an essential component of the Windows architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory lets organizations centrally manage and share information on network resources and users while acting as the central authority for network security.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this section are specifically for the SmartConnector for Microsoft Active Directory Windows Event Log – Native: Active Directory.

Audit Active Directory Objects in Windows

When you use Windows auditing, you can track both user activities and Windows activities. When you use auditing, you can specify which events are written to the Security log. For example, the Security log can maintain a record of both valid and invalid logon attempts and events that relate to creating, opening, or deleting files or other objects.

When you audit Active Directory events, Windows writes an event to the Security log on the domain controller. For example, if a user attempts to log on to the domain using a domain user account and the logon attempt is unsuccessful, the event is recorded on the domain controller and not on the computer on which the logon attempt was made. This is because it is the domain controller that attempted to authenticate the logon attempt but could not do so.


To enable auditing of Active Directory objects:

1. Configure an audit policy setting for a domain controller. (When you configure an audit policy setting, you can audit objects, but you cannot specify which object you want to audit.)
2. Configure auditing for specific Active Directory Objects. After you specify the events to audit for files, folders, printers, and Active Directory Objects, Windows tracks and logs these events.

Configure an Audit Policy Setting for a Domain Controller

Auditing is turned off by default. For domain controllers, an audit policy setting is configured for all domain controllers in the domain. To audit events that occur on domain controllers, configure an audit policy setting that applies to all domain controllers in a non-Local Group Policy object (GPO) for the domain. You can access this policy setting through the Domain Controller's organizational unit. To audit user access to Active Directory objects, configure the Audit Directory Service Access event category in the audit policy setting.

The computer on which you want to configure an audit policy setting must be granted the Manage Auditing and Security Log user right. By default, Windows grants these rights to the Administrators group.

 The files and folders you want to audit must be on Microsoft Windows NT file system (NTFS) volumes.

To configure an audit policy setting for a domain controller (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. From the **View** menu, click **Advanced Features**.
3. Right-click **Domain Controllers**; then click **Properties**.
4. Click the **Group Policy** tab, click **Default Domain Controller Policy**, and then click **Edit**.
5. Click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **Audit Policy**.
6. In the right pane, right-click **Audit Directory Services Access**, and then click **Security**.
7. Click **Define These Policy Settings**, then click to select one or both of the following check boxes:
Success: Click to audit successful attempts for the event category
Failure: Click to audit failed attempts for the event category
8. Right-click any other event category that you want to audit; then click **Security**.
9. Click **OK**.
10. Because the changes you make to your computer's audit policy setting takes affect only when the policy setting is propagated (or applied) to your computer, to initiate policy propagation, either enter `secedit/refreshpolicy machine_policy` at the command prompt and then restart the computer or wait for automatic policy propagation, which occurs at regular intervals you can configure. By default policy propagation occurs every eight hours.

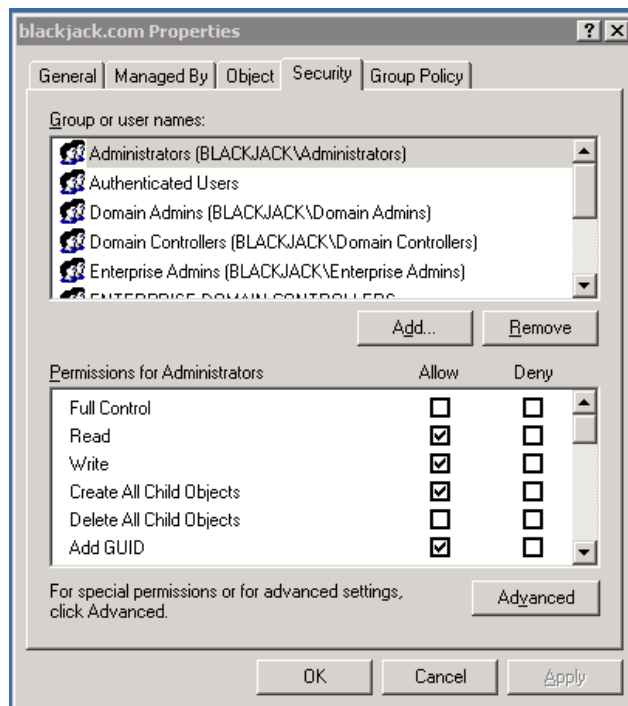
Configure Auditing for Specific Active Directory Objects

After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

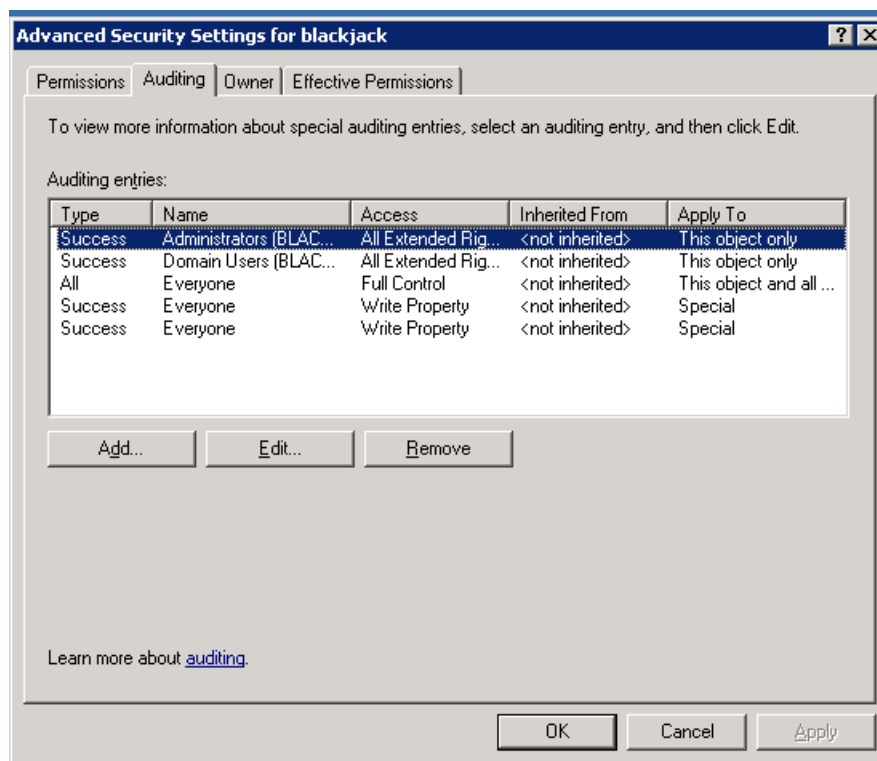
To configure auditing for specific Active Directory objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.

2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Active Directory object you want to audit (blackjack.com in the example) and select **Properties**.



4. Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



5. To add an object, click **Add**.
6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Active Directory Event Mappings

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

NTDS Database Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Microsoft Active Directory Domain services version)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 NTDS Database Mappings

General

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain services version

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Microsoft Active Directory Domain services version)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)

ArcSight Field	Vendor Field
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5, '\', %6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

ArcSight Field	Vendor Field
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5, '\', %6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

ArcSight Field	Vendor Field
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5,',',%6,',',%7,',',%8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7 (Time Seen)
Device Custom String 4	%5 (Processing Stats)
Device Custom String 5	%6 (Most Frequent Record Type)

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,',';%6,',';%7,',';%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

Windows 2008 NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5,',';%6,',';%7,',';%8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7
Device Custom String 4	%5
Device Custom String 5	%6

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,',';%6,',';%7,',';%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)

ArcSight Field	Vendor Field
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS LDAP Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

ArcSight Field	Vendor Field
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5, '\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\','%6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Windows 2008 NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5,'\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5, '\', %6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS LDAP Mappings

1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	%3 (Reason or Error Code)

1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	Both ('Internal event:Function', %1, ' entered')

1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	Both ('Internal event:Function', %1, ' exited')

1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	%1 (Source address)
Reason	%3 (Reason or Error Code)
Device Custom String 5	Internal ID

1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'

ArcSight Field	Vendor Field
Device Custom Number 3	Attempts
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'
Source Address	%1 (Source address)

1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	Both ('The LDAP server returned an error value:',%1)
Reason	%1 (Reason or Error Code)

1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	%1 (Host name)
Reason	%2 (Reason or Error Code)

1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	%1 (Host name)
Device Custom String 5	Site

2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	%2 (Host name)

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2089

ArcSight Field	Vendor Field
Name	'This directory partition has not been backed up'
Message	'This directory partition has not been backed up since at least the following number of days'
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	'Registry Key'
File Name	All of (%3,'\\',%4)

2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher.'
Device Custom Number 1	number of simple binds performed without SSL/TLS
Device Custom Number 2	number of negotiate/Kerberos/NTLM/Digest binds performed without signing

2889

ArcSight Field	Vendor Field
Name	'LDAP bind without requesting signing or performed a simple bind'
Message	'The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection'
Source User Name	%2 (User name)
Source Address	%1 (Source address)

Windows 2012/Windows 8 NTDS LDAP Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	%3 (Reason or Error Code)

1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	Both ('Internal event:Function', %1, ' entered')

1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	Both ('Internal event:Function', %1, ' exited')

1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	%1 (Source address)
Reason	%3 (Reason or Error Code)
Device Custom String 5	Internal ID

1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'
Device Custom Number 3	Attempts
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'
Source Address	%1 (Source address)

1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	Both ('The LDAP server returned an error value:',%1)
Reason	%1 (Reason or Error Code)

1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	%1 (Host name)
Reason	%2 (Reason or Error Code)

1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	%1 (Host name)
Device Custom String 5	Site

2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

2089

ArcSight Field	Vendor Field
Name	'This directory partition has not been backed up'
Message	'This directory partition has not been backed up since at least the following number of days'
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	'Registry Key'
File Name	All of (%3,'\\',%4)

2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher.'
Device Custom Number 1	number of simple binds performed without SSL/TLS
Device Custom Number 2	number of negotiate/Kerberos/NTLM/Digest binds performed without signing

2889

ArcSight Field	Vendor Field
Name	'LDAP bind without requesting signing or performed a simple bind'
Message	'The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection'
Source User Name	%2 (User name)
Source Address	%1 (Source address)

Local Administrator Password Solution

MS Local Administrator Password Solution is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Local Administrator Password Solution

Configuring MS Local Administrator Password Solution

For complete information about Microsoft's Reporting and MS Local Administrator Password Solution, see "Remote Access (DirectAccess, Routing and Remote Access)" topic in the TechNet Library for Windows Server:

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Microsoft Local Administrator Password Solution

Event 5

ArcSight Field	Vendor Field
Name	__ifThenElse(%1, "Validation passed for new local admin password", "Validation failed for new local admin password against local password policy")
Message	__ifThenElse(%1, "Validation passed for new local admin password", "Validation failed for new local admin password against local password policy")
Reason	%1

Event 10

ArcSight Field	Vendor Field
Name	__stringConstant("Password expiration too long for computer")
Message	__stringConstant("Password expiration too long for computer")
Device Action	__stringConstant("Resetting password now")
Device Custom Number 1	__safeToLong(%1)
Device Custom String1 Label	Excessive Days
Device Custom String2 Label	Days to change password

Event 11

ArcSight Field	Vendor Field
Name	__stringConstant("It is not necessary to change password yet")
Message	__stringConstant("It is not necessary to change password yet")
Device Custom Number 2	__safeToLong(%1)

Event 12

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been changed")
Message	__stringConstant("Local Administrator password has been changed")

Event 13

ArcSight Field	Vendor Field
Name	__stringConstant("Local Administrator password has been reported to AD")
Message	__stringConstant("Local Administrator password has been reported to AD")

Event 14

ArcSight Field	Vendor Field
Name	__stringConstant("Finished Successfully")
Message	__stringConstant("Finished Successfully")

Event 15

ArcSight Field	Vendor Field
Name	__stringConstant("Beginning Processing")
Message	__stringConstant("Beginning Processing")

Event 16

ArcSight Field	Vendor Field
Name	__stringConstant("Admin account management not enabled")
Message	__stringConstant("Admin account management not enabled")
Device Action	__stringConstant("Exiting")

Microsoft Antimalware Logs

Microsoft Antimalware is a network service in Windows Server 2012, Windows Server 2012 R2 and Windows Server 2016.

Microsoft Antimalware is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system.

The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

This section provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft antimalware and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this section are specifically for Microsoft Antimalware.

Mappings for Antimalware

Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain

ArcSight Field	Vendor Field
Source User Name	User
Sid	SID
File Path	Scan resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom Number 1	Scan Time Hours
Device Custom Number 2	Scan Time Minutes
Device Custom Number 3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1005

ArcSight Field	Vendor Field
Device Custom String 1 Label	Scan ID
Device Custom String 1	Scan ID
Device Custom String 5	Error Code
Device Custom String 5 Label	Error Code
Device Event Category	Scan Type
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Reason	Error Code

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom String 1	Threat Name
Device Custom Number 1	Threat ID
Device Custom Number 2	Severity ID
Device Custom Number 3	Category ID
FWLink	FWLink
File Path	Path
Device Severity	Severity Name
Device Custom String 4	Category Name
Device Custom String2	Signature Version
(Concatenating both the fields)	Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Detection ID
Device Custom Date 1	Detection Time
Device Custom Number 1	Threat ID
Device Custom String 1	Threat Name
Device Custom Number 2	Severity ID
Device Custom String 3	Severity Name
Device Custom Number 3	Category ID
Device Custom String 4	Category Name
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID

ArcSight Field	Vendor Field
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2)	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2)	Engine Version

Event 1117

ArcSight Field	Vendor Field
Product Version	Device Version
Detection ID	Device Custom String 5
Detection Time	Device Custom Date 1
Threat ID	Device Custom Number 1
Threat Name	Device Custom String 1
Severity ID	Device Custom Number 2
Severity Name	Device Custom String 3

ArcSight Field	Vendor Field
Category ID	Device Custom Number 3
Category Name	Device Custom String 4
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action Name	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String

ArcSight Field	Vendor Field
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1150

ArcSight Field	Vendor Field
Device Version	Product Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 2000

ArcSight Field	Vendor Field
Device Venison	Product Version
File Id	Current Signature Version
Old File Id	Previous Signature Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index

ArcSight Field	Vendor Field
Device Custom String 6	Update Type
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Current Engine Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Previous Engine Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom String 5	Error Code
Reason	Error Description
File Path	FWLink

Event 2002

ArcSight Field	Vendor Field
Product Verison	Device Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Previous Engine Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Current Engine Version
Source Nt Domain	Domain
Source User Name	User

ArcSight Field	Vendor Field
Sid	SID
Feature Index	Feature Index
Feature Name	Feature Index Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path

ArcSight Field	Vendor Field
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Error Code
Reason	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
File Id	Feature ID
Device Custom Number 1	Configuration
Device Custom Number 1 Label	Configuration

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	New Value

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

Microsoft Windows Defender AntiVirus

Microsoft Windows Defender AntiVirus is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

This section provides information about configuring Microsoft Windows Defender AntiVirus as a log source and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Microsoft Windows Defender AntiVirus

For complete information about Microsoft's Reporting and Microsoft Windows Defender AntiVirus, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Microsoft Windows Defender AntiVirus

Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
File Path	Scan Resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Hours"
Device Custom Number1	Scan Time Hours
Device Custom Number2 Label	"Minutes"
Device Custom Number2	Scan Time Minutes
Device Custom Number3 Label	"Seconds"
Device Custom Number3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String1 Label	"Scan ID"
Device Custom String1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameter

ArcSight Field	Vendor Field
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

Event 1009

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
FWLink	FWLink
File Path	Path
Old File ID	Severity Name
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Device Custom String2Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1 Label	"Action Time"
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID

Event 1015

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
FWLink	FWLink
Source Process Name	Process Name
File Path	Path Found
Request Context	Detection Origin
Old File Type	Detection Type
Source Service Name	Detection Source

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User

ArcSight Field	Vendor Field
Origin ID	Origin ID
Request Context	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

Event 1117

ArcSight Field	Vendor Field
Device Version	Product Version
Start Time	Detection Time
Device Custom Number1 Label	"Threat ID"
Device Custom Number1	Threat ID
Device Custom Number2 Label	"Severity ID"
Device Custom Number2	Severity ID
Device Custom Number3 Label	"Category ID"
Device Custom Number3	Category ID
Device Custom String6 Label	"Detection ID"
Device Custom String6	Detection ID
Device Custom String1 Label	"Threat Name"

ArcSight Field	Vendor Field
Device Custom String1	Threat Name
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String4 Label	"Category Name"
Device Custom String4	Category Name
Old File ID	Severity Name
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
FWLink	FWLink
File Path	Path
Request context	Detection Origin
Source Service Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
Origin ID	Origin ID
Request Context	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description

ArcSight Field	Vendor Field
Post Clean Status	Post Clean Status
Additional Actions ID	Additional Actions ID
Remediation User	Remediation User

Event 1150

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version

Event 1151

ArcSight Field	Vendor Field
Device Version	Platform Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String2	Signature Version,Engine Version
Device Custom String1 Label	"RTP State/ OA State/ IOAV State/ BM State"
Device Custom String 1	RTP State/ OA State/ IOAV State/ BM State
Device Custom Number1	safeToLong(updateRevisionNumber)
Device Custom Number1 Label	"Last AV Signature Age"
Device Custom Number1	AV signature age
Device Custom Number2 Label	"Last AS Signature Age"
Device Custom Number2	AS signature age
Device Custom Number3 Label	"Last quick scan age"
Device Custom Number3	Last quick scan age
Device Floating Point1 Label	"Last full scan age"
Device Floating Point1	Last full scan age
File Create Time	AV signature creation time
Old File Create Time	AS signature creation time
Start Time	Last quick scan start time

ArcSight Field	Vendor Field
End Time	Last quick scan end time
Device Custom String4 Label	"Last Quick Scan Source"
Device Custom String4	Last quick scan source
Device Custom Date1 Label	"Last full scan start time"
Device Custom Date1	Last full scan start time
Device Custom Date2 Label	"Last full scan end time"
Device Custom Date2	Last full scan end time
Device Custom String6 Label	"Last full scan source"
Device Custom String6	Last full scan source
Product status	Product status

Event 2000

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String6 Label	"Update Type"
Device Custom String6	Update Type
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description
File Path	Source Path

Event 2002

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Device Custom String2 Label	"Current/ Previous Engine Version"
Device Custom String2	Current Engine Version, Previous Engine Version
Feature Index	Feature Index
Device Event Category	Feature Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Source User ID	SID
Signature Type Index	Signature Type Index
Device Event Category	Signature Type

ArcSight Field	Vendor Field
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String1	Dynamic Signature Version
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom Date1	Dynamic Signature Compilation Timestamp
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 2030

ArcSight Field	Vendor Field
Device Version	Product Version

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
File ID	Feature ID
File Hash	Feature Name
Reason	Error Code
Device Custom String5 Label	"Error Description"
Device Custom String5	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
Device Custom Number	"Configuration"
Device Custom Number1 Label	Configuration
File ID	Feature ID

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	"New Value"

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

Microsoft DNS Server Analytics

Microsoft DNS Server Analytic Logs is a Windows system service and device driver that enables the Microsoft Windows Event Log – Native (WiNC) SmartConnector to monitor and collect the analytic events / logs from the DNS Server.

It provides information about operational events such as dynamic updates, zone transfers, and DNSSEC zone signing and unsigning.

This section provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft DNS Server Analytic Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Configuring Microsoft DNS Server Analytic Logs

For information about configuring Microsoft DNS Logging and Microsoft DNS analytic events logs, see Microsofts [DNS Logging and Diagnostics](#).

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)

ArcSight Field	Vendor Field
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port '%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user '%3,' connected on port '%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user 'One of (%2,%3),' has connected and has been successfully authenticated on port 'One of (%3,%4)','. Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)

ArcSight Field	Vendor Field
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user '%2,' connected on port '%3,' on '%4,' at '%5,' and disconnected on '%6,' at '%7,'. The user was active for '%8,' minutes, '%9,' seconds, '%10,' bytes were sent and '%11,' bytes were received. The reason for disconnecting was '%12,'. The tunnel used was '%13,'. The quarantine state was '%14,','')

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user '%2,' connected on port '%3,' has been assigned address '%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source Address	%2 (Address)
Message	Both ('The user with ip address '%2,' has disconnected')

Microsoft Exchange Mailbox Access Auditing

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions. Microsoft Exchange 2007 Service Pack 2 is supported by this SmartConnector.

This section provides information about the SmartConnector for Microsoft Exchange Access Auditing Windows Event Log Native and its event mappings to ArcSight data fields. This connector supports Microsoft Exchange Server 2007 and 2007 SP3 audit application events for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 versions.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

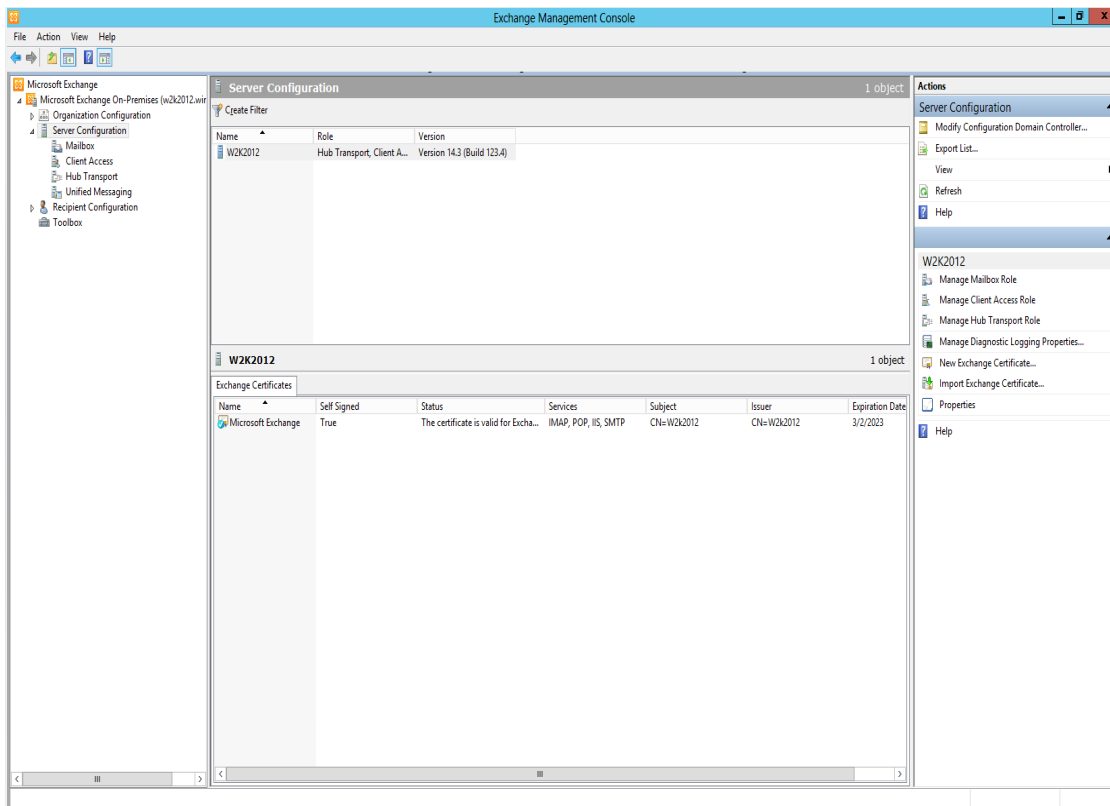
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Exchange Audit.

Configuring Mailbox Access Auditing

Use the Exchange Management Console to access the configuration area for mailbox access auditing.

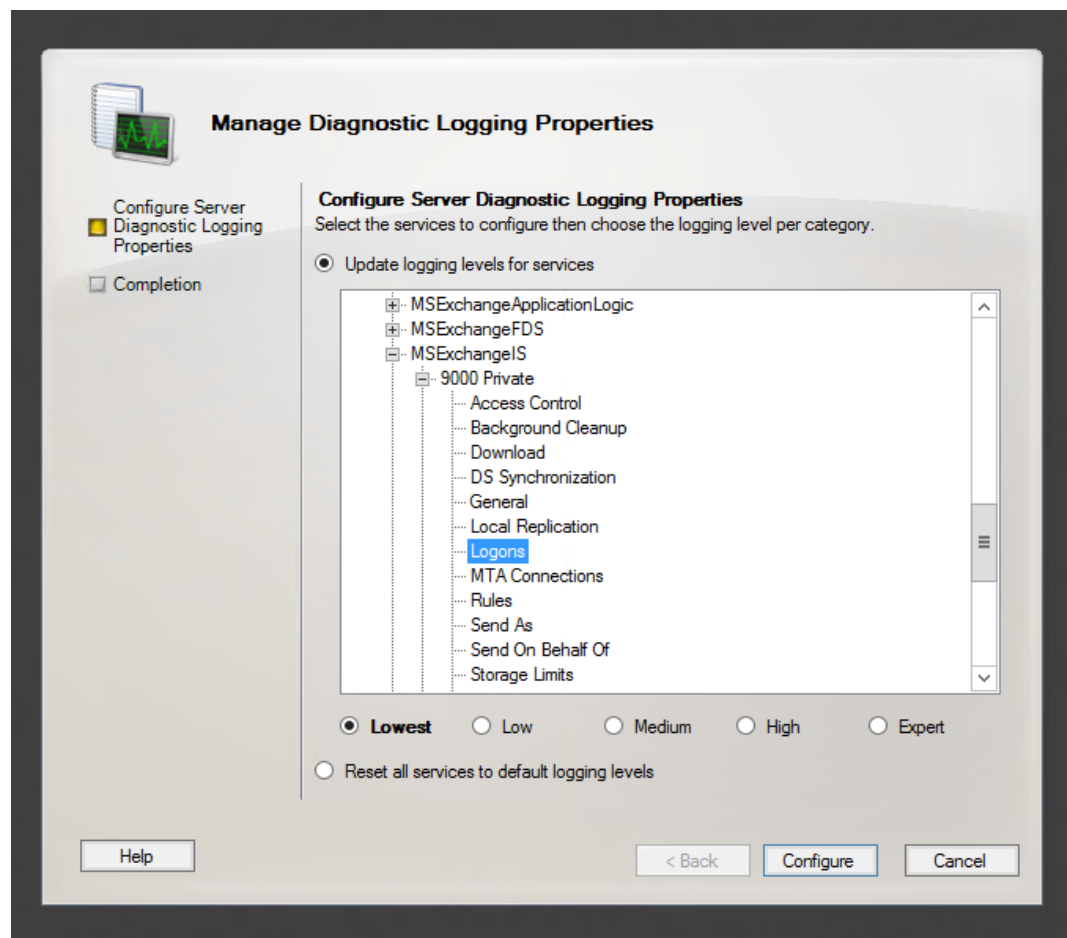
Enabling Mailbox Access Auditing

The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox access auditing on a particular mailbox server:

1. Select that server in the Exchange Management Console and then select the **Manage Diagnostics Logging Properties** menu option from the action pane; the **Manage Diagnostics Logging Properties** window is displayed.



2. Expand the **MExchangeIS** category and then expand the **9000 Private** category.
3. Under the **MExchangeIS\9000 Private** category, configure auditing for any or all of the four possible actions:
 - Folder Access, to log events that correspond to opening folders, such as the Inbox, Outbox, or Sent Items folders
 - Message Access, to log events that correspond to explicitly opening messages
 - Extended Send As, to log events that correspond to sending a message as a mailbox-enabled user
 - Extended Send On Behalf Of, to log events that correspond to sending a message on behalf of a mailbox-enabled user.
4. When you complete the auditing level configuration, click **Configure**.

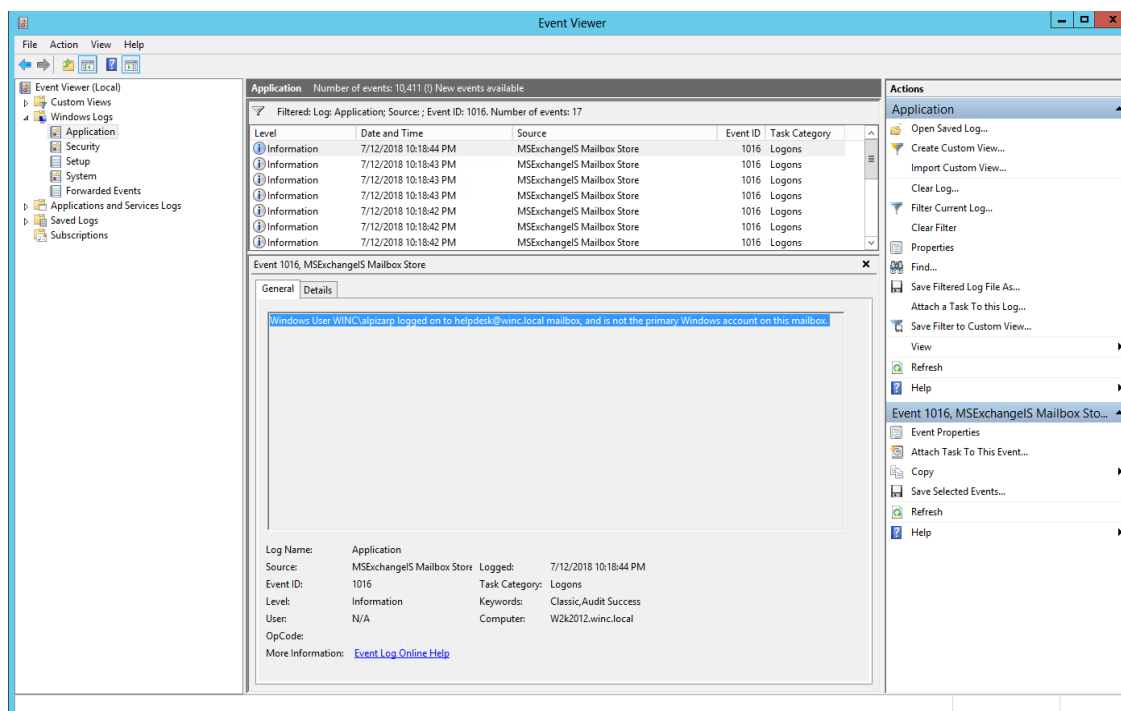
For more information about Exchange mailbox access auditing, see

http://www.msexchange.org/articles_tutorials/exchange-server-2007/compliance-policies-archiving/exchange-2007-mailbox-access-auditing-part1.html

For examples of configuring Exchange mailbox access auditing, see <http://www.howexchangeworks.com/2009/09/mailbox-access-auditing-in-exchange.html>

Accessing the Audited Information

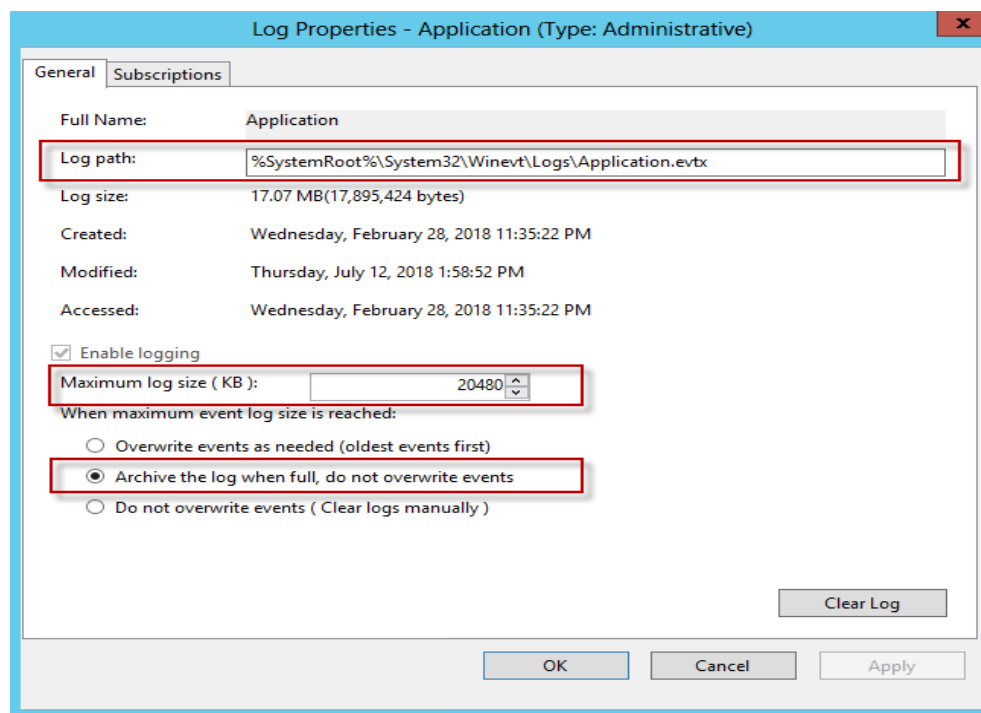
To view the information logged, navigate to **Event Viewer > Applications & Services Log > Exchange Auditing**.



Changing Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User
"service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -
InheritanceType All
```

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Exchange Events 10100, 10101 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier

ArcSight ESM Field	Device-Specific Field
File Name	%2 (Message ID or Folder name depending upon event)
File Path	%1 (Folder path)
Name	A folder in mailbox was opened by user.
Source Host Name	%9 (Account Name)
Source Process Name	%11 (Process Name)
Source Service Name	%13 (Application ID)
Target Address	Address
Destination User ID	%5 (Accessing User (full Exchange ID))
Destination User Name	%4 (Account Name)
Destination User Privileges	One of ('Administrative rights were used', '')

Exchange Event 10102 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
File Path	Folder path (when relevant)
Name	A message in mailbox was opened by user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address

Exchange Events 10104, 10106 Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier
Device Custom String 6	Sent as user
File Name	%3 (Message ID or Folder name, depending upon event)
Name	User sent a message on behalf of another user.
Source Host Name	10% (Machine Name)
Source Process Name	12% (Process Name)
Source Service Name	14% (Application ID)
Destination User ID	%6 (Accessing User (full Exchange ID))
Destination User Name	%5 (Account Name)
Destination User Privileges	One of ('Administrative rights were used', '')
Destination Host Name	%11 (Address)
Destination Address	%11 (Address)

Exchange Online Message Tracking

Message tracking, or message tracing, as it is called in Office 365, is one of the most basic tools used by administrators to monitor the email flow. As emails travel through Office 365, some information about them gets stored in logs and is available for administrative purposes. No matter if users delete or purge messages, the administrator is able to view basic information about sent and received emails.

This section provides information about configuring Exchange Online Message Tracking and event mappings.

Message tracing does not allow you to peek into a message's contents. Still, it can provide quite a lot of important data about emails:

- Sender and Recipient
- Send and receive dates
- Subject and size
- Status and details of events. There are seven possible values in the delivery status field: delivered, failed, pending, expanded, quarantined, filtered as spam and unknown.
- IP address used to send the message
- Message ID a unique number identifying a message. If a message is sent to more than one recipient, it will display once for every recipient in the message trace search, but all those entries will have the same Message-ID and different Message Trace ID

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'Exchange Online'
Name	Both('Message ',Status)
External Id	MessageTraceId
Device Receipt Time	Received
Device Event Class Id	Both('Message ',Status)
Device Custom String 3	Subject
Device Custom String 6	Organization

ArcSight ESM Field	Device-Specific Field
Source Address	FromIP
Source User Name	SenderAddress
Destination Address	ToIP
Destination User Name	RecipientAddress
File Size	Size
File Id	MessageId

Microsoft Exchange Mailbox Store

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions. Microsoft Exchange 2010 Service Pack 1 is supported by this SmartConnector.

This section provides information about configuring Microsoft Exchange Mailbox Store and understanding its event mappings to ArcSight data fields. This connector supports , Windows Server 2008 R2.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP1 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

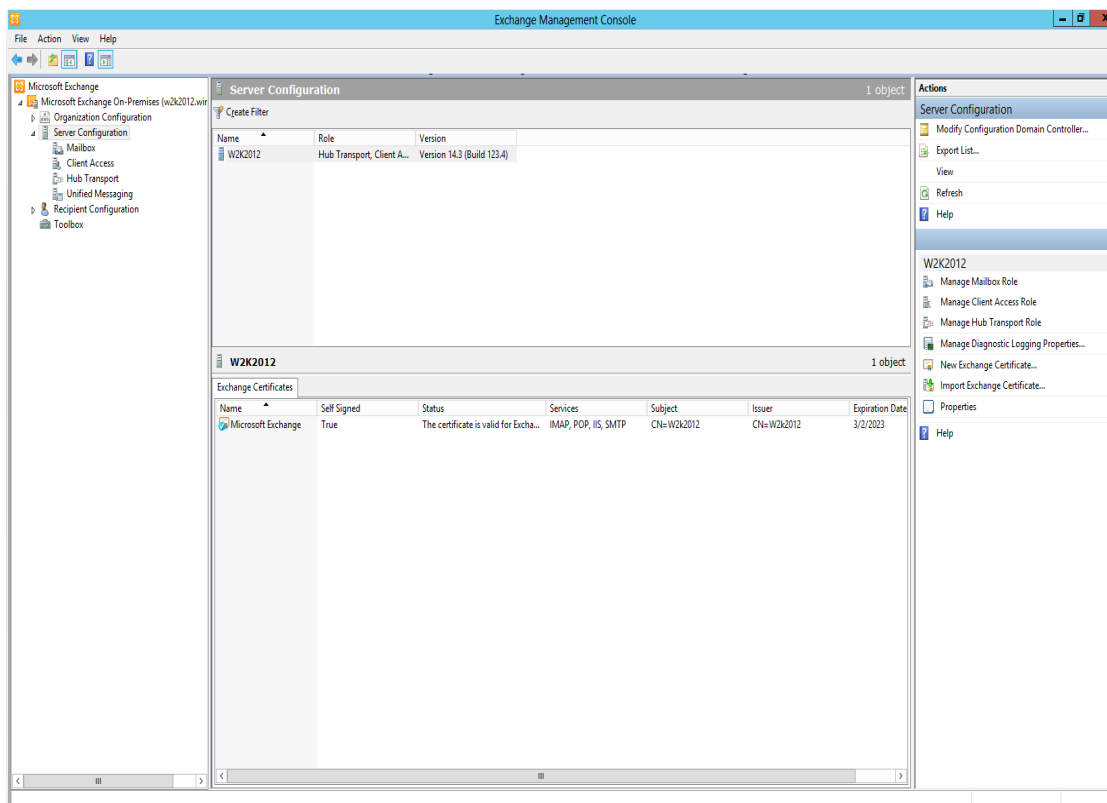
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Microsoft Exchange Mailbox Store Windows Event Log Native.

Configuring Mailbox Store Auditing

Use the Exchange Management Console to access the configuration area for mailbox store auditing.

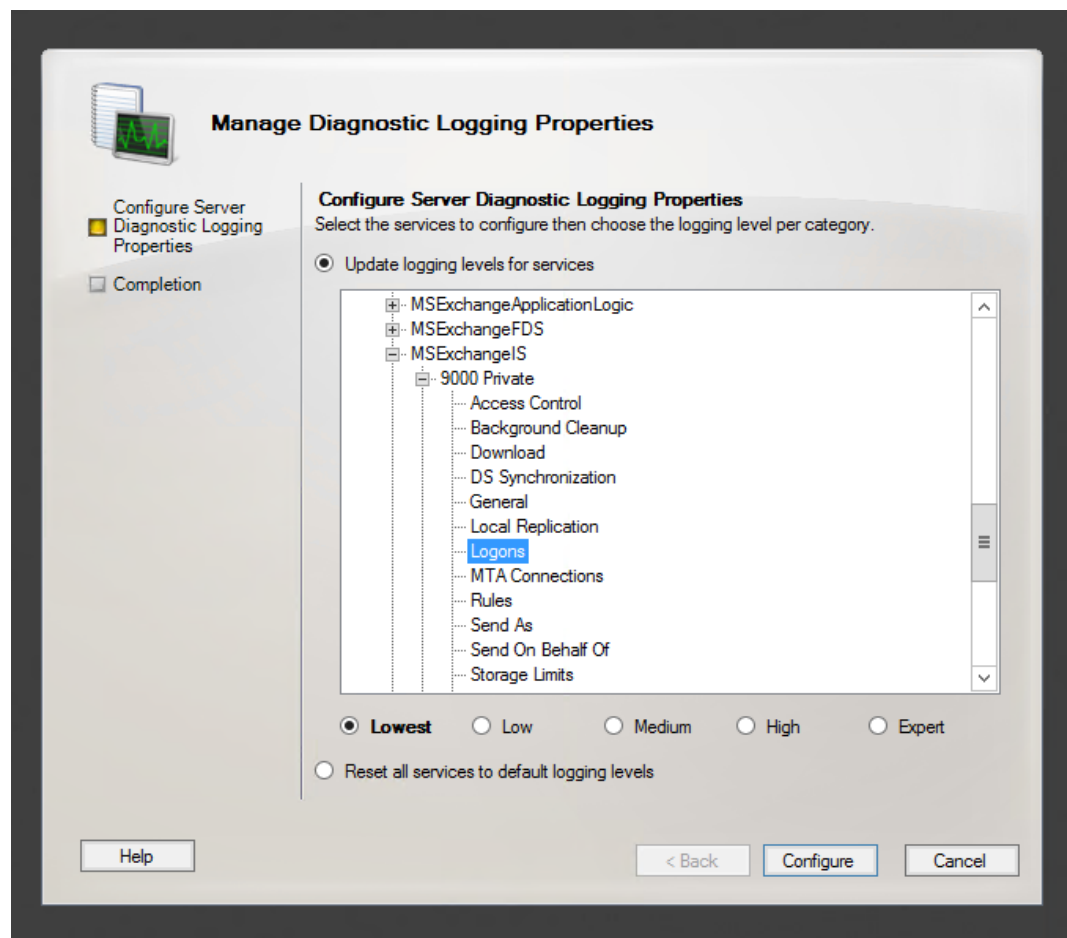
Enabling Mailbox Store

To access the configuration area for mailbox store auditing, use the Exchange Management Console. The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox store auditing on a particular mailbox server:

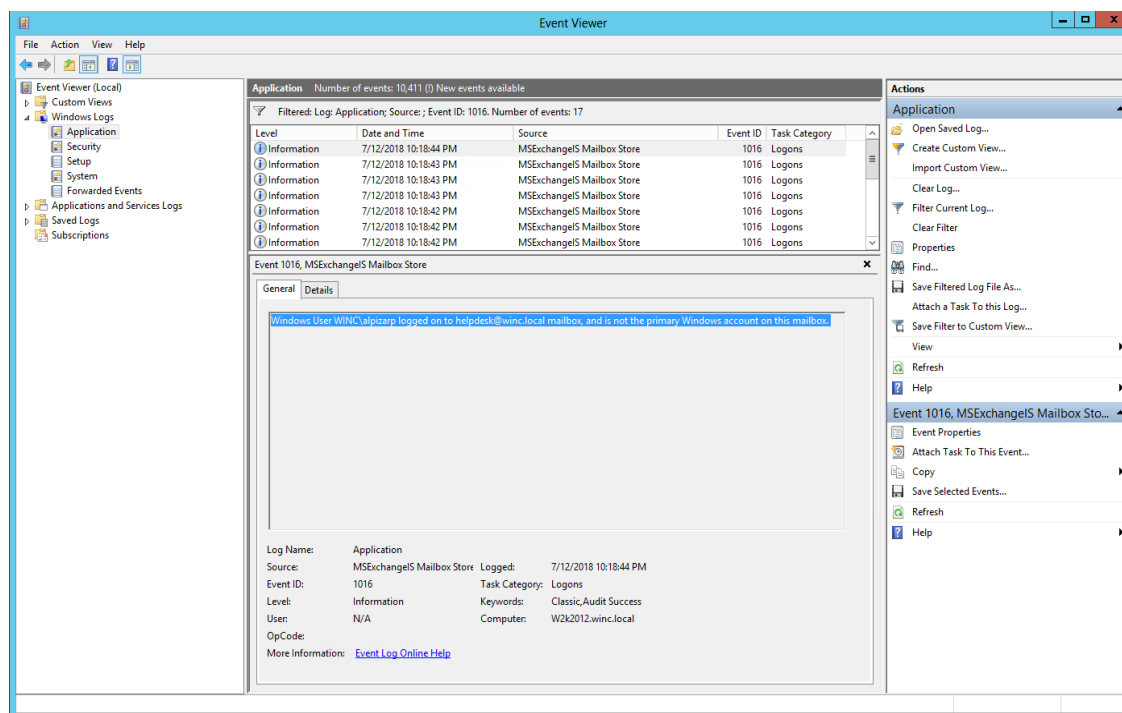
1. Select that server in the Exchange Management Console and then select the **Manage Diagnostics Logging Properties** menu option from the action pane; the **Manage Diagnostics Logging Properties** window is displayed.



2. In this window, expand the **MExchangeIS** category and then expand the **9000 Private** category.
3. Under the **MExchangeIS\9000 Private** category, configure MailBox Store for Event 1016 by selecting **Logons**.
4. When you have finished configuring the mailbox store levels, click **Configure**.
5. To view events, go to Windows Event Viewer, 1016 events are saved in Application Windows Events.

Accessing the Audited Information

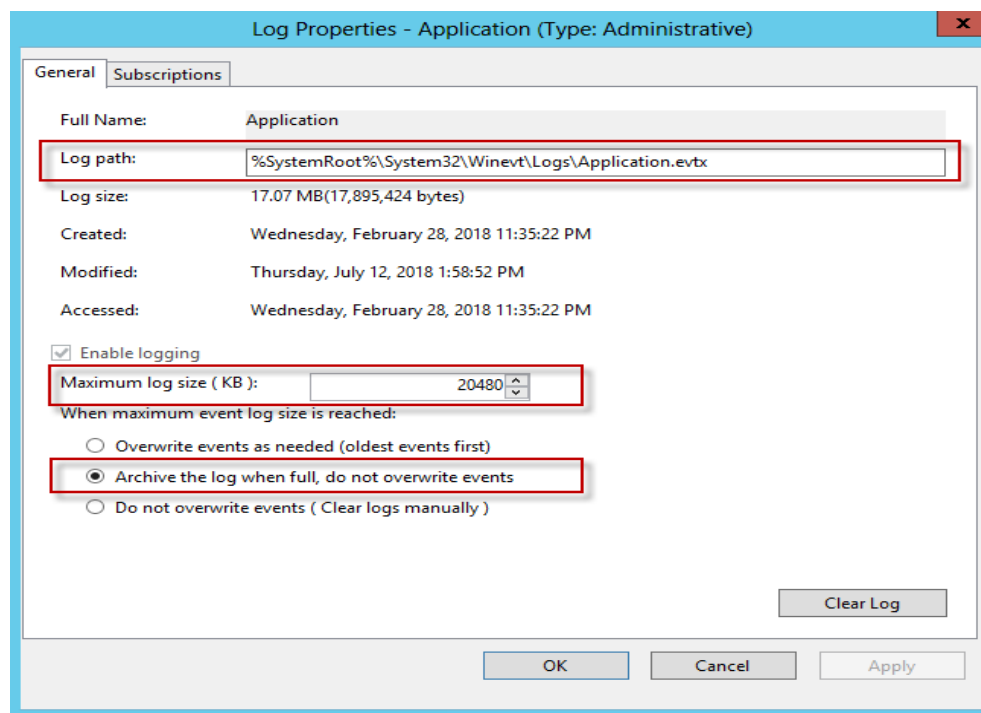
To view the information logged, navigate to **Event Viewer > Applications & Services Log > Exchange Auditing**.



Changing Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User  
"service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -  
InheritanceType All
```

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

General Exchange Events Mappings

ArcSight ESM Field	Device-Specific Field
Device Vendor	Microsoft
Device Product	Exchange Server

Exchange Events 1016 Mappings

ArcSight ESM Field	Device-Specific Field
Device Customer String3	%2 (Mail Box)
Source Nt Domain	%1
Source User Name	%1

Microsoft Forefront Protection 2010

Microsoft Forefront Protection 2010 for Exchange Server (FPE) provides protection against malware and spam by including multiple scanning engines in a single solution. FPE provides customers with an administration console that includes customizable configuration settings, filtering options, monitoring features and reports, anti-spam protection, and integration with the Forefront Online Protection for Exchange (FOPE) product.

This section provides information about configuring Microsoft Forefront Protection and its event mappings to ArcSight data fields. This connector supports Microsoft Forefront Protection 2010 events for Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 Standard with Exchange 2010.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Forefront Protection.

Configuring Forefront Protection

To enable writing events to the Windows Event Log from Forefront Protection:

1. In the Forefront Protection 2010 for Exchange Server Administrator Console, click **Policy Management**, and under **Global Settings**, click **Advanced Options**.
2. In the **Global Settings - Advanced Options** pane, under the **Logging Options** section, select the **Enable event logging** check box. When checked (the default), you can use the associated check boxes to individually enable or disable the following options (which are enabled by default):
 - **Incidents**—Enables or disables event logging for incidents.
 - **Engines**—Enables or disables event logging for engines.
 - **Operational**—Enables or disables logging for all other events, such as system information and health events.

When the **Enable event logging** check box is cleared, incidents logging is suspended for incidents, engines, and operational events.

3. Click **Save**.



Note: The relevant Microsoft Exchange and Microsoft Forefront Server protection services must be restarted in order for any changes to these settings to take effect. This typically includes the Microsoft Exchange Transport, Microsoft Exchange Information Store, and Microsoft Forefront Server Protection Controller services.

See **Microsoft TechNet → Microsoft Forefront TechCenter Library → Forefront Protection 2010 for Exchange Server → Operations → Configuring logging options** for more information.

Device Event Mapping to ArcSight Fields

The following sections lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Windows 2008

General

ArcSight ESM Field	Device-Specific Field
Device Product	'Forefront Protection'
Device Vendor	'Microsoft'

Event ID 7000

ArcSight ESM Field	Device-Specific Field
Message	'All the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	'All the antimalware engines selected in the Forefront Administration Console'

Event ID 7001

ArcSight ESM Field	Device-Specific Field
Message	'Not all the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	'Not all the antimalware engines selected in the Forefront Administration Console'

Event ID 7002

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have been updated successfully at the last attempt'

Event ID 7003

ArcSight ESM Field	Device-Specific Field
Name	'Not all of the antimalware engines enabled for updates have successfully updated at the last attempt'

Event ID 7004

ArcSight ESM Field	Device-Specific Field
Name	'Less than half of the antimalware engines enabled for updates have updated successfully at the last attempt.'

Event ID 7005

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have updated successfully in the last five days'

Event ID 7006

ArcSight ESM Field	Device-Specific Field
Name	'At least one of the antimalware engines enabled for updates has not been updated in the last five days.'

Event ID 7007

ArcSight ESM Field	Device-Specific Field
Name	'None of the antimalware engines enabled for updates have been updated in the last five days.'

Event ID 7008

ArcSight ESM Field	Device-Specific Field
Name	'The antimalware engines selected for transport scanning have been initialized.'

Event ID 7010

ArcSight ESM Field	Device-Specific Field
Name	The antimalware engines selected for realtime scanning have been initialized.'

Event ID 7012

ArcSight ESM Field	Device-Specific Field
Name	'The transport scan job is enabled'

Event ID 7015

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scan job is enabled.'

Event ID 7018

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scanning processes are running normally with no issues.'

Event ID 7021

ArcSight ESM Field	Device-Specific Field
Name	'The transport scanning processes are running normally with no issues.'

Event ID 7024

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running and the Forefront Agent is registered.'
Destination Service Name	'MS Exchange Transport Service'

Event ID 7025

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running but the Forefront Agent is not registered'
Destination Service Name	'MS Exchange Transport Service'

Event ID 7026

ArcSight ESM Field	Device-Specific Field
Name	'The MS Information Store is running and the Forefront VSAPI Library is registered.'

Event ID 7028

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period.'

Event ID 7033

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period'

Event ID 7035

ArcSight ESM Field	Device-Specific Field
Name	'There is at least amount of disk space available.'

Event ID 7040

ArcSight ESM Field	Device-Specific Field
Name	'The Eventing Service (FSCEventing) is functioning.'
Destination Service Name	'FSC Eventing'

Event ID 7044

ArcSight ESM Field	Device-Specific Field
Name	'The Mail Pickup Service (FSEMailPickup) is functioning.'
Destination Service Name	'FSEMailPickup'

Event ID 7046

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and definitions have been updated in the last one hour'

Event ID 7048

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and the last definition update was over 12 hours ago.'

Event ID 7051

ArcSight ESM Field	Device-Specific Field
Name	'The Monitor Service (FSCMonitor) is functioning.'
Destination Service Name	'FSCMonitor'

Event ID 7064

ArcSight ESM Field	Device-Specific Field
Name	'No archived undeliverable items exist'

FSC Controller

Event ID 1000

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is running.'
Destination Service Name	'Forefront Protection'

Event ID 1001

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service has stopped.'
Destination Service Name	'Forefront Protection'

Event ID 1020

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is starting.'
Destination Service Name	'Forefront Protection'

Event ID 1021

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is stopping.'
Destination Service Name	'Forefront Protection'

Event ID 1022

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Version'
Device Version	%1 (version)
Additional data	%2 (Virus Protection Feature)

Event ID 1023

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Service Pack'
Additional data	%1 (ServicePack)
Message	Both ('Forefront Protection Service Pack:',%1)

Event ID 1024

ArcSight ESM Field	Device-Specific Field
Name	'Product ID'
Additional data	%1 (ProductID)
Message	Both ('Product ID:', %1)

Event ID 1025

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Components'
Message	All of (Licensed Components: Component, License Type, Expiration Date)

Event ID 1026

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Engines'
Additional data	%1 (LicensedEngines)
Message	Both ('Licensed Engines:', %1)

Event ID 1028

ArcSight ESM Field	Device-Specific Field
Name	'System Information'
Additional data	%1 (System Information)
Message	Both ('System Information:', %1)

Event ID 1037

ArcSight ESM Field	Device-Specific Field
Name	'Event Tracing session has been started.'
Device Severity	'Information'

Event ID 1041

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has been started'

Event ID 1043

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has stopped'

Event ID 1044

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has completed'

Event ID 2102

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection application is still within the license period'

Event ID 5167

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection Monitor detected abnormal process shutdown'
Source Process Name	%1 (process name)
Message	Both ('Microsoft Forefront Protection Monitor detected abnormal' %1,' shutdown')

Event ID 5183

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan exceeded the allowed scan time limit'

Event ID 8046

ArcSight ESM Field	Device-Specific Field
Name	'AD Mark Created'

Event ID 8055

ArcSight ESM Field	Device-Specific Field
Name	'Ad Mark Removed'
Message	'Failed to Delete Reg Key'

FSC Eventing

Event ID 1075

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has started.'
Destination Service Name	'Forefront Protection Eventing'

Event ID 1076

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has stopped.'
Destination Service Name	'Forefront Protection Eventing'

FSC Manual Scanner

Event ID 1045

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan started.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1048

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan stopped.'
Request Client Operation	%1 (Request Client Operation)

Event ID 1052

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan has been completed.'
Request Client Operation	%1 (Request Client Operation)

FSC Scheduled Scanner

Event ID 2080

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan enabled.'

Event ID 2081

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan disabled.'

Event ID 3009

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan found virus.'
Device Custom String 4	mailbox name
Message	%2 (Message)
Device Custom String 1	virus name
Device Custom String 6	incident
Additional data	%4 (scan engine)
Device Action	%5 (Device Action)
File Name	%3 (File Name)

FSC Realtime Scanner

Event ID 2000

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan enabled.'

Event ID 2001

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan disabled.'

FSC Transport Scanner

Event ID 2007

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan enabled.'

Event ID 2008

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan disabled.'

Event ID 3002

ArcSight ESM Field	Device-Specific Field
Name	'Internet scan found virus'
File Path	%1 (folder)
Message	%2 (Message)
File Name	%4 (file name)
Device Custom String 6	Incident
Device Action	%6 (Device Action or State)
Device Custom String 1	virus name
Additional data	%3 (message ID)
Additional data	%5 (scan engine)

FSC Monitor

Event ID 1007

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store process started.'
Destination Process Name	'Information Store'

Event ID 1008

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store shutdown.'
Destination Process Name	'Information Store'

Event ID 1013

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is active.'

Event ID 1014

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is inactive.'

FSE On Demand Nav

Event ID 1049

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service is running.'
Destination Process Name	'FseOnDemandNav'

Event ID 1050

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service has stopped.'
Destination Process Name	'FseOnDemandNav'

FSE Mail Pickup

Event ID 1029

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service is running.'
Destination Service Name	'Forefront Protection Mail Pickup'

Event ID 1030

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service has stopped.'
Destination Service Name	'Forefront Protection Mail Pickup'

FSE IMC

Event ID 1002

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service started.'
Destination Service Name	'FSEIMC'

Event ID 1003

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service stopped.'
Destination Service Name	'FSEIMC'

FSE VS API

Event ID 5066

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan exceeded the allowed scan time limit'

FSC VSS Writer

Event ID 1094

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has started.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Event ID 1095

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has stopped.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Get Engine Files

Event ID 2011

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection did not detect any new scan engine updates'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection performed a successful scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 2017

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection has rolled back a scan engine'
Additional data	%1 (scan engine)

Event ID 2034

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection is attempting a scan engine update.'
Request URL	%2 (request url)
Additional data	%1 (scan engine)

Event ID 2109

ArcSight ESM Field	Device-Specific Field
Name	'The VBuster scan engine is no longer supported'
Message	'Updates are no longer available for this engine, and therefore the update check for this engine has been disabled. Please review the scan engine chosen for your scan jobs and make another selection to ensure up-to-date protection'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event ID 6012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Reason	%2 (Error Code)
Message	%3 (Error Detail)

Event ID 6014

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update.'
Additional data	%1 (scan engine)
Request URL	%2 (request url)
Additional data	%3 (proxy settings)
Reason	%4 (Error Code)
Message	%5 (Error Detail)

Event ID 6019

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Message	%2 (Error Detail)

Event ID 6020

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)
Message	%3 (Message)

Microsoft Netlogon

Netlogon is a Windows Server process in Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2008. The process is responsible for communication between systems in response to a logon request. This handles authentication of users and other services within a domain.

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Netlogon Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides main mappings for the Windows Event Log SmartConnectors. The field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Netlogon Logs

For information about Microsoft's netlogon events logs configuration, see <https://support.microsoft.com/en-in/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc> in the Microsoft TechNet Library.

Mappings for Microsoft Netlogon

General

ArcSight Field	Vendor Field
Device Product	"NETLOGON"
Device Vendor	'Microsoft'

Event 5827

ArcSight Field	Vendor Field
Device Custom String 1	%3 (Account Type)
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4 (Machine Operating System)
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5 (Machine Operating System Build)
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6 (Machine Operating System Service Pack)
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Denied"
Source Host Name	%1 (Machine SamAccountName)
Source Nt Domain	%2 (Domain)
Name	"Netlogon service denied vulnerable Netlogon secure channel connection from a machine account"

Event 5828

ArcSight Field	Vendor Field
Destination Nt Domain	%3 (Trust Target)
Device Custom String 1	%1 (Account Type)
Device Custom String 1 Label	"Account Type"
Event Outcome	"Denied"
Source Address	%4 (Client IP Address)
Source Nt Domain	%2 (Trust Name)
Name	"Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account"

Event 5829

ArcSight Field	Vendor Field
Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection"

Event 5830

Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because account is allowed in group policy"

Event 5831

ArcSight Field	Vendor Field
Destination Nt Domain	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Account Type"
Event Outcome	"Allowed"
Source Address	%4
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because trust account is allowed in group policy"

Microsoft Network Policy Server

Internet Authentication Service (IAS) was renamed Network Policy Server (NPS) starting with Windows Server 2008. The content of this guide applies to both IAS and NPS. Throughout the text, NPS is used to refer to all versions of the service, including the versions originally referred to as IAS.

Windows Server 2008 and Windows Server 2016 are supported.

Following sections provide information about configuring Microsoft Network Policy Server (NPS) and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Network Policy Server.

Configuring NPS Logging

NPS logging is also called RADIUS accounting, and should be configured to your requirements whether NPS is used as a RADIUS server, proxy, NAP policy server, or any combination of the three configurations.

To configure NPS logging, you must configure the events logged and viewed with Event Viewer and determine other information you want to log. In addition, you must decide whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

Using the event logs in Event Viewer, you can monitor Network Policy Server (NPS) errors and other events that you configure NPS to record.

NPS records connection request failure events in the System and Security event logs by default. Connection request failure events consist of requests that are rejected or discarded by NPS. Other NPS authentication events are recorded in the Event Viewer system log on the basis of

the settings that you specify in the NPS snap-in. Some events that might contain sensitive data are recorded in the Event Viewer security log.

Use this procedure to configure Network Policy Server (NPS) to record connection request failure and success events in the Event Viewer system log.

Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

To configure NPS event logging using the Windows interface:

1. Open the Network Policy Server (NPS) snap-in.
2. Right-click NPS (Local), and then click Properties.
3. On the General tab, select each required option, and then click OK.

Mappings for Network Policy Server

Delete this text and replace it with your own content.

Mappings for Windows 2016, 2012, and 8

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address',%1)
Source Address	%1 (client IP address)

Event 25

ArcSight ESM Field	Device-Specific Field
Name	'The address of remote RADIUS server in remote RADIUS server group resolves to local address will be ignored'
Message	Both ('The address of remote RADIUS server '%1,' in remote RADIUS server group '%2,' resolves to local address '%3,'. The address will be ignored.')
Source Address	%3 (address)
Additional data	%2 (ServerGroup)
Destination Address	%1 (address)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Message	Both ('A LDAP connection with domain controller '%1,' for domain '%2,' is established')
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain '%1')
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Message	Both ('NPS cannot log accounting information in the primary data store ('%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: '%2')

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	%1 (domain name)
Reason	%2 (reason code)

Mappings for Windows 2008 R2

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Source Address	%1 (client IP address)
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address ','%1)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)
Message	Both (A LDAP connection with domain controller ','%1,' for domain ','%2,' is established)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain' ','%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Destination Host Name	%1 (host name)
Reason	%2 (reason code)
Message	Both ('NPS cannot log accounting information in the primary data store (';%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: '%2')

Microsoft Service Control Manager

Service Control Manager (SCM) is a special system process under Windows NT family of operating systems that starts, stops, and interacts with Windows service processes. It is located in %SystemRoot%\System32\services.exe executable. Service processes interact with SCM through a well-defined API, and the same API interface is used internally by the interactive Windows service management tools such as the MMC snap-in Services.msc and the command-line Service Control utility sc.exe.

The following sections provide information about configuring Service Control Manager and its event mappings to ArcSight data fields.

Supported versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft Service Control Manager.

Mappings for Windows 2016, 2012, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

7000

ArcSight Field	Vendor Field
Name	'Service failed to start'
Message	'The 'param1' service failed to start due to error: 'param2''

ArcSight Field	Vendor Field
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)
Reason	param2

7001

ArcSight Field	Vendor Field
Name	'A service depends on other service which failed to start'
Message	'The 'param1' service depends on the 'param2' service which failed to start because of error: 'param3''
Destination Service Name	param1
Source Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

7002

ArcSight Field	Vendor Field
Name	'The 'param1' service depends on the 'param2' group and no member of this group started'
Destination Service Name	param1

7003

ArcSight Field	Vendor Field
Name	'A service depends on a nonexistent service'
Message	'The 'param1' service depends on a nonexistent service 'param2''
Destination Service Name	param1
Source Service Name	param2

7005

ArcSight Field	Vendor Field
Name	'The 'param1' call failed with error 'param2'
Device Custom String 4	Param2 (Reason or Error Code)

7006

ArcSight Field	Vendor Field
Name	'The 'param1' call failed for 'param2' with the following error 'param3''
Device Action	param2 (action)
Device Custom String 4	Param3 (Reason or Error Code)

7007

ArcSight Field	Vendor Field
Name	'The system reverted to its last known good configuration'
Message	'The system is restarting'

7008

ArcSight Field	Vendor Field
Name	'No backslash is in the account name'

7009

ArcSight Field	Vendor Field
Name	'Timeout waiting for the service to connect'
Message	'Timeout 'param1' waiting for the 'param2' service to connect'
Destination Service Name	param2

7010

ArcSight Field	Vendor Field
Name	'Timeout waiting for ReadFile'

7011

ArcSight Field	Vendor Field
Name	'Timeout waiting for a transaction response from the 'param2' service'
Destination Service Name	param2

7012

ArcSight Field	Vendor Field
Name	'Message returned in transaction has incorrect size'

7015

ArcSight Field	Vendor Field
Name	'Boot-start or system-start driver 'param1' must not depend on a service'

7016

ArcSight Field	Vendor Field
Name	'The 'param1' service has reported an invalid current state'
Destination Service Name	param1

7017

ArcSight Field	Vendor Field
Name	'Detected circular dependencies demand starting 'param1''
Destination Service Name	param1

7018

ArcSight Field	Vendor Field
Name	'Detected circular dependencies auto-starting services'

7019

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a service in a group which starts later.'
Destination Service Name	param1

7020

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a group which starts later'
Destination Service Name	param1

7021

ArcSight Field	Vendor Field
Name	'About to revert to the last known good configuration because the 'param1' service failed to start'
Destination Service Name	param1

7022

ArcSight Field	Vendor Field
Name	'The 'param1' service hung on starting'
Destination Service Name	param1

7023

ArcSight Field	Vendor Field
Name	'A service terminated with error.'
Message	The 'param1' service terminated with the following error 'param2''
Destination Service Name	param1
Reason	param2
Device Custom String 4	param2 (Reason or Error Code)

7024

ArcSight Field	Vendor Field
Name	'The 'param1' service terminated with the following service-specific error'
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)

7025

ArcSight Field	Vendor Field
Name	'At least one service or driver failed during system startup'
Message	'Use Event Viewer to examine the event log for details'

7026

ArcSight Field	Vendor Field
Name	'The boot-start or system-start driver(s) did not load'
Message	'The following boot-start or system-start driver(s) did not load: 'param1''
Device Process Name	param1

7027

ArcSight Field	Vendor Field
Name	'Windows could not be started as configured'
Message	'A previous working configuration was used instead'

7028

ArcSight Field	Vendor Field
Name	'The 'param1' Registry key denied access to SYSTEM account programs'
Message	'The Service Control Manager took ownership of the Registry key'
File Name	param1

7030

ArcSight Field	Vendor Field
Name	'The 'param1' service is marked as an interactive service'
Destination Service Name	param1
Message	'The system is configured to not allow interactive services. This service may not function properly.'

7031

ArcSight Field	Vendor Field
Name	Both ('The 'param1,' service terminated unexpectedly')
Destination Service Name	param1 (service name)
Message	Both ('The 'param1,' service terminated unexpectedly. It has done this 'param2,' time(s). The following corrective action will be taken in 'param3,' milliseconds: 'param5')
Device Action	param5 (action)

7032

ArcSight Field	Vendor Field
Name	'The Service Control Manager tried to take a corrective action 'param1' after the unexpected termination of the 'param2' service'
Device Action	param1
Message	'This action failed with error'
Destination Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)

7033

ArcSight Field	Vendor Field
Name	'The Service Control Manager did not initialize successfully'
Message	'The security configuration server (scserv.dll) failed to initialize with error 'param1'. The system is restarting.'
Device Custom String 4	param1 (Reason or Error Code)

7034

ArcSight Field	Vendor Field
Name	'A service terminated unexpectedly'
Message	'It has done this 'param2' times'
Destination Service Name	param1
Device Custom Number 3	param2 (Count)

7035

ArcSight Field	Vendor Field
Name	'The 'param1' service was successfully sent a 'param2' control'
Destination Service Name	param2

7036

ArcSight Field	Vendor Field
Name	'Service entered the 'param2" state'
Message	The 'param1' service entered the 'param2' state.'
Destination Service Name	param1
Device Action	param2

7037

ArcSight Field	Vendor Field
Name	'The Service Control Manager encountered an error undoing a configuration change to the 'param1' service'
Message	'The service's 'param2' is currently in an unpredictable state. If you do not correct this configuration, you may not be able to restart the 'param1' service or may encounter other errors. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1

7038

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to the following error: 'param3'. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

7039

ArcSight Field	Vendor Field
Name	'A service process other than the one launched by the Service Control Manager connected when starting the 'param1' service'
Destination Service Name	param1
Message	'The Service Control Manager launched process 'param2' and process 'param3' connected instead. Note that if this service is configured to start under a debugger, this behavior is expected.'

7040

ArcSight Field	Vendor Field
Name	'Start type of 'param1' service was changed from 'param2' to 'param3''
Message	'Start type of 'param1' service was changed from 'param2' to 'param3''
Destination Service Name	param1
Device Action	param3

7041

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password.'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	'Logon failure: the user has not been granted the requested logon type at this computer'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to error. This service account does not have the necessary user right 'Log on as a service''
Reason	'Logon failure: the user has not been granted the requested logon type at this computer'

7042

ArcSight Field	Vendor Field
Name	'A service was successfully sent a control'
Destination Service Name	param1 (service name)
Device Custom String 4	Reason or Error Code
Message	'The 'param1' service was successfully sent a 'param2' control. The reason specified was 'param3' ['param4'] Comment: 'param5''
Reason	Both ('param3,' 'param4')

7043

ArcSight Field	Vendor Field
Name	'The 'param1' service did not shutdown properly after receiving a preshutdown control'
Destination Service Name	param1

7045

ArcSight Field	Vendor Field
Name	'A service was installed in the system'
Destination Service Name	ServiceName
File Path	ImagePath
Device Custom String 5	StartType
Device Custom String 6	AccountName

Microsoft SQL Server Audit

With SQL Server 2008, Microsoft introduced an SQL Server Audit feature that provides a true auditing solution for enterprise customers. While SQL Trace can be used to satisfy many auditing needs, SQL Server Audit offers a number of advantages that can help DBAs more easily achieve their goals, such as meeting regulatory compliance requirements.

The SQL Server Audit feature is intended to replace SQL Trace as the preferred auditing solution. SQL Server Audit is meant to provide full auditing capabilities and only auditing capabilities, unlike SQL Trace, which is also used for performance debugging.

The following sections provide information about configuring Microsoft SQL Server Audit and its event mappings to ArcSight data fields.

Supported Versions

Microsoft Windows Server Version	Microsoft SQL Server Version
2008, 2008 R2	2008, 2012
2012	2012 SP1, 2014, 2016

SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft SQL Server Audit.

Configuring SQL Server Audit

For complete information about auditing in SQL Server, see Microsoft's SQL Server documentation at [https://msdn.microsoft.com/en-us/library/cc280525\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/cc280525(v=sql.120).aspx). This link takes you to the SQL Server 2014 version. You can select another version from the **Other Versions** drop down menu, but the basic steps are the same for sending audit events to an application log. From the left pane at this link, click **Create a Server Audit** and **Server Audit Specification** for detailed instructions.

Using SQL Server Management Studio, create a server audit as follows:

1. In Object Explorer, expand the **Security** folder.
2. Right-click the **Audits** folder and select **New Audit** to open a **Create Audit** window.
3. Enter a name for your audit (for example, **LoginFailed**). For **Audit destination**, select **ApplicationLog** from the list.
4. Click **OK** to accept the default settings and save the new audit specification.
5. The new audit will appear in the **Audits** folder. To enable the audit, select the audit you created, right-click, and select **Enable Audit**.

Customizing Event Source Mapping

For information about customizing event source mapping, see [Customizing Event Source Mapping](#).

Microsoft SQL Server Audit Application Event Log Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Destination User Name	''''

Event 615

ArcSight Field	Vendor Field
Name	'Could not find database'
Message	'Could not find database ID ',%1,', name ',%2,'

Event 849

ArcSight Field	Vendor Field
Name	'Using locked pages for buffer pool'
Message	'Using locked pages for buffer pool'

Event 852

ArcSight Field	Vendor Field
Name	'Using conventional memory in the memory manager'
Message	'Using conventional memory in the memory manager'

Event 919

ArcSight Field	Vendor Field
Name	'User is changing database script level'
Message	'User ',%1,' is changing database script level entry ',%2,' to a value of ',%3
Source User Name	%1
Device Custom Number 1	%2 (Level entry)
Device Custom Number 2	%3 (Changed value)

Event 958

ArcSight Field	Vendor Field
Name	'The resource database build version'
Message	'The resource database build version is ',%1
Device Custom String 4	%1 (Database build version)

Event 1486

ArcSight Field	Vendor Field
Name	'Database Mirroring Transport is disabled in the endpoint configuration'
Message	'Database Mirroring Transport is disabled in the endpoint configuration'

Event 1814

ArcSight Field	Vendor Field
Name	'Could not create tempdb'
Message	'Could not create tempdb. You may not have enough disk space available.'

Event 1945

ArcSight Field	Vendor Field
Name	'Warning! The maximum key length'
Message	One of ('Warning! The maximum key length for a "%1," index is "%2," bytes. The index "%3," has maximum length of "%4," bytes. For some combination of large values, the insert/update operation will fail.'). ('Warning! The maximum key length is "%1," bytes. The index "%2," has maximum length of "%3," bytes. For some combination of large values, the insert/update operation will fail.')
Device Custom String 1	Both (One of (%2, %1), 'bytes') (Maximum key length)
Device Custom String 2	One of (%3,%2) (Index)
Device Custom String 3	Both (One of (%4, %3), 'bytes') (Maximum index)
Device Custom String 4	%1 (Index Type)

Event 2007

ArcSight Field	Vendor Field
Name	'The module depends on the missing object'
Message	'The module '%1,' depends on the missing object '%2,'. The module will still be created; however, it cannot run successfully until the object exists.'
Device Custom String 1	%1 (Module)
Device Custom String 2	%2 (Missing object)

Event 2812

ArcSight Field	Vendor Field
Name	'Could not find stored procedure'
Message	'Could not find stored procedure '%1
Device Custom String 2	%1 (Stored procedure)

Event 3406

ArcSight Field	Vendor Field
Name	'Transactions rolled forward in database'
Message	%1' transactions rolled forward in database '%2, '(';%3,')'
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3407

ArcSight Field	Vendor Field
Name	'Transactions rolled back in database'
Message	%1,' transactions rolled back in database '%2, '(';%3,') ' '
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3408

ArcSight Field	Vendor Field
Name	'Recovery is complete'
Message	'Recovery is complete. This is an informational message only. No user action is required.'

Event 3421

ArcSight Field	Vendor Field
Name	'Recovery completed for database'
Message	'Recovery completed for database '%1,' (database ID '%2,') in '%3,' second(s) (analysis '%4,' ms, redo '%5,' ms, undo '%6,' ms.)'
Device Custom String 1	%1 (Database name)
Device Custom String 2	%4 ms (Analysis time)

ArcSight Field	Vendor Field
Device Custom String 3	%5 ms (Redo time)
Device Custom String 4	%6 ms (Undo time)
Device Custom String 5	%3 s (Completed recovery time)
Device Custom String 6	%2 (Database ID)

Event 3454

ArcSight Field	Vendor Field
Name	'Recovery is writing a checkpoint in database.'
Message	'Recovery is writing a checkpoint in database '%1,' ('%2,') '
Device Custom String 1	%1 (Database name)
Device Custom Number 1	%2 (Database ID)

Event 5084

ArcSight Field	Vendor Field
Name	'Setting database option'
Message	'Setting database option '%1,' to '%2,' for database '%3,' '
Device Custom String 1	%3 (Database name)
Device Custom String 2	%1 (Old option)
Device Custom String 3	%2 (New option)

Event 5579

ArcSight Field	Vendor Field
Name	'File system access'
Message	'#FILESTREAM: effective level = '%1,', configured level = '%2,', file system access share name = '%3,' '

Event 5701

ArcSight Field	Vendor Field
Name	'Changed database context'
Message	'Changed database context to ',%1
Device Custom String 1	%1 (Database name)
Device Action	'Changed'

Event 5703

ArcSight Field	Vendor Field
Name	'Changed language setting'
Message	'Changed language setting to ',%1
Device Custom String 1	%1 (Language setting)
Device Action	'Changed'

Event 6253

ArcSight Field	Vendor Field
Name	'Common language runtime (CLR) functionality initialized using CLR'
Message	'Common language runtime (CLR) functionality initialized using CLR version ',%1,' from ',%2
File Path	%2
Device Custom String 4	%1 (File version)

Event 6527

ArcSight Field	Vendor Field
Name	'.NET Framework runtime has been stopped'
Message	'.NET Framework runtime has been stopped'

Event 8128

ArcSight Field	Vendor Field
Name	'Execute extended stored procedure.'
Message	'Using ',%1,' version ',%2,' to execute extended stored procedure ',%3,'. This is an informational message only; no user action is required.'
File Name	%1
Device Custom String 3	%2 (File version)
Device Custom String 4	%3 (Extended stored procedure)

Event 9013

ArcSight Field	Vendor Field
Name	'Tail of the log for database is being rewritten'
Message	'Tail of the log for database ',%1,' is being rewritten to match the new sector size of ',%2,' bytes. ',%3,' bytes at offset ',%4,' in file ',%5,' will be written'

Event 9666

ArcSight Field	Vendor Field
Name	'Service endpoint is in disabled or stopped state'
Message	'The ',%1,' endpoint is in disabled or stopped state'
Destination Service Name	%1

Event 9688

ArcSight Field	Vendor Field
Name	'Service Broker manager has started'
Message	'Service Broker manager has started'

Event 9689

ArcSight Field	Vendor Field
Name	'Service Broker manager has shut down'
Message	'Service Broker manager has shut down'

Event 10981

ArcSight Field	Vendor Field
Name	'Resource governor reconfiguration succeeded'
Message	'Resource governor reconfiguration succeeded'

Event 12288

ArcSight Field	Vendor Field
Name	'Package started'
File Name	%1

Event 12291

ArcSight Field	Vendor Field
Name	'Package failed'
File Name	%1

Event 15268

ArcSight Field	Vendor Field
Name	'Authentication mode'
Message	'Authentication mode is ',%1
Device Custom String 3	%1 (Authentication mode)

Event 15457

ArcSight Field	Vendor Field
Name	'Configuration option changed'
Message	'Configuration option ',%1,' changed from ',%2,' to ',%3,'. Run the RECONFIGURE statement to install'
Device Custom String 3	%1 (Configuration option)
Device Custom Number 1	%2 (Old value)
Device Custom Number 2	%3 (New value)

Event 15477

ArcSight Field	Vendor Field
Name	'Caution: Changing any part of an object name could break scripts and stored procedures'
Message	'Caution: Changing any part of an object name could break scripts and stored procedures'

Event 17069

ArcSight Field	Vendor Field
Name	'Microsoft SQL Server 2012 (SP1)'
Message	%1

Event 17101

ArcSight Field	Vendor Field
Name	'Microsoft Corporation'
Message	'Microsoft Corporation'

Event 17103

ArcSight Field	Vendor Field
Name	'All rights reserved'
Message	'All rights reserved'

Event 17104

ArcSight Field	Vendor Field
Name	'Server process ID'
Message	'Server process ID is ',%1
Destination Process ID	%1

Event 17107

ArcSight Field	Vendor Field
Name	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'
Message	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'

Event 17108

ArcSight Field	Vendor Field
Name	'Password policy update was successful'
Message	'Password policy update was successful'
Device Action	'Update'

Event 17110

ArcSight Field	Vendor Field
Name	'Registry startup parameters'
Message	'Registry startup parameters ',%1
Device Custom String 1	%1 (Parameters)

Event 17111

ArcSight Field	Vendor Field
Name	'Logging SQL Server messages'
Message	'Logging SQL Server messages in file ',%1
File Name	%1

Event 17115

ArcSight Field	Vendor Field
Name	'Command Line Startup'
Message	'Command Line Startup Parameters: ',%1

ArcSight Field	Vendor Field
Device Action	'Startup'
Device Custom String 1	%1 (Parameters)

Event 17125

ArcSight Field	Vendor Field
Name	'Using dynamic lock allocation'
Message	'Using dynamic lock allocation. Initial allocation of ',%1,' Lock blocks and ',%2,' Lock Owner blocks per node'
Device Custom Number 1	%1 (Lock blocks)
Device Custom Number 2	%2 (Lock owner blocks)

Event 17126

ArcSight Field	Vendor Field
Name	'SQL Server is now ready for client connections'
Message	'SQL Server is now ready for client connections'

Event 17136

ArcSight Field	Vendor Field
Name	'Clearing tempdb database'
Message	'Clearing tempdb database'

Event 17137

ArcSight Field	Vendor Field
Name	'Starting up database'
Message	'Starting up database ',%1
Device Custom String 1	%1 (Database name)

Event 17147

ArcSight Field	Vendor Field
Name	'SQL Server is terminating because of a system shutdown'
Message	'SQL Server is terminating because of a system shutdown. This is an informational message only. No user action is required.'

Event 17148

ArcSight Field	Vendor Field
Name	'SQL Server is terminating'
Message	'SQL Server is terminating in response to a 'stop' request from Service Control Manager'

Event 17152

ArcSight Field	Vendor Field
Name	'Node configuration'
Message	'Node configuration: node '%1', CPU mask: '%2' : '%3,' Active CPU mask: '%4', '%5'. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.'
Device Custom String 2	%1 (Node)
Device Custom String 3	%2 (CPU mask)
Device Custom String 4	%4 (Active CPU mask)
Device Custom String 5	%3 (Flag CPU mask)
Device Custom String 6	%5 (Flag Active CPU mask)

Event 17162

ArcSight Field	Vendor Field
Name	'SQL Server is starting'
Message	'SQL Server is starting at normal priority base (=7)'

Event 17164

ArcSight Field	Vendor Field
Name	'SQL Server detected sockets'
Message	'SQL Server detected ',%1,' sockets with ',%2,' cores per socket and ',%3,' logical processors per socket, ',%4,' total logical processors; using ',%5,' logical processors based on SQL Server licensing. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected sockets)
Device Custom Number 2	%2 (Cores per socket)
Device Custom Number 3	%3 (Processors per socket)
Device Custom String 3	%4 (Total processors)
Device Custom String 4	%5 (Using processors)

Event 17176

ArcSight Field	Vendor Field
Name	'This instance of SQL Server last reported using a process ID'
Message	'This instance of SQL Server last reported using a process ID of ',%1,' at ',%2,' (local) ',%3,' (UTC). This is an informational message only; no user action is required.'
Destination Process ID	%1
Device Custom Date 1	%2, 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (local))
Device Custom Date 2	%3 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (UTC))

Event 17177

ArcSight Field	Vendor Field
Name	'This instance of SQL Server has been using a process ID'
Message	'This instance of SQL Server has been using a process ID of ',%1,' since ',%2,' (local) ',%3,' (UTC). '

Event 17199

ArcSight Field	Vendor Field
Name	'Restart SQL Server using the trace flag'
Message	'Dedicated administrator connection support was not started because it is disabled on this edition of SQL Server. If you want to use a dedicated administrator connection, restart SQL Server using the trace flag ',%1,'. This is an informational message only. No user action is required.'
Device Custom Number 1	%1 (Trace flag)

Event 17201

ArcSight Field	Vendor Field
Name	'Dedicated admin connection support was established'
Message	'Dedicated admin connection support was established for listening locally on port ',%1
Destination Port	%1

Event 17550

ArcSight Field	Vendor Field
Name	'DBCC TRACEON, server process'
Message	'DBCC TRACEON ',%1,' server process ID (SPID) ',%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' %1
Destination Process ID	%2

Event 17551

ArcSight Field	Vendor Field
Name	'DBCC TRACEOFF, server process'
Message	'DBCC TRACEOFF ',%1,' server process ID (SPID) ',%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' ,%1
Destination Process ID	%2

Event 17561

ArcSight Field	Vendor Field
Name	'index restored'
Message	'index restored for ',%2,', '%3
Device Custom String 1	%2 (Report server database)
Device Custom String 3	%3 (Object name)

Event 17656

ArcSight Field	Vendor Field
Name	'Warning'
Message	'Warning *****'

Event 17658

ArcSight Field	Vendor Field
Name	'SQL Server started in single-user mode'
Message	'SQL Server started in single-user mode. This is an informational message only. No user action is required.'

Event 17663

ArcSight Field	Vendor Field
Name	'Server name'
Message	'Server name is ',%1
Destination Host Name	%1

Event 17811

ArcSight Field	Vendor Field
Name	'The maximum number of dedicated administrator connections for this instance'
Message	'The maximum number of dedicated administrator connections for this instance is "',%1,'"."

ArcSight Field	Vendor Field
Device Custom Number 1	%1 (Maximum administrator connections)

Event 18453

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using Windows authentication'
Destination User Name	%1
Destination NT Domain	%1
Device Custom String 1	%2 (Windows authentication)

Event 18454

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using SQL Server authentication'
Source User Name	%1
Source Address	%2
Device Custom IPv6 Address 2	%2 (Source IPv6 Address)

Event 18456

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user '%1', '%2' '%3
Device Custom String 3	%2 (Login failed)
Source User Name	%1
Source Address	%3

Event 18488

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',%1,'. Reason: The password of the account must be changed. ',%2
Source User Name	%1
Source Address	%2

Event 18496

ArcSight Field	Vendor Field
Name	'System Manufacturer and System Model Information'
Message	'System Manufacturer: ',%1,' System Model: ',%2,' '
Device Custom String 1	%1 (System Manufacturer)
Device Custom String 2	%2 (System Model)

Event 19030

ArcSight Field	Vendor Field
Name	'SQL Trace was started'
Message	'SQL Trace ID ',%1,' was started by login ',%2,' '
Device Custom String 1	%1 (Trace ID)
Source User Name	%2

Event 19031

ArcSight Field	Vendor Field
Name	'SQL Trace stopped'
Message	'SQL Trace stopped. Trace ID = ',%1,'. Login Name = ',%2
Source User Name	%2

Event 19032

ArcSight Field	Vendor Field
Name	'SQL Trace was stopped due to server shutdown'
Message	'SQL Trace was stopped due to server shutdown. Trace ID = '%1,'. This is an informational message only; no user action is required.'
Device Custom Number 1	%1 (Trace ID)

Event 26018

ArcSight Field	Vendor Field
Name	'A self-generated certificate was successfully loaded for encryption'
Message	'A self-generated certificate was successfully loaded for encryption'

Event 26022

ArcSight Field	Vendor Field
Name	'Server is listening'
Message	'Server is listening on ['%1,' <','%2,'> '%3,']'
Device Custom String 4	%1 (Listening Address)
Application Protocol	%2
Destination Port	%3

Event 26037

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Server Principal Name'
Message	'Error: '%1,', state: '%2,'. Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos'

Event 26048

ArcSight Field	Vendor Field
Name	'Server local connection provider is ready to accept connection'
Message	'Server local connection provider is ready to accept connection on [','%1,']'
File Path	%1

Event 26067

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Service Principal Name (SPN)'
Message	'The SQL Server Network Interface library could not register the Service Principal Name (SPN) '%1,' for the SQL Server service. Windows return code: '%2,', state: '%3,'. Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This is an informational message. Further action is only required if Kerberos authentication is required by authentication policies and if the SPN has not been manually registered.'
Source Service Name	%1
Reason	%2
Device Custom String 1	%3 (State)

Event 26076

ArcSight Field	Vendor Field
Name	'SQL Server is attempting to register a Service Principal Name (SPN)'
Message	'SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.'

Event 30090

ArcSight Field	Vendor Field
Name	'New instance of full-text filter daemon host process has been successfully started.'
Message	'A new instance of the full-text filter daemon host process has been successfully started.'

Event 33090

ArcSight Field	Vendor Field
Name	'Attempting to load library into memory'
Message	'Attempting to load library '%1,' into memory. This is an informational message only. No user action is required'
File Name	%1

Event 33204

ArcSight Field	Vendor Field
Name	'SQL Server Audit could not write to the security log'
Message	'SQL Server Audit could not write to the security log'

Event 33205

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Event Class ID	All of (class_type, ' ', action_id)
Device Action	action_id
Event Outcome	succeeded
File ID	object_id
File Type	class_type
File Name	object_name
File Size	sequence_number
File Hash	audit_schema_version

ArcSight Field	Vendor Field
Old File ID	transaction_id
Message	statement
Source User ID	server_principal_id
Source User Name	server_principal_name
Source NT Domain	server_principal_name
Destination User ID	One of (server_principal_id, target_server_principal_id)
Destination NT Domain	One of (target_server_principal_name, server_principal_name)
Destination Host Name	server_instance_name
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	statement
Device Custom String 3	database_name
Device Custom String 4	Device Custom String 4 = database_principal_name
Device Custom String 5	One of (target_database_principal_name, database_principal_name)
Device Custom String 6	schema_name
Old File Name	All of('Additional Information : ',additional_information)
Source Address	One of(additional_information, device address (In case the address is local machine))
Source Host Name	device host name (In case the address is local machine)
Destination User Name	One Of(target_server_principal_name,server_principal_name)
Device Custom IPv6 Address 2	additional_information

Event 33217

ArcSight Field	Vendor Field
Name	'SQL Server Audit is starting the audits'
Message	'SQL Server Audit is starting the audits. This is an informational message. No user action is required.'

Event 33218

ArcSight Field	Vendor Field
Name	'SQL Server Audit has started the audits'
Message	'SQL Server Audit has started the audits. This is an informational message. No user action is required.'

Event 49903

ArcSight Field	Vendor Field
Name	'Detected RAM'
Message	'Detected ',%1,' of RAM. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected RAM)

Event 49904

ArcSight Field	Vendor Field
Name	'Service account'
Message	'The service account is ',%1,'. This is an informational message; no user action is required.'
Source Service Name	%1

Event 49910

ArcSight Field	Vendor Field
Name	'Software Usage Metrics is disabled'
Message	'Software Usage Metrics is disabled'

Event 49916

ArcSight Field	Vendor Field
Name	'UTC adjustment'
Message	'UTC adjustment.'
Device Custom String 1	All of 1%, :, 2% (UTC Adjustment)

Event 49917

ArcSight Field	Vendor Field
Name	'Default collation'
Message	All of 'Default collation',%1,' (',%2,' ',%3,').'
Device Custom String 1	%2 (Language)
Device Custom String 4	%1 (SQL collation)
Device Custom Number 2	%3 (Language ID)

Microsoft Sysmon

Microsoft Sysmon Logs is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, users can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

The following sections provide information about Microsoft Sysmon Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

This connector supports Microsoft Sysmon Operational version 11 events.

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Sysmon Logs

For complete information about Microsoft's Reporting and Microsoft Sysmon Logs, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Microsoft Sysmon Logs

General

ArcSight Field	Vendor Field
Destination Process Id	ProcessId
Device Product	'Sysmon'
Device Vendor	'Microsoft'
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Destination Process Name	Image
Destination Service Name	CommandLine
Device Action	'Process Create'
Device Custom String 1	IntegrityLevel
Device Custom String 4	CommandLine
Device Custom String 6	LogonGuid
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
Message	Description
Name	'Process Created'
Old File Hash	MITRE ID
Old File Id	ParentProcessGuid
Old File Name	OriginalFileName
Old File Path	CurrentDirectory
Source Nt Domain	__extractNTDomain(User)
Source Process Id	ParentProcessId
Source Process Name	ParentImage

ArcSight Field	Vendor Field
Source Service Name	ParentCommandLine
Source User Id	LoginId
Source User Name	__extractNTUser(User)

Event 2

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File creation time changed'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File creation time changed'
Name	'File creation time changed'
Old File Create Time	PreviousCreationUtcTime
Old File Hash	MITRE ID

Event 3

ArcSight Field	Vendor Field
Destination Address	__oneOfAddress(DestinationIp) (for destination aware)
Device Custom IPv6 Address 2	__stringToIPv6Address(SourceIp) (for non-destination aware)
Device Custom IPv6 Address 3	__stringToIPv6Address(DestinationIp) (for non-destination aware)
Destination Host Name	DestinationHostname
Destination Port	__safeToInteger(DestinationPort)
Destination Process Name	Image
Device Action	__concatenate("Initiated :",Initiated)
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Network connection detected'

ArcSight Field	Vendor Field
Name	'Network connection detected'
Old File Hash	MITRE ID
Source Address	__oneOfAddress(SourceIp) (for destination aware)
Source Host Name	SourceHostname
Source Nt Domain	__extractNTDomain(User)
Source Port	__safeToInteger(SourcePort)
Source Port Name	SourcePortName
Source User Name	__extractNTUser(User)
Transport Protocol	Protocol

Event 4

ArcSight Field	Vendor Field
Additional Data.Schema Version	SchemaVersion
Device Action	State
Device Receipt Time	UtcTime
Message	'Sysmon service state changed'
Name	'Sysmon service state changed'

Event 5

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Process Terminated'
Name	'Process Terminated'
Old File Hash	MITRE ID

Event 6

ArcSight Field	Vendor Field
Device Action	'Driver Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	'Driver Loaded'
Name	'Driver Loaded'
Old File Hash	MITRE ID

Event 7

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Image Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	Description
Name	'Image Loaded'
Old File Hash	MITRE ID
Old File Name	OriginalFileName

Event 8

ArcSight Field	Vendor Field
Destination Process Name	TargetImage
Device Action	'CreateRemoteThread detected'
Device Process Id	SourceProcessId
Device Receipt Time	UtcTime
File Id	TargetProcessGuid
Message	'CreateRemoteThread detected'
Name	'CreateRemoteThread detected'
Old File Hash	MITRE ID
Old File Id	SourceProcessGuid
Source Process Name	SourceImage

Event 9

ArcSight Field	Vendor Field
Device Action	'RawAccessRead detected'
Device Custom String 5	Device
Device Receipt Time	UtcTime
Destination Process Name	Image
File Id	ProcessGuid
Message	'RawAccessRead detected'
Name	'RawAccessRead detected'
Old File Hash	MITRE ID

Event 10

ArcSight Field	Vendor Field
Additional Data.Source Thread Id	SourceThreadId
Destination Process Name	TargetImage

ArcSight Field	Vendor Field
Device Action	'Process accessed'
Device Custom String 1	GrantedAccess
Device Process Id	__safeToInteger(SourceProcessId)
Device Receipt Time	UtcTime
File Id	TargetProcessGUID
Message	'Process accessed'
Name	'Process accessed'
Old File Id	SourceProcessGUID
Old File Hash	MITRE ID
Old File Path	CallTrace
Source Process Name	SourceImage

Event 11

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File Created'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File created'
Name	'File created'
Old File Hash	MITRE ID

Event 12

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry object added or deleted'
Device Custom String 1	EventType

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry object added or deleted'
Name	'Registry object added or deleted'
Old File Hash	MITRE ID

Event 13

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry value set'
Device Custom String 1	EventType
Device Custom String 4	Details
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry value set'
Name	'Registry value set'
Old File Hash	MITRE ID

Event 14

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry key and value rename'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	NewName

ArcSight Field	Vendor Field
Name	'Registry key and value rename'
Old File Hash	MITRE ID
Old File Path	TargetObject

Event 15

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File stream created'
Device Receipt Time	UtcTime
File Hash	Hash
File Id	ProcessGuid
File Create Time	CreationUtcTime
File Path	TargetFilename
Message	'File stream created'
Name	'File stream created'
Old File Hash	MITRE ID

Event 16

ArcSight Field	Vendor Field
Device Action	'Sysmon config state changed'
Device Receipt Time	UtcTime
File Hash	ConfigurationFileHash
Message	'Sysmon config state changed'
Name	'Sysmon config state changed'
Source Process Name	Configuration

Event 17

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Created'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Create Pipe'
Name	'Create Pipe'
Old File Hash	MITRE ID

Event 18

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Connected'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Pipe Connected'
Name	'Pipe Connected'
Old File Hash	MITRE ID

Event 19

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
Name	'WmiEventFilter activity detected'
Old File Hash	MITRE ID
Old File Path	EventNamespace
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 20

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
File Path	Destination
File Type	Type
Name	'WmiEventConsumer activity detected'
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 21

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Filter
Device Custom String 5	Consumer
Device Receipt Time	UtcTime
Name	'WmiEventConsumerToFilter activity detected'

ArcSight Field	Vendor Field
Old File Hash	MITRE ID
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 22

ArcSight Field	Vendor Field
Destination Address	__regexToken(QueryResults)
Destination Process Name	Image
Device Action	'Dns query'
Device Custom String 1	QueryName
Device Custom String 4	QueryResults
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Dns query'
Name	'Dns query'
Old File Hash	MITRE ID

Event 23

ArcSight Field	Vendor Field
Device Custom String 1	IsExecutable
Device Custom String 4	Archived
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Hash	Hashes
File Path	TargetFilename
Message	__concatenate("File has been deleted from ",__extractNTDomain(TargetFilename))
Name	'File Delete'
Old File Hash	MITRE ID

ArcSight Field	Vendor Field
Source Nt Domain	__extractNTDomain(User)
Source Process Name	Image
Source User Name	__extractNTUser(User)

Event 255

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
Device Action	__stringConstant("Level : Error")
Message	Description
Name	'Error report'
Source Process Name	ID

User 32 Service

Routing and Remote Access is a network service in Windows Server 2008 R2 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about User 32 Service and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows Server 2008 R2

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft User 32.

Configuring Remote Access

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 1074

ArcSight Field	Vendor Field
Name	The process has initiated the shutdown/restart of computer.
Message	concatenate(The process "%1," has initiated the "%5," of computer "%2," on behalf of user "%7," for the following reason: "%3)
Source Process Name	%1
Destination Host Name	%2
Reason	%3
Device Custom String4	Reason Code
Device Custom String5	Shutdown Type
Device Custom String6	Comment

Microsoft Windows AppLocker

Microsoft Windows AppLocker is a network service in Windows 10, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 and Windows 2019 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows AppLocker and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Microsoft Windows AppLocker

For complete information about Microsoft's Reporting and Microsoft Windows AppLocker, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Microsoft Windows AppLocker

Event 8001

ArcSight Field	Vendor Field
Name	"The AppLocker policy was applied successfully to this computer."

Event 8002

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8003

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8004

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8005

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8006

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Event 8007

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6:	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullFilePath or FilePath

Microsoft Windows ESENT

Microsoft Windows ESENT is an embeddable and transactional database engine which is used for data storage. You can use ESENT for applications that need reliable, high-performance, and low-overhead storage of structured or semi-structured data. The ESENT engine can help with data needs ranging from something as simple as a hash table that is too large to store in memory to something more complex such as an application with tables, columns, and indexes.

The following sections provide information about configuring Microsoft Windows ESENT Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)

Mappings for Microsoft Windows ESENT Logs

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'ESENT'
Device Version	'Unknown'

Event Id 102

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is starting a new instance

Event Id 103

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine stopped the instance

Event Id 105

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine started a new instance

Event Id 224

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4 to %5
Name	Deleting log files

Event Id 225

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	No log files can be truncated

Event Id 300

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is initiating recovery steps

Event Id 301

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
File Type	%6
Device Custom String 1	%7
Device Custom String 1 Label	Number of times log record seen
Name	The database engine has finished replaying log file

Event Id 302

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine has successfully completed recovery steps

Event Id 325

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine created a new database"

ArcSight Field	Vendor Field
Source Process Id	%2
Source Service Name	%1

Event Id 326

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine attached a database"
Source Process Id	%2
Source Service Name	%1
Source Process Name	%3

Event Id 327

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine detached a database"
Source Process Id	%2
Source Service Name	%1

Event Id 330

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%7
Device Custom String 4 Label	Default engine version
Name	The database format version is being held back

Event Id 335

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%5
Reason	%7
Name	Replay of a create for database at log position was deferred

Event Id 455

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%5
Device Custom String 4 Label	Error
Name	Error occurred while opening log file

Event Id 641

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Device Custom String 4	%5
Device Custom String 4 Label	Log format version
Device Custom String 5	%6
Device Custom String 5 Label	Current log format version
Name	The log format feature version could not be used

Microsoft Windows BITS Client Logs

Microsoft Windows Background Intelligent Transfer Service (BITS) helps programmers and system administrators to download files from or upload files to HTTP web servers and share files using Server Message Block (SMB) protocol. BITS will take the cost of the transfer into consideration, as well as the network usage so that the user's foreground work has as little impact as possible. It also handles network interruptions, pausing, and automatically resuming transfers, even after a reboot. BITS includes PowerShell cmdlets for creating and managing transfers as well as the BitsAdmin command-line utility.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows BITS Client Logs and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019 (*)

Mappings for Microsoft Windows BITS Client

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows BITS Client'

Event ID 3

ArcSight Field	Vendor Field
Destination Nt Domain	string2
Destination User Name	string2
Device Custom String 4	string

ArcSight Field	Vendor Field
Device Custom String 4 Label	"Job Title"
Message	All of("The BITS service created a new job: ",string," , with owner ",string2)
Name	"The BITS service created a new job"

Event ID 4

ArcSight Field	Vendor Field
Device Custom Number 1	fileCount
Device Custom Number 1 Label	"File count"
Device Custom String 4	jobTitle
Device Custom String 4 Label	"Job Title"
Device Custom String 5	jobId
Device Custom String 5 Label	"Job ID"
Device Custom String 6	jobOwner
Device Custom String 6 Label	"Job Owner"
Message	All of("The transfer job is complete.User: ",User," , Transfer job: ",jobTitle," , Job ID: ",jobId," , Owner: ",jobOwner," , File count: ",fileCount)
Name	"The transfer job is complete"
Source Nt Domain	User
Source User Name	User

Event ID 59

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"

ArcSight Field	Vendor Field
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS started the ",name," transfer job that is associated with the ",url," URL")
Name	"BITS started the transfer for job"

Event ID 60

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring for job"

ArcSight Field	Vendor Field
Old File Name	Both("Proxy :",proxy)
Old File Path	Both("Bandwidth Limit :",bandwidthLimit)
Reason	Both ("0x",hr)

Event ID 61

ArcSight Field	Vendor Field
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring the job"
Old File Name	Both("Proxy :",proxy)
Reason	Both("0x",hr)

Microsoft Windows Event

The Windows event log is a detailed record of system, security and application notifications stored by the Windows operating system that is used by administrators to diagnose system problems and predict future issues.

These event logs are used to record important hardware and software actions that the administrator can use to troubleshoot issues with the operating system. The Windows operating system tracks specific events in its log files, such as application installations, security management, system setup operations on initial startup, and problems or errors.

The following sections provide information about the Microsoft Windows Event Log and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Windows Event Log.

Configuring Windows Update Client

For complete information about Microsoft's Reporting and Windows-Update Client, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Windows Update Client

Windows-Windows Update Client is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provides information about Windows Update Client and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Windows Update Client

For complete information about Microsoft's Reporting and Windows-Windows Update Client, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Windows-WindowsUpdateClient

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft-Windows-WindowsUpdateClient'

Event 16

ArcSight Field	Vendor Field
Name	'Unable to Connect: Windows is unable to connect to the automatic updates service'

Event 17

ArcSight Field	Vendor Field
Name	'Installation Ready: The following updates are downloaded and ready for installation'

Event 18

ArcSight Field	Vendor Field
Name	'Installation Ready : The updates are downloaded and scheduled for installation'
Device Custom String 4 Label	stringConstant("Scheduled Install Date")
Device Custom String 4	schedinstalldate
Device Custom String 5 Label	stringConstant("Scheduled Install Time")
Device Custom String 5	schedinstalltime
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 19

ArcSight Field	Vendor Field
Name	'Installation Successful: Window successfully installed the updates'
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 20

ArcSight Field	Vendor Field
Name	Installation Failure: Windows failed to install the Updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 21

ArcSight Field	Vendor Field
Name	Restart Required : The computer must be restarted
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 22

ArcSight Field	Vendor Field
Name	Restart Required : The computer will be restarted

Event 27

ArcSight Field	Vendor Field
Name	Automatic Updates is now paused

Event 28

ArcSight Field	Vendor Field
Name	Automatic Update is now resumed

Event 43

ArcSight Field	Vendor Field
Name	Installation Started: Windows has started installing the updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Event 44

ArcSight Field	Vendor Field
Name	Downloading Started: Windows Update started downloading an update
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")

ArcSight Field	Vendor Field
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant("Update Revision Number"))

Microsoft Windows WMI Activity Trace

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft Windows WMI Activity Trace and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Mappings for Microsoft Windows WMI Activity Trace

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	Microsoft Windows WMI Activity Trace
Name	WMI-Activity Query executed on Win23 BIOS
Device Custom String 1	ClientMachineFQDN
Device Custom String 3	CorrelationId
Device Custom String 4	IsLocal
Device Custom String 5	Operation
Device Custom Number 1	OperationId
Device Custom Number 2	GroupOperationId
Source Host Name	ClientMachine
Source User Name	User

ArcSight Field	Vendor Field
Source Process Id	ClientProcessId
File Create Time	ClientProcessCreationTime
File Path	NamespaceName

Microsoft Windows WMI Analytic and Operational

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components.

The following sections provide information about Windows Update Client and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 10
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Mappings for WMI Analytics Operations

Delete this text and replace it with your own content.

Mappings for Microsoft Windows WinRM Analytic

Event 788

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Processing Client Request For Operation
Device Action	operationName

Event 789

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	"Entering The Plugin For Operation".
Device Action	operationName
Request Url	resourceUri

Event 1050

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	"Sending Response For Operation"
Device Action	operationName

Event 1295

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	User Authenticated Successfully
Destination User Name	username

Mappings for Microsoft Windows WinRM Operational

Event 6

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Creating WSMAN Session
File Path	connection

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Creating WSMAN Shell
File Id	shellId
Request Url	resourceUri

Event 15

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WSMAN Command

Event 142

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WSMAN Operation Identify Failed
Device Action	operationName
Device Custom Number 3	errorCode
Device Custom Number 3 Label	Error Code

Event 161

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WinRM Cannot Process The Request
Message	authFailureMessage

Event 162

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Authenticating The User Failed

Event 169

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Destination User Name	username
Request Method	authenticationMechanism

Event 81

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operationName

Event 82

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operation
Request Url	resourceURI

Microsoft WINS Server

Microsoft WINS servers are designed to prevent the administrative difficulties that are inherent in the use of both IP broadcasts and static mapping files such as LMHOSTS files. Microsoft WINS is designed to eliminate the need for IP broadcasts (which use valuable network bandwidth and cannot be used in routed networks), while providing a dynamic, distributed database that maintains computer name-to-IP-address mappings.

WINS servers use a replicated database that contains NetBIOS computer names and IP address mappings (database records). When Windows-based computers log on to the network, their computer name and IP address mapping are added (registered) to the WINS server database, providing support for dynamic updates. The WINS server database is replicated among multiple WINS servers in a LAN or WAN. One of the benefits of this database design is that it prevents different users from registering duplicate NetBIOS computer names on the network.

WINS clients, referred to as WINS-enabled clients, are configured to use the services of a WINS server. Windows NT-based clients are configured with the IP address of one or more WINS servers by using the WINS Address tab on the Microsoft TCP/IP Properties page in Control Panel > Network.

The following sections provide information about configuring Microsoft WINS Server and its event mappings to ArcSight data fields.

Supported versions

- Microsoft Windows 8
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Microsoft WINS Server.

Configuring WINS

You can run the Registry Editor program at the command prompt to configure a WINS server by changing the values of the Registry parameters. Parameters for logging include:

Configuration Option	Description
Logging Enabled	Specifies whether logging of database changes to J50.log files should be turned on.
Log Detailed Events	Specifies whether logging events is verbose mode. (This requires considerable computer resources and should be turned off if you are tuning for performance.)

Windows 2016, 2012, and 8

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

4097

ArcSight Field	Vendor Field
Name	'WINS initialized properly and is now fully operational'

4098

ArcSight Field	Vendor Field
Name	'WINS was terminated by the service controller'
Message	'WINS will gracefully terminate'

4119

ArcSight Field	Vendor Field
Name	'WINS received a packet that has the wrong format'

4143

ArcSight Field	Vendor Field
Name	'WINS scavenged its records in the WINS database'
Message	'The number of records scavenged is given in the data section'

4178

ArcSight Field	Vendor Field
Name	'The WINS Pull configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4179

ArcSight Field	Vendor Field
Name	'The WINS Push configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4180

ArcSight Field	Vendor Field
Name	'The WINS\\Parameters key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4181

ArcSight Field	Vendor Field
Name	'# The subkey could not be created or opened'
Message	'This key should be there if you want WINS to do consistency checks on its database periodically. NOTE: Consistency checks have the potential of consuming large amounts of network bandwidth. Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

4224

ArcSight Field	Vendor Field
Name	'WINS encountered a database error'
Message	'This may or may not be a serious error. WINS will try to recover from it'

4252

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Pull key'

4253

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Push key'

4309

ArcSight Field	Vendor Field
Name	'System Resource Information'
Device Custom Number 1	Processor Count
Device Custom Number 2	Physical Memory
Device Custom Number 3	Memory available for allocation

4318

ArcSight Field	Vendor Field
Name	'WINS could not start due to a missing or corrupt database'
Message	'Restore the database using WINS Manager (or winscl.exe found in the Windows 2000 Resource Kit) and restart WINS'

4325

ArcSight Field	Vendor Field
Name	'WINS could not read the Initial Challenge Retry Interval from the registry'

4326

ArcSight Field	Vendor Field
Name	'WINS could not read the Challenge Maximum Number of Retries from the registry'

4329

ArcSight Field	Vendor Field
Name	'The WINS server has started a scavenging operation'

4330

ArcSight Field	Vendor Field
Name	'The WINS server has completed the scavenging operation'

4337

ArcSight Field	Vendor Field
Name	'WINS Server could not initialize security to allow the read-only operations'

5001

ArcSight Field	Vendor Field
Name	'WINS is scavenging the locally owned records from the database'
Message	'The version number range that is scavenged is given in the data section, in the second to fifth words, in the order: from_version_number (low word, high word) to_version_number (low word, high word)'

5002

ArcSight Field	Vendor Field
Name	'WINS is scavenging a chunk on N records in the version number range from X to Y'
Message	'N, X and Y (low word, high word for version numbers) are given in the second to sixth words in the data section'

Oracle Audit

Auditing is a default feature of the Oracle server. The standard audit commands allow all system privileges to be audited along with access at the object level to any table or view on the database for select, delete, insert or update. Audit can be run for either successful or unsuccessful attempts or both. It can be for each individual user or for all users, and it can also be done at the session level or access level. At action level a single record is created per action and at session level one record is created for all audit actions per session.



Note: None of the connector versions support Oracle Multitenant at this time.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit and its event mappings to ArcSight data fields. Oracle database versions 10g, 11g, 12cR1 and 18c with Microsoft Windows Server 2012 are supported.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Native: Oracle Audit.

Configuring Auditing

For complete information about Oracle database auditing, see "Configuring Auditing" in the *Oracle Database Security Guide* for your database version.

Enabling Auditing

Database auditing is enabled and disabled by the AUDIT_TRAIL initialization parameter in the database initialization parameter file, `init.ora`. Setting it to OS enables database auditing and directs all audit records to an operating system file:

```
AUDIT_TRAIL=OS
```

Auditing Administrative Users

Sessions for users who connect as SYS can be fully audited, including all users connecting as SYSDBA or SYSOPER. Use the AUDIT_SYS_OPERATIONS initialization parameter to specify whether such users are to be audited. For example, the following setting specifies that SYS is to be audited:

```
AUDIT_SYS_OPERATIONS = TRUE
```

The default value, FALSE, disables SYS auditing.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Oracle Windows Event Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Oracle'

Event ID 4

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Initializing SGA for instance ',%1)
Name	'Initializing SGA for instance'

Event ID 5

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Both ('Initializing SGA for process ',%1,' in instance ',%2)
Name	'Initializing SGA for process in instance'
Destination Process Name	%1 (Destination Process Name)

Event ID 8

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Shutdown normal performed on instance ',%1)
Name	'Shutdown normal performed on instance'

Event ID 12

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('All process in instance ', '%1, ' stopped')
Name	'All process in instance stopped'

Oracle Audit SYSDBA Event Mappings to ArcSight ESM Fields

Event ID 34

ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessId
Destination User Name	DATABASE USER
Destination User Privileges	PRIVILEGE
Device Action	first word from ACTION
Device Custom Number 1	STATUS
Device Custom String 6	CLIENT TERMINAL
Device Event Class Id	first word of ACTION
Device External ID	DBID
Device Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
Message	first word from ACTION
Name	first word from ACTION
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

Oracle Audit Trail Event Mappings to ArcSight ESM Fields

Event ID 34

ArcSight ESM Field	Device-Specific Field
Additional data	LOGOFF_DEAD
Additional data	LOGOFF_LREAD
Additional data	LOGOFF_LWRITE
Additional data	LOGOFF_PREAD
Additional data	OBJ_CREATOR
Additional data	SESSIONCPU
Additional data	SES_TID
Additional data	STATEMENT
Destination Host Name	USERHOST
Destination NT Domain	USERHOST
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom Number 1	RETURNCODE
Device Custom Number 2	SESSIONID
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 4	SES_LABEL
Device Custom String 5	SES_ACTIONS
Device Event Class Id	ACTION
Device External ID	DBID
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'

ArcSight ESM Field	Device-Specific Field
File Name	Object name
Name	ACTION
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source NT Domain	OSSUSERID
Source User Name	OS_USERID
Reason	RETURNCODE
Transport Protocol	PROTOCOL
Device Custom IPv6 Address 2	Source IPv6 Address
File Name	Name
Source Port	Port

Oracle Unified Audit Trail Event Mappings to ArcSight ESM Fields

Event ID 36

ArcSight ESM Field	Device-Specific Field
Device External ID	DBID
Device Custom Number 2	SESID
Device Custom Number 3	ENTRYID
Destination User Name	DBUSER
Source User Name	CURUSER
Device Action	ACTION
Name	ACTION
Device Custom Number 1	RETCODE
Reason	RETCODE
Device Event Class Id	ACTION
File Name	OBJNAME
Device Product	'Oracle'
Device Custom String 3	SCHEMA
Old File ID	CLIENTID

Powershell

PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes.

PowerShell commands let you manage computers from the command line. PowerShell providers let you access data stores, such as the registry and certificate store, as easily as you access the file system. PowerShell includes a rich expression parser and a fully developed scripting language.

As it is widely used by the black hat community for initial access and further lateral movement within an enterprise, it is critical to properly collect and parse Windows Powershell logs. This would open the doors to writing correlation and hunt/search tools to find the APT's and other advanced threats.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Powershell and its event mappings to ArcSight data fields.

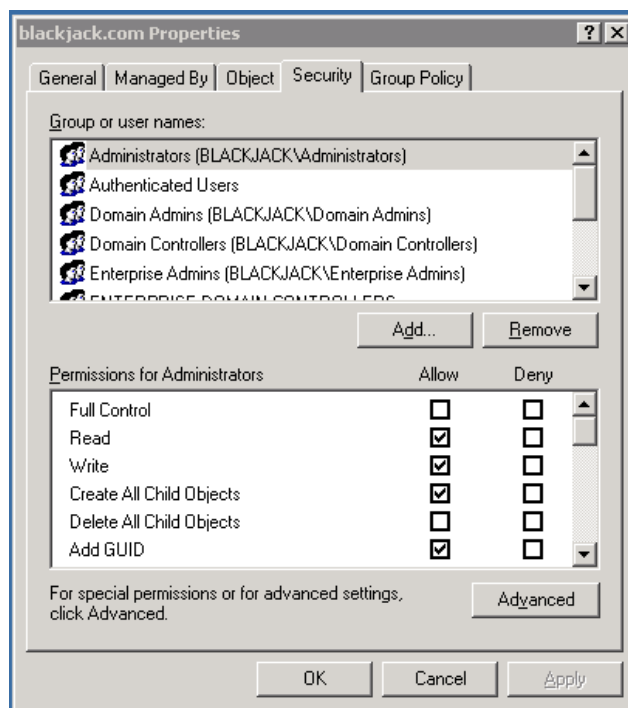
The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Microsoft Powershell Windows Event Log – Native: Powershell.

Configuring Auditing for Specific Powershell Objects

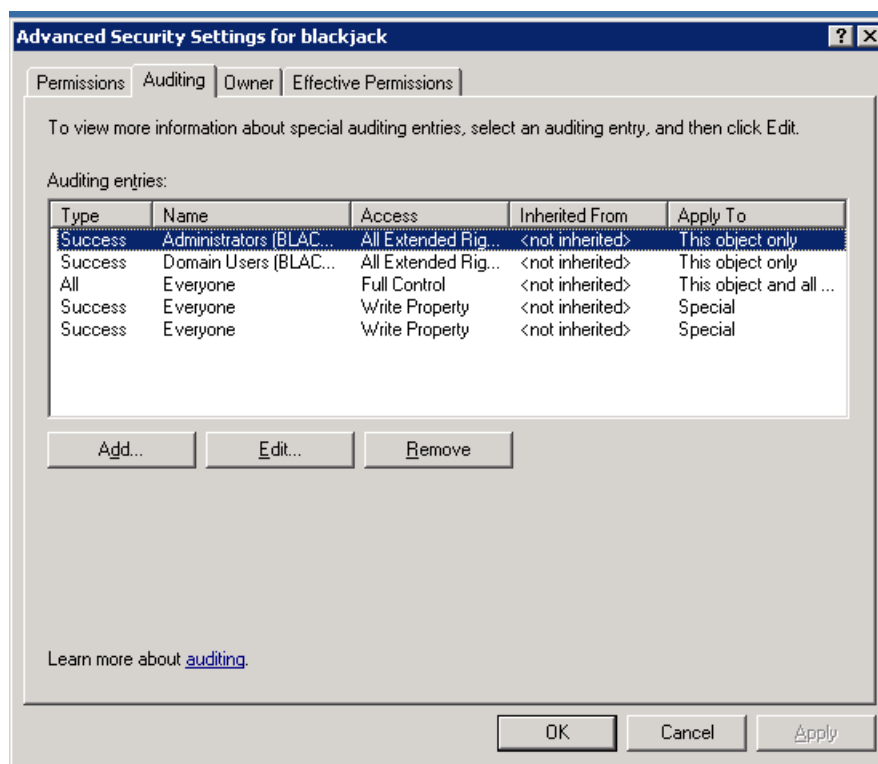
After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

To configure auditing for specific Powershell objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Powershell Users and Computers**.
2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Powershell object you want to audit (blackjack.com in the example) and select **Properties**.



- Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



- To add an object, click **Add**.

6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Mappings for PowerShell Events

Delete this text and replace it with your own content.

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'PowerShell'

Windows PowerShell Mappings

Event 400, 403

ArcSight Field	Vendor Field
Name	'Engine state is changed'
Message	'Engine state is changed from',%2,'to',%1
File Hash	%1
Old FileHash	%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath

ArcSight Field	Vendor Field
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 500, 501

ArcSight Field	Vendor Field
Name	'Command State'
Message	'Command "',%1," is ',%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId')(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 600

ArcSight Field	Vendor Field
Name	'Provider State'
Message	'Provider "',%1," is ',%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId')(Host Information)
Request Client Application	HostApplication

ArcSight Field	Vendor Field
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 800

ArcSight Field	Vendor Field
Name	'Pipeline execution details for command line'
Message	'Pipeline execution details for command line: ',%1
Device Custom String 1	%3(Details)
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ',HostName,', Host Version: ',HostVersion,', Host ID: ',HostId')(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
Old File Name	ScriptName
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Windows Microsoft-Windows-PowerShell/Operational Mappings

Event 4100

ArcSight Field	Vendor Field
Name	'Error Message'
Device Custom String 1	UserData(User Data)
Device Severity	Severity
Device Custom String 4	All of ('Host Name: ',Host Name,', Host Version: ',Host Version,', Host ID: ',Host Id)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Permission	CommandLine
Device Custom Number 2	SequenceNumber(Sequence Number)
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID
Message	Error Message, ' ',Recommended Action
Reason	Fully Qualified Error ID

Event 4103

ArcSight Field	Vendor Field
Name	'Command Invocation'
Message	Payload
Device Custom String 1	UserData(User Data)
Device Severity	Severity

ArcSight Field	Vendor Field
Device Custom String 4	All of ('Host Name: ',Host Name,', Host Version: ',Host Version,', Host ID: ',Host Id')(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	Command Name
File Type	Command Type
Old File Name	Script Name
File Path	Command Path
File Permission	Command Line
Device Custom Number 2	SequenceNumber(Sequence Number)
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID

Event 4104

ArcSight Field	Vendor Field
Name	'Creating Scriptblock text'
Message	'Creating Scriptblock text(',MessageNumber,' of ',MessageTotal,'\\):',ScriptBlockText
Device Custom Number 1	MessageNumber(Message Number)
Device Custom Number 2	Message Total
File Name	ScriptBlockText
File Path	Path

Event 4105

ArcSight Field	Vendor Field
Name	'Started invocation of ScriptBlock'
Message	'Started invocation of ScriptBlock ID',ScriptBlockId

ArcSight Field	Vendor Field
File ID	ScriptBlockId
Old File ID	RunspaceId

Event 8193

ArcSight Field	Vendor Field
Name	'Creating Runspace object'
Message	'Creating Runspace object Instance Id:',param1
Device Custom String 5	param1(Instance Id)

Event 8194

ArcSight Field	Vendor Field
Name	'Creating RunspacePool object'
Message	'Creating RunspacePool object Instance Id:',InstanceId
Device Custom String 5	param1(Instance Id)
Device Custom Number 1	MaxRunspaces(Max Runspaces)
Device Custom Number 2	MinRunspaces(Min Runspaces)

Event 8195

ArcSight Field	Vendor Field
Name	'Opening RunspacePool'
Message	'Opening RunspacePool'

Event 8196, 12039

ArcSight Field	Vendor Field
Name	'Modifying activity Id and correlating'
Message	'Modifying activity Id and correlating'

Event 8197

ArcSight Field	Vendor Field
Name	'Runspace state changed'
Message	'Runspace state changed to ',param1
Device Action	param1

Event 24577

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has started to run script file'
Message	'Windows PowerShell ISE has started to run script file ',FileName
File Path	FileName

Event 24579

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the current command'
Message	'Windows PowerShell ISE is stopping the current command'

Event 24580

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is resuming the debugger'
Message	'Windows PowerShell ISE is resuming the debugger'

Event 24581

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the debugger'
Message	'Windows PowerShell ISE is stopping the debugger'

Event 24582

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping into debugging'
Message	'Windows PowerShell ISE is stepping into debugging'

Event 24583

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping over debugging'
Message	'Windows PowerShell ISE is stepping over debugging'

Event 24584

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping out of debugging'
Message	'Windows PowerShell ISE is stepping out of debugging'

Event 24592

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling all breakpoints'
Message	'Windows PowerShell ISE is enabling all breakpoints'

Event 24593

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling all breakpoints'
Message	'Windows PowerShell ISE is disabling all breakpoints'

Event 24594

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing all breakpoints'
Message	'Windows PowerShell ISE is removing all breakpoints'

Event 24595

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is setting the breakpoint'
Message	'Windows PowerShell ISE is setting the breakpoint at line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24596

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing the breakpoint'
Message	'Windows PowerShell ISE is removing the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24597

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling the breakpoint'
Message	'Windows PowerShell ISE is enabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24598

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling the breakpoint'
Message	'Windows PowerShell ISE is disabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24599

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has hit a breakpoint'
Message	'Windows PowerShell ISE has hit a breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 40961

ArcSight Field	Vendor Field
Name	'PowerShell console is starting up'
Message	'PowerShell console is starting up'

Event 40962

ArcSight Field	Vendor Field
Name	'PowerShell console is ready for user input'
Message	'PowerShell console is ready for user input'

Event 53249

ArcSight Field	Vendor Field
Name	'Scheduled Job started'
Message	'Scheduled Job ',ScheduledJobDefName,' started at ',StartTime
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
Start Time	Start Time

Event 53250

ArcSight Field	Vendor Field
Name	'Scheduled Job completed'
Message	'Scheduled Job ',ScheduledJobDefName,' completed at ',StopTime,' with state ',State

ArcSight Field	Vendor Field
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
End Time	StopTime
Device Action	State

Event 53504

ArcSight Field	Vendor Field
Name	'Windows PowerShell has started an IPC listening thread'
Message	'Windows PowerShell has started an IPC listening thread on process: ',param1,' in AppDomain: ',param2
Destination Process Id	param1
Device Custom String 1	param2(App Domain)

Remote Access

Routing and Remote Access is a network service in Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, and Windows Server 2016 that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Remote Access Service and its event mappings to ArcSight data fields.

Supported Versions

- Microsoft Windows 8
- Microsoft Windows 10
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

The *SmartConnector for Microsoft Windows Event Log – Windows Security Event Mappings* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for Microsoft Remote Access.

Configuring Remote Access

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)":

<http://technet.microsoft.com/en-us/library/hh831416>

Mappings for Remote Access Events

Delete this text and replace it with your own content.

Mappings for Windows 2016, 2012, 2012 R2, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

20088

ArcSight Field	Vendor Field
Name	'Remote Access Server acquired IP Address'
Message	Both ('The Remote Access Server acquired IP Address '%1,' to be used on the Server Adapter.')
Destination Address	%1 (Assigned Address)

20106

ArcSight Field	Vendor Field
Name	'Unable to add interface'
Message	One of ('Unable to add the interface '%1,' with the Router Manager for the '%2,' protocol. The following error occurred: '%3'), ('Unable to add the interface '%2,' with the Router Manager for the '%3,' protocol. The following error occurred: '%4'))
Device Outbound Interface	One of (%1, %2)
Application Protocol	One of (%2, %3)
Device Custom String 5	Routing Domain ID

20169

ArcSight Field	Vendor Field
Name	'Unable to contact a DHCP server'
Message	Both ('The Automatic Private IP Address '%1,' will be assigned to dial-in clients. Clients may be unable to access resources on the network.')
Source Address	%2 (Address)

20184

ArcSight Field	Vendor Field
Name	'Interface is unreachable'
Message	Both ("Interface ",One of(%1,%2)," is unreachable because it is not currently connected to the network.")
Device Inbound Interface	One of (%1, %2)
Device Custom String 5	Routing Domain ID

20249

ArcSight Field	Vendor Field
Name	'Failed to authenticate'
Message	Both ('The user '%2,' has connected and failed to authenticate on port '%3,'. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)

20252

ArcSight Field	Vendor Field
Name	'Authentication process did not complete'
Message	Both ('The user connected to port '%2,' has been disconnected because the authentication process did not complete within the required amount of time.')
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)

20255

ArcSight Field	Vendor Field
Name	'Connection was prevented'
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Message	%4 (Message Text)

20258

ArcSight Field	Vendor Field
Name	'Account does not have Remote Access privilege'
Message	Both ('The account for user '%3,' connected on port '%4,' does not have Remote Access privilege. The line has been disconnected.')
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)

20266

ArcSight Field	Vendor Field
Name	'Successfully authenticated'
Message	Both ('The user '%3,' has connected and has been successfully authenticated on port '%4,'. Data sent and received over this link is strongly encrypted.')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)

ArcSight Field	Vendor Field
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)

20271

ArcSight Field	Vendor Field
Name	'Failed an authentication attempt'
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Message	Both ('The user '%2,' connected from '%3,' but failed an authentication attempt due to the following reason: '%4')
Reason	%5 (Reason)

20272

ArcSight Field	Vendor Field
Name	'User connected and disconnected'
Message	Both (The user '%One of (%2, %3),' connected on port '%One of (%3, %4),' on '%One of (%4, %5),' at '%One of (%5, %6),' and disconnected on '%One of (%6, %7),' at '%One of (%7, %8),''. The user was active for '%One of (%8, %9),' minutes '%One of (%9, %10),' seconds. '%One of (%10, %11),' bytes were received. The reason for disconnecting was '%One of (%12, %13),''. The tunnel used was '%One of (%13, %14),''. The quarantine state was '%One of (%14, %15),''.')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of (%3, %4)
Start Time	Both (One of (%4, %5),' '%One of (%5, %6)))

ArcSight Field	Vendor Field
End Time	Both (One of(%6,%7)," ",One of(7,%8))
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	One of (%10, %11)
Bytes In	One of (%11, %12)
Additional data	One of (%12, %13)
Additional data	One of (%13, %14)
Additional data	One of (%14, %15)

20274

ArcSight Field	Vendor Field
Name	'User connected and has been assigned address'
Message	Both ('The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' has been assigned address ',One of (%4, %5))
Device Custom String 4	correlation-ID
Device Custom String 5	Routing Domain ID
Source User Name	One of (%2, %3)
Source NT Domain	One of (%2, %3)
Application Protocol	One of (%3, %4)
Source Port	One of %3, %4)
Destination Address	One of (%4, %5)

20275

ArcSight Field	Vendor Field
Name	'User disconnected'
Message	Both ('The user with ip address ',One of (%2, %3),' has disconnected')
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Source Address	One of (%2, %3)

Mappings for Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user '%2,' has connected and failed to authenticate on port '%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port '%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)

ArcSight Field	Vendor Field
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user '%2,' connected on port '%3,' on '%4,' at '%5,' and disconnected on '%6,' at '%7,'. The user was active for '%8,' minutes, '%9,' seconds, '%10,' bytes were sent and '%11,' bytes were received. The reason for disconnecting was '%12,. The tunnel used was '%13,'. The quarantine state was '%14,','')

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user '%2,' connected on port '%3,' has been assigned address '%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address '%2,' has disconnected')

Collecting Forwarded Events

The connector has the ability to read events forwarded to a Windows Event Collector host. Windows Event Collection is a Microsoft capability that lets a Windows host collect events from multiple sources. Collecting forwarded events is different than the traditional event collection because the events are collected from multiple sources.

With Microsoft Windows Event Collector (WEC), you can subscribe to receive and store events on a local computer (event collector) that are forwarded from any number of remote computers (event sources). Before using this feature, refer to Microsoft Windows documentation, to know more about Windows Event Collector functionality.



Note: When configuring Windows Event Collection (WEC), Microsoft by default adds to every forwarded event a RenderingInfo section that is a textual description of an event. This extra section introduces negative impacts on the resource usage of the WEC machine as well as the performance of the connector. Therefore, Micro Focus advises that you disable the RenderingInfo section.

To do so, run the following command from the Windows command console: `wecutil ss <subscription-name> /cf:events`, where subscription-name is the WEC configuration created for event forwarding. This can be found in the Event Viewer > Subscriptions folder.

Event Collector for Windows Event Forwarding

You can forward events from a source host to any log type on the collector machine to which the connector would normally have access.



Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types

Source Hosts Windows OS Version

When the connector is configured with the log that has forwarded events, the Windows OS version of the event source host is not populated automatically in the normalized events. To have this value populated, the Windows OS version should be provided as a source host file or the Active Directory should be configured. If the Windows OS version is available from the source host file as well as Active Directory, the value from Active Directory takes precedence. Active Directory as Source for OS Version

When this selection is chosen during connector configuration, the connector pulls the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information. Newly discovered hosts are added to the lookup automatically without reconfiguring the connector itself.

Active Directory information is checked upon connector startup and every 24 hours (86400000 milliseconds). To change the time setting, locate the `agent.properties` file in `$ARCSIGHT_HOME/current/agent` and set the `hostbrowsingthreadsleeptime` parameter to the number of milliseconds between host browsing queries.) This value should be greater than 0; if the value is set to 0, it will not perform periodic host browsing. For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it should be placed within the same forest as the Active Directory.

File as Source for OS Version

When this selection is chosen during connector configuration, create a source host file in .csv format that contains the host name and Windows OS version and upload this file during the connector installation/configuration process (the WEF Source Hosts File Name in step 9).



Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the WEF Source Hosts File Name field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

```
hostsa.domaina.com,Windows 7
```

```
hostsb.domainb.com,Windows 8
```

```
hostsc.domainb.com,Windows Server 2012
```

```
Hostsd.domaind.com,Windows Server 2016
```

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

```
Windows Vista
```

```
Windows Server 2008
```

```
Windows Server 2008 R2
```

```
Windows Server 2012
```

```
Windows Server 2012 R2
```

```
Windows Server 2016
```

```
Windows 7
```

```
Windows 8
```

```
Windows 10
```



Note: OS version information is optional; events may still be parsed in a majority of cases.

Once configured, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Additional Connector Configurations

You can refer to the following sections for additional and optional connector configurations:

Configuring Custom Logs and Filtering

If you selected **Custom logs** in the **Select logs for event collection** section of the initial configuration window, and you want to add filtering for the local host, check **Custom Logs** in the **Select logs for event collection** section to ensure this window is displayed for you to enter filter parameters.

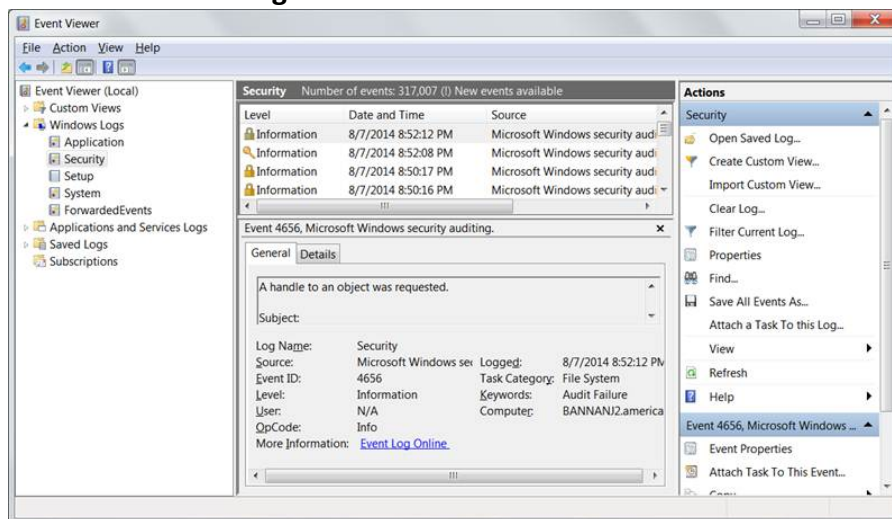
The parameters for each host are given in full along with descriptions in the following table. Selections from the initial parameter entry window for the local host are reflected in the first row of the table. Select options and provide custom log and filter information for each additional host manually.

After entering the parameter information, click **Next**.

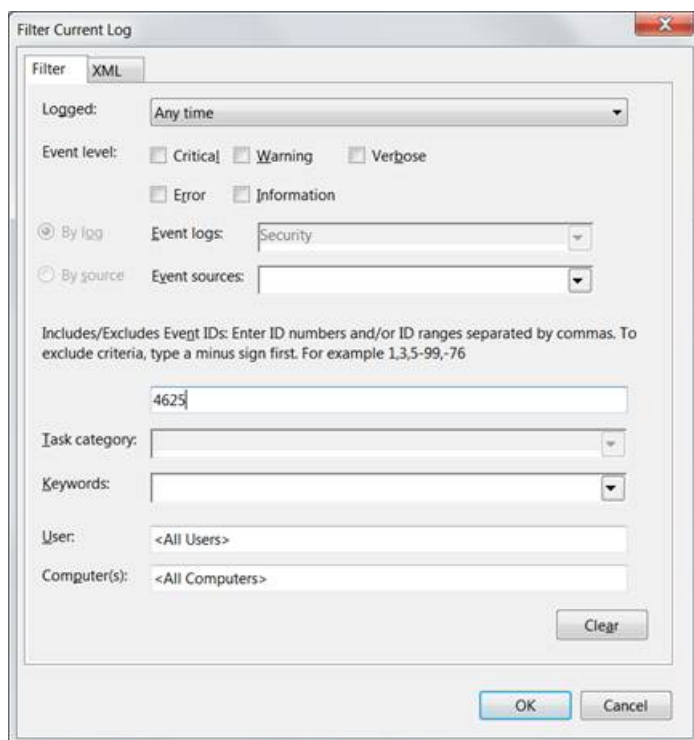
Configuring Filter

To configure a filter, first launch the event viewer and select the event log that needs the filter setting.

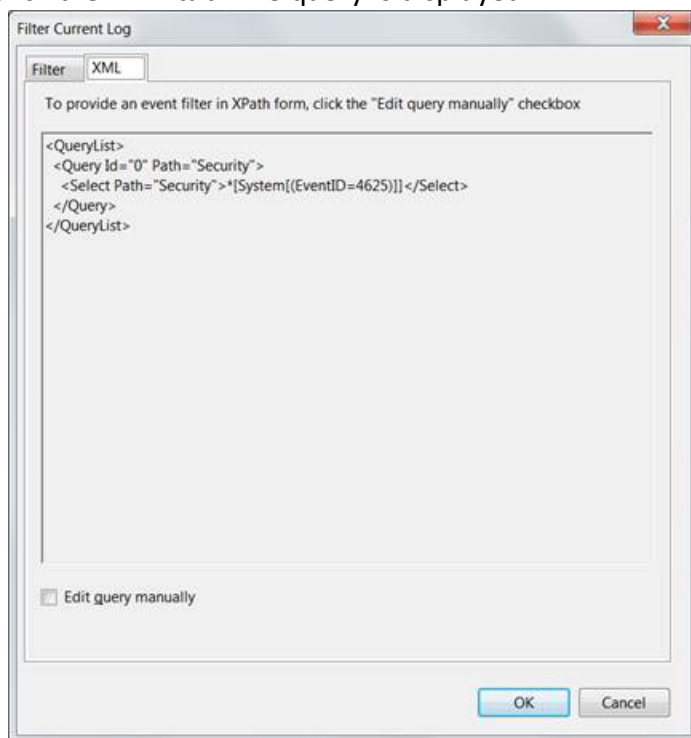
1. Click **Filter current log** to set the filter.



For example, to collect the logon failure events whose Event ID is 4625, enter the Event ID number as shown in the following figure.



2. Click the **XML** tab. The query is displayed in XML.



The expression that appears between `<Select>` and `</Select>` is the value that can be entered in the filter. Here it writes `*[System[(EventID=4625)]]`. This can be copied to the **Filter** column in the host table parameter for the desired event log.



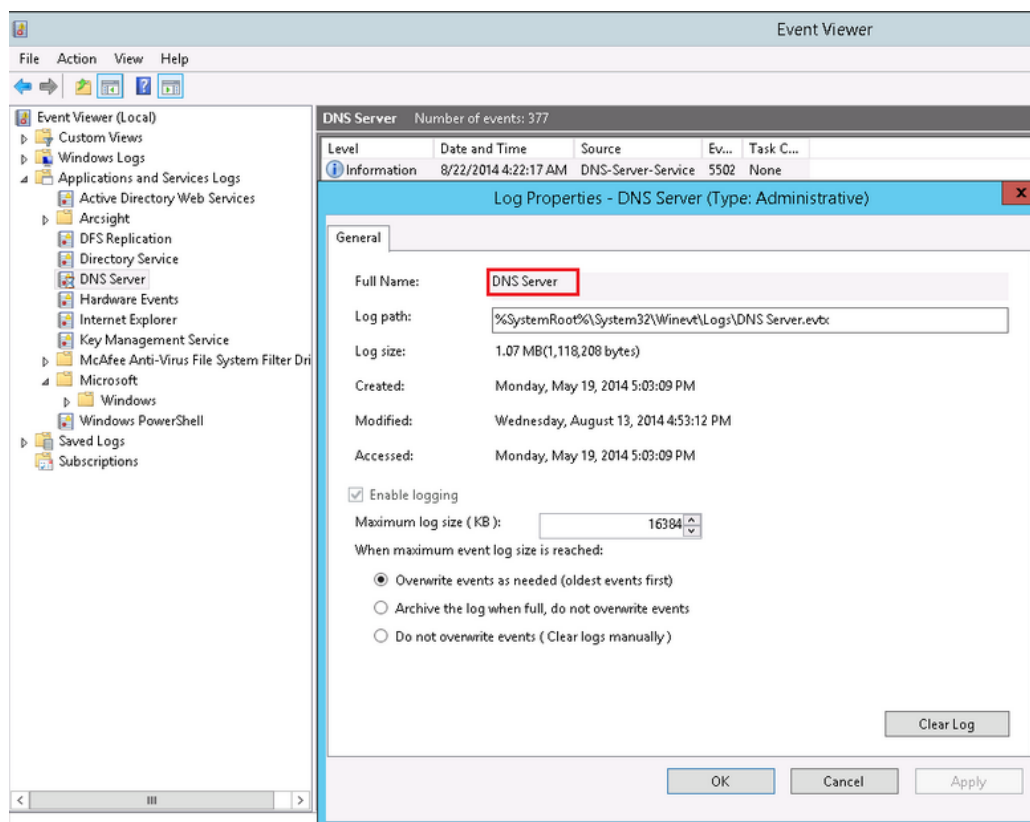
Note: In certain cases, the text cannot be directly copied to the Filter column in the UI wizard. If the filter text contains "gt;", "lt;", "gt;=" or "lt;=" , you must replace it with ">","<",">=" or "<=" respectively.

Specifying Custom Log Names

In the Windows Host parameters window, a column for the **Custom Log Names** parameter lets you specify names of custom event logs. Applications also can generate events for a custom application event log, such as DNS Server, Directory Service, Exchange Auditing, and so on. (Parsing support for only the event header is supported for application events.)

For example, specify `Directory Service` for Active Directory and `Exchange Auditing` for Microsoft Exchange Audit. For Microsoft Windows Print Service Admin log, use `Microsoft-Windows-PrintService/Admin`.

To identify the Custom Event Log Name, select the **Custom Application Event Log** in the Microsoft Windows **Event Viewer**. The log name can be found from the properties of the event log in the **Full Name** field, as shown in the following figure.



For more information about setting this parameter, see [“Advanced Configuration Parameters per Host.”](#)

Configuring the Host Browsing Thread Sleep Time

If you selected **Use Active Directory for OS version** to specify the Windows OS version for the hosts from which you want to collect eventSelect this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information.

Newly discovered hosts are added to the lookup automatically without having to reconfigure the connector itself. Active Directory information is verified every time the connector starts and every 24 hours (86400000 milliseconds).

To change the time setting:

1. Open the `agent.properties` file in `$ARCSIGHT_HOME/current/agent`
2. Set the **hostbrowsingthreadsleeptime** parameter to the number of milliseconds between host browsing queries. This value must be greater than 0. If the value is set to 0, then it does not perform periodic host browsing.

Creating a Source Hosts File

During connector configuration, if **File as Source for OS Version** is selected, then create a source host file in .csv format with the host name and Windows OS version, and upload the file during the connector configuration.



Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the **WEF Source Hosts File Name** field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

```
hostsa.domaina.com,Windows 7
hostsb.domainb.com,Windows 8
hostsc.domainb.com,Windows Server 2012
Hostsd.domaind.com,Windows Server 2016
```

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

```
Windows Vista
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows 7
Windows 8
Windows 10
```



Note: OS version information is optional; events may still be parsed in a majority of cases.

After the configuration, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Collecting Events from the Event Log

To set up the connector to collect application events:

1. From `$ARCSIGHT_HOME\current\bin`, double-click **runagentsetup.bat**.
2. Select **Modify Connector** on the window displayed and click **Next**.
3. Select **Modify connector parameters** and click **Next**.
4. Select **Navigate to the Modify table parameters** window.
5. To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Directory Service** in the **Custom Log Names** field.

You can specify multiple Custom Log Names in a comma-separated format; for example:

Directory Service, Exchange Auditing

6. Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
7. Select **Exit** and click **Next** to exit the configuration wizard.
8. Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Native*.

Configure Advanced Options

This section documents some of the advanced configuration parameters available with this connector. The table following the procedure for accessing advanced configuration parameters details the parameters you may choose to adjust, depending upon the needs of your enterprise.

Access Advanced Parameters

After SmartConnector installation, you can edit the `agent.properties` file to modify parameters. This file can be found at `$ARCSIGHT_HOME\current\user\agent`.

Advanced Container Configuration Properties

Specify	Parameter	Default
The protocol used between the connector and the collector. Currently supports TCP protocol.	<code>mq.transport.protocol</code>	<code>tcp</code>
The port used between the connector and the collector. The specified port will be bound during the connector installation. If more than one connector is to be installed on the same host, configure this with an unused port number.	<code>mq.server.listener.port</code>	<code>61616</code>
The maximum disk size (in Kilobytes) to be used for message persistence by the MQ component.	<code>mq.persistent.storage.limit</code>	<code>409600</code>
The maximum memory size (in Kilobytes) to be used by the MQ component.	<code>mq.memory.limit</code>	<code>65536</code>
The frequency to clean up the processed messages from persistent store in milliseconds. The storage needs to be cleaned up in order to receive more messages from winc-agent.	<code>mq.persistent.storage.cleanup.interval</code>	<code>10000</code>
The number of messages, event batches to preload in memory. Received messages from the winc-agent are persisted into the memory store, but it has to be loaded into the memory for processing. Preloading reduces the waiting time for the data loading and helps with performance.	<code>mq.consumer.prefetch.size</code>	<code>80</code>
Whether the SID translation is required or not. The SID should be present in the remote host. Note: There may be a slight performance hit when being used.	<code>winc.winc-agent.enableSidTranslation</code>	<code>True</code>
This property enables disk space check.	<code>mq.enable.space.check</code>	<code>True</code>
Time interval to check if the persist storage is more than 70%.	<code>mq.storage.check.interval</code>	<code>10</code>

Specify	Parameter	Default
If the activemq persist storage usage is greater than 70%, the space increases. The modified storage limit is updated in <code>agent.properties</code> .	<code>mq.max.percentage.used</code>	70
Maximum allocated divisions in the disk space.	<code>mq.max.disk.allocation</code>	50
If the mq persist store usage is less than 30%, the space decreases. The mq persist storage space should not be less than 409600 (default). The modified storage limit is updated in <code>agent.properties</code> .	<code>mq.min.percentage.used</code>	30

Advanced Common Configuration Parameters

Specify	Parameter	Default
Thread count for event processing threads dedicated for a single collector.	<code>eventprocessthreadcount</code>	10
The queue size used to hold the ready to execute event processing task to improve performance. Larger queue length means bigger memory footprint and it does not necessarily help with performance improvement, as a limited number of threads are available for processing.	<code>Executequeuelength</code>	100
By default the statistics are calculated every 10 minutes and dumped into both the <code>agent.log</code> and to the <code>EventStats</code> report file in <code>user/agent/agentdata</code> . This interval governs how often stats are calculated. Stats include average per last interval for events per second.	<code>pdastatsinterval</code>	600000ms
Whether to preserve the last ID processed before connector terminated or device went down.	<code>preservestate</code>	true
Event count before writing the preserve state.	<code>preservedstatecount</code>	100
Time interval in ms before writing the preserve state.	<code>preservedstateinterval</code>	10000

Advanced Configuration Parameters per Host

Specify	Parameter	Default
Whether to get the real-time events or read from the beginning of the event logs	startatend	true
To collect application events from custom application event logs, provide a comma separated list of the custom application event logs. Workgroup hosts have their separate shared SID cache.	eventlogtypes	null

Advanced Configuration Parameters for SID and GUID Translation

Specify	Parameter	Default
To enable GUID translation	enableguidtranslation	false
Size of the cache to store the GUIDs and their translated values	guidcachesize	50000
Time-to-live in ms for the GUID entries in the caches	guidcachetimetolive	600000
Interval in milliseconds (ms) at which the SID and GUID entries are to be expired from the caches	sidguidcacheexpirationthreadsleeptime	600000
Interval in ms at which the SID and GUID caches are persisted to disk files. Each domain's SID cache is persisted to a separate disk file. The SID cache for workgroup hosts is persisted to a separate shared disk file.	sidguidcachepersistencethreadsleeptime	600000

Customizing Event Source Mapping

The Windows Event Log – Native application/system event parser loading mechanism relies on the event source for each event and attempts to load a parser with the following name convention:

```
<Channel>\<ProviderName>.sdkkeyvaluefilereader.properties
```

This convention works in the vast majority of cases but sometimes the parser needs more flexibility. In these cases, you can customize where to find these parsers by redirecting the

variables `Channel` and `ProviderName`. For even more flexibility, the input `ProviderName` can be matched against a regular expression to avoid duplicate entries with minimal changes.

Creating an Override Map File

1. Navigate to `$ARCSIGHT_HOME/current/user/agent/fcp/winc/core_maps` and create an override map file with the name `customeventsource.map.csv` including the following columns:

```
SourceChannel
SourceProviderNamePattern
TargetProviderName
TargetChannel
```

The `SourceProviderNamePattern` value can be a string or a regular expression.

2. If there is no `winc/coremaps` subdirectory at `$ARCSIGHT_HOME/current/user/agent/fcp`, create one.
3. The last field `TargetChannel` is optional and, if empty, will be understood as the same as `SourceChannel`.

Customizing Event Parsing in a Clustered Environment

The default parser filename convention can cause problems in clustered environments, where the same event from different clusters can have different customized provider names. For example, SQL Server application events have the `ProviderName` `MSSQLSERVER`, resulting in a parser name of `application\mssqlserver.sdkkeyvaluefilereader.properties`.

In a clustered SQL Server environment, you can customize and configure the provider name for each cluster as `SQLSERVER01`, `SQLSERVER02`, and so forth. However, if the connector expects `MSSQLSERVER` as the provider name, the parsing fails for events with customized provider names, if the different providers have different names

To avoid this outcome, you can map all these different providers into one provider name value using the map file `$ARCSIGHT_HOME/user/agent/fcp/winc/core_maps/customeventsource.map.csv`.

The following are example entries based for a clustered environment:

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
Application, MSSQLSERVER.*, MSSQLSERVER, Application
```

The following are contents of a sample `customeventsource.map.csv` file with two entries:

```
#SourceChannel, SourceProviderNamePattern, TargetProviderName,
System,      Service.*,      service_control_manager,
Application, MSSQLSERVER.*,  MSSQLSERVER,
```

Creating Custom Parsers for System and Application Events

The SmartConnector provides complete parsing of both the Windows event header and event description for all security events and some system events.

For all system and application events, the connector provides complete parsing of the Windows event header. Also, the connector provides a framework to create and deploy your own parsers to parse the event description. Such a parser can parse events specific to a Channel and ProviderName.

- When collecting events from system event logs (such as NTServicePack, Service Control Manager, WINS), select **System** for **Windows Log type**.
- When collecting events from application event logs (such as Microsoft Forefront Protection 2010 for Exchange, Microsoft SQL Server Audit), select **Application** for **Windows Log type**.



Note: Custom Parsers or overrides you create are customizations. These are not certified for use through the ArcSight Quality Assurance Life Cycle of Testing. These are to be developed, tested, and maintained by the creator of the Custom Parser or override.

Before Creating a Parser

Complete the following steps before creating a parser:

1. Generate the system or application events of interest.
2. Configure the connector to collect the system or application events and preserve the raw events.
3. Run the connector to collect the system or application events and to generate the ArcSight raw events. The raw events will contain key-value pairs in JSON format. Using these generated raw events, see ["Create and Deploy Your Own Parser"](#) to map the values of these keys to the ArcSight event schema fields by creating a parser file.



Note: Not all raw events will have key-value pairs in the event body. Such events do not require that you create a parser to map anything to the ArcSight event schema fields. But you can still choose to create a parser to map the event name or description for such events.

Creating and Deploying Your Own Parser

To create and deploy your own parser:

1. Navigate to the directory location to deploy the parser file:

```
$ARCSIGHT_HOME\user\agent\fc\winc
```

2. Identify the Channel for the events that need to be parsed (for example: System, Application, Directory Service, DNS Server, Key Management Service, and so on).
3. Identify the provider name of the events that need to be parsed, as events collected from a single channel can be generated by multiple provider names. For example, events collected from Channel: System can be generated by ProviderName: Service Control Manager, WINS, and so on.
4. Identify the SectionName of the event body that needs to be parsed, such as EventData, UserData, and so on.
 - a. To parse the EventData section of the event body, create a key value parser file with the following naming convention, in the directory location identified in **Step 1**.

```
\{Normalized Channel}\{Normalized ProviderName}.sdkkeyvaluefilereader.  
properties
```

For example, the key-value parser file name for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: EventData

will be:

```
\security\microsoft_windows_eventlog.sdkkeyvaluefilereader.properties
```

- b. To parse the other sections of the event body, such as UserData, create a JSON parser file with the following naming convention, in the directory location identified in **Step 1**.

```
\{Normalized Channel}\{Normalized ProviderName}.{Normalized  
SectionName}.jsonparser.properties
```

For example, the key-value parser file name for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

will be:


```
\security\microsoft_windows_eventlog.userdata.jsonparser.properties
```



Note: Normalize the Channel, ProviderName, and SectionName values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the Locale and Encoding values.

5. Create mappings in these parsers as per your requirements by using conditional mappings based upon the ArcSight externalId field, which is already mapped to the Windows Event ID.

Because the connector already maps the Windows event header fields to ArcSight event fields as previously mentioned, those mappings need not be re-defined (unless you need to override the mapping values). The only mappings required are for mapping the specific event description.

- a. The following event header key-value parser can be used as a reference for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: EventData

to map the event name fields:

```
key.delimiter=&&
key.value.delimiter==
key.regex=([^\&=]+)

event.deviceVendor=__getVendor("Microsoft")

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=2

# The event logging service has shut down.
conditionalmap[0].mappings[0].values=1100
conditionalmap[0].mappings[0].event.flexString1=
conditionalmap[0].mappings[0].event.name=__stringConstant("The event
logging service has shut down.")

# The security log is now full.
conditionalmap[0].mappings[1].values=1104
conditionalmap[0].mappings[1].event.flexString1=
conditionalmap[0].mappings[1].event.name=__stringConstant("The security
log is now full.")
```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

- b. The `UserData` section from following sample JSON parser can be used as a reference:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

Sample `UserData` section:

```
{
  "UserData": {
    "LogFileCleared":
      "@xmlns:auto-ns3":
"http://schemas.microsoft.com/win/2004/08/events",
      "@_xmlns_":
http://manifests.microsoft.com/win/2004/08/windows/eventlog",
      "SubjectUserSid": "S-1-5-18",
      "SubjectUserName": "SYSTEM",
      "SubjectDomainName": "NT AUTHORITY",
      "SubjectLogonId": "0x3e7"
    }
  }
}
```

- c. The following `EventBody` JSON parser can be used as a reference:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

Sample `EventBody` section:

```
trigger.node.location=/UserData
event.deviceVendor=__getVendor("Microsoft")
token.count=7
token[0].name=SubjectUserSid
token[0].location=LogFileCleared/SubjectUserSid
token[0].type=String

token[1].name=SubjectUserName
token[1].location=LogFileCleared/SubjectUserName
token[1].type=String

token[2].name=SubjectDomainName
token[2].location=LogFileCleared/SubjectDomainName
```

```

token[2].type=String

token[3].name=SubjectLogonId
token[3].location=LogFileCleared/SubjectLogonId
token[3].type=String

token[4].name=Reason
token[4].location=AuditEventsDropped/Reason
token[4].type=String

token[5].name=Channel
token[5].location=AutoBackup/Channel
token[5].type=String

token[6].name=BackupPath
token[6].location=AutoBackup/BackupPath
token[6].type=String

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=1101
conditionalmap[0].mappings[0].event.name=__stringConstant("Audit events
have been dropped by the transport. The real time backup file was
corrupt due to improper shutdown.")
conditionalmap[0].mappings[0].event.deviceCustomNumber3=__safeToLong
(Reason)
conditionalmap[0].mappings[0].event.deviceCustomNumber3Label=__
stringConstant("Reason Code")

conditionalmap[0].mappings[1].values=1102
conditionalmap[0].mappings
[1].event.destinationNtDomain=SubjectDomainName
conditionalmap[0].mappings[1].event.destinationUserName=__extractNTUser
(__oneOf(SubjectUserName,SubjectUserSid))
conditionalmap[0].mappings[1].event.destinationUserId=SubjectLogonId
conditionalmap[0].mappings[1].event.name=__stringConstant("The audit
log was cleared.")

conditionalmap[0].mappings[2].values=1105
conditionalmap[0].mappings[2].event.fileType=Channel
conditionalmap[0].mappings[2].event.fileName=BackupPath
conditionalmap[0].mappings[2].event.name=__stringConstant("Event log
automatic backup")

```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

6. Start the connector.

Verify categorization of new events to see if additional categorization are required. For information about categorization, see the Technical Note *ArcSight Categorization: A Technical Perspective* available from the Micro Focus Software Support site. For more information about creating parsers, see the *ArcSight FlexConnector Developer's Guide*, available from the Micro Focus [Software Support](#) and the [Micro Focus Security Community](#).

Customizing Localization Support for the Native Connector

ArcSight SmartConnectors provide the event collection layer for ArcSight SIEM. Therefore, in the context of SmartConnectors, localization is related to the collection, parsing, and normalization of event messages that are generated by localized events and written in non-English languages. Localization (L10 N) is the process of converting a program to run in a particular locale or country, which includes displaying all the text and translating the user interface into the native language.

To add location support beyond that provided by ArcSight, complete the following these steps.

1. Identify the Channel, ProviderName, locale, and encoding of the event for which you want to localize the event data.
2. Configure the host table parameters with the appropriate locale and encoding parameter values identified in step 1.

```
agents[x].windowshoststable[y].locale=<Locale>
agents[x].windowshoststable[y].encoding=<Encoding>
```

where x is the index of the connector and y is the index of hosts in the connector configuration.

Example:

```
agents[0].windowshoststable[0].locale=de_DE
agents[0].windowshoststable[0].encoding=UTF-8
```

3. To add support for locales and encodings not shown in the connector host table configuration selections, change the Locale and Encoding values of the following lines in the agent.properties file (which can be found at \$ARCSIGHT_HOME\current\user\agent):
4. Enter the type of character set encoding of the events in the log file, for example event.name. Create your content relative to this location: \$ARCSIGHT_

HOME\user\agent\fcg\winc\.

5. Identify the parser from which you want to invoke the localization extra-processor map file.

```
$ARCSIGHT_HOME\user\agent\winc\<<NormalizedChannel>\
  <NormalizedProviderName>.sdkkeyvaluefilereader.properties
```

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\
  microsoft_windows_security_auditing.sdkkeyvaluefilereader.properties
```



Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

6. For each locale and encoding combination, declare an extra-processor map file within this parser.

```
extraprocessor[4].type=map
extraprocessor
[4].filename=winc/<NormalizedChannel>/<NormalizedProviderName.
  <Locale>.<Encoding>.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype>equals
extraprocessor[4].conditionvalues=<Locale>|<Encoding>
extraprocessor[4].charencoding=<Encoding>
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

Example:

```
extraprocessor[4].type=map
extraprocessor[4].filename=winc/security/
  microsoft_windows_security_auditing.fr_CA.UTF-8.110n.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype>equals
extraprocessor[4].conditionvalues=fr_CA|UTF-8
extraprocessor[4].charencoding=UTF-8
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

7. Create the L10N extra-processor map file:

```
$ARCSIGHT_HOME\user\agent\winc\<<NormalizedChannel>\
<NormalizedProviderName>.<Locale>.<Encoding>.l10n.map.csv
```



Note: When creating, editing, or saving the L10N extra-processor map file, don't use an application with a default of **ASCII**, **UTF-8**, or other generic encoding. Create the file on the localized device or in a localized editor, and be sure that the encoding isn't overwritten when you save it.

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\
microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
```



Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

8. Within this file, declare the getters and setters, and add all the localization content. Use the event.externalId field as the getter, and the field that you want to localize as the setter. A sample file is shown for French:

```
event.externalId,set.event.name
"4886","Les services de certificats ont reçu une demande de certificat."
"4887","Les services de certificats ont approuvé une demande de
certificat et émis un certificat."
"4884","Les services de certificats ont importé un certificat dans sa
base de données."
"4885","Le filtre d'audit des services de certificats modifié."
"4882","Les autorisations de sécurité pour les services de certificats
ont été modifiées."
"4883","Les services de certificats ont récupéré une clé archivée."
"4880","Les services de certificats ont démarré."
"4881","Les services de certificats se sont arrêtés."
...
...
```



Note: Additional mapping can be set from ESM. Go to your ESM Console and run **Get Additional Data**. The command can only collect additional data from supported sources. Unsupported sources collect additional data from the event header.

Troubleshooting

This section has the following information:

Parameters not functioning as expected

Symptom: The **RenameFileInTheSameDirectory** and **DeleteFile** parameters are not functioning as expected.

Solution: The **usenonlockingwindowsfilereader** parameter must be set to **true** in Windows environments for the **RenameFileInTheSameDirectory** and **DeleteFile** parameters to work as expected.

Log message for resource adjustment

Symptom: While the connector is starting, it logs that the temporary store will be downsized.

```
2015-01-26 15:11:17,668][ERROR]
[default.org.apache.activemq.broker.BrokerService]
[external] Temporary Store limit is 51200 mb, whilst the temporary data
directory: C:\arcsight\SmartConnectors\current\activemq-data\localhost\tmp_
storage only has
47568 mb of usable space - resetting to maximum available 47568 mb.
```

Solution: This message indicates that the system disk space is low. Although this may not cause an immediate impact, check for adequate disk storage to ensure it does not run out while running the connector. To avoid this log message, make sure the system has 50 GB of disk space available.

A Non-administrator User Is Unable to Run Windows Native Connector and the Log File Has Permission Error

Issue: If any user other than administrator tries to run Windows Native connector, it does not run and the log file shows the following error:

```
[FATAL][default.com.arcsight.agent.am.e][init] Could not initialize the
Obfuscation key manager
[FATAL][default.com.arcsight.agent.am.e][init]
com.arcsight.common.config.n: An error occurred in configuration. Unable to
load properties from file '<install
path>\current\user\agent\keys\obfuscationkey'.
```

Error was: '<install path>\current\user\agent\keys\obfuscationkey (Access is denied)'

Solution: This issue occurs because only the administrators are authorized to access <install path>\current\user\agent\agent.properties and <install path>\current\user\agent\keys\obfuscationkey in the SmartConnector 7.15.0 or later.

For a non-administrator user to run this connector, change the owner of the **agent.properties** and **obfuscationkey** files to a corresponding user with the **Full control** permission. If there are more than one users who need permission to run the connector, add these users in the same group so that the owner of the **agent.properties** and **obfuscationkey** files can be assigned to this group.

Windows Common Security Mappings

The following security event mappings generally apply to all Windows Server 2012, Windows Server 2016, and Windows 10 Windows Event Log Security Events.

Micro Focus ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Error or Warning; Low when Device Severity = Information or Audit_success
Destination Host Name	One of (Target Server Name, Computer Name, Target Server:Target Server Name)
Destination NT Domain	One of (Domain Name, Subject:Account Domain, New Token Information:Account Domain, Subject:Domain Name)
Destination Port	Network Information:Destination Port
Destination Process Name	One of (Process Information:New Process Name, Process Information:Process Name)
Destination Service Name	Service Information:Service Name
Destination User ID	One of (Subject:Logon ID, New Token Information:Logon ID)
Destination User Name	One of (Account Name, Subject:Account Name, Subject:Security ID, User, New Token Information:Account Name)
Destination User Privileges	One of (Additional Information:Privileges, New Right:User Right, Removed Right:User Right, Access Granted:Access Right, Access Removed:Access Right)
Device Action	One of (Account Action, Allowed, 'No', 'Blocked')
Device Custom IPv6 Address 2	Source IPv6 Address

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Logon Type
Device Custom Number 2	Value of CrashOnAuditFail
Device Custom Number 3	Count
Device Custom String 1	One of (Access Request Information:Access Mask, Operation:Accesses, Operation:Access Mask)
Device Custom String 2	EventCategory
Device Custom String 4	One of (Error Code, Additional Information:Failure Code, Additional Information:Reason Code, Additional Information:Error Code, Failure Information:Failure Reason, Audit Events Dropped:Reason, Reason, Reason for Rejection, Error Information:Reason, Error Information:Error, Process Information:Exit Status)
Device Custom String 5	One of (Authentication Package Name, Authentication Package, Authentication, Detailed Authentication Information:authentication Package)
Device Event Category	Event logType
Device Event Class ID	Both (Event Source , Event ID)
Device Host Name	Computer Name
Device NT Domain	One of (Domain Name, Subject:Account Domain)
Device Product	'Microsoft Windows'
Device Receipt Time	DetectTime
Device Severity	EventType
Device Vendor	'Microsoft'
External ID	Event ID
File ID	One of (Object Handle ID, Object:Object Handle)
File Name	Object:Object Name
File Type	One of (Object Type, Object:Object Type)
Message	Message
Name	Description
Source Address	One of (Network Information:Source Network Address, Local Network Address, Additional Information:Client Address)
Source Host Name	One of (Subject:Client Name, Network Information:Workstation Name, Source Workstation, Additional Information:Client Name)

Micro Focus ArcSight ESM Field	Device-Specific Field
Source NT Domain	Subject:Client Domain
Source Port	One of (Network Information:Source Port, Network Information:Port, Network Information:Client Port)
Source Process Name	One of (Logon Process Name, process Information:Caller Process ID)

Specific Windows Security Event Mappings

Event Id 1100

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The event logging service has shut down.'

Event Id 1101

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Audit events have been dropped by the transport. The real time backup file was corrupt due to improper shutdown.'
Device Custom Number 3	Reason

Event Id 1102

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The audit log was cleared.'
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination User ID	SubjectLogonId

Event Id 1104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The security log is now full.'

Event Id 1105

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Event log automatic backup.'
File Type	Channel
File Name	BackupPath

Event Id 1074

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	The process has initiated the shutdown/restart of computer.
Message	concatenate(The process "%1," has initiated the "%5," of computer "%2," on behalf of user "%7," for the following reason: "%3")
Source Process Name	%1
Destination Host Name	%2
Reason	%3
Device Custom String4	Reason Code
Device Custom String5	Shutdown Type
Device Custom String6	Comment

Event Id 4608

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.'

Event Id 4609

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows is shutting down. All logon sessions will be terminated by this shut down.'

Event Id 4610

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.'
Device Custom String 5	AuthenticationPackageName

Event Id 4611

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A trusted logon process has been registered with the Local Security Authority. This logon process will be trusted to submit logon requests.'
Destination Process Name	LogonProcessName
Source Process Name	LogonProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4612

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.'
Device Custom Number 3	AuditsDiscarded
Message	'This event is generated when audit queues are filled and events must be discarded. This most commonly occurs when security events are being generated faster than they are being written to disk, or when the auditing system loses connectivity to the event log, such as when the event log service is stopped.'

Event Id 4614

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes.'
Device Custom String 5	'NotificationPackageName'

Event Id 4615

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Invalid use of LPC port.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'Windows Local Security Authority (LSA) communicates with the Windows kernel using Local Procedure Call (LPC) ports. If you see this event, an application has inadvertently or intentionally accessed this port which is reserved exclusively for LSA's use. The application (process) should be investigated to ensure that it is not attempting to tamper with this communications channel.'

Event Id 4616

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The system time was changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom Date 1	Both (PreviousDate, PreviousTime)
Device Custom Date 2	Both (NewDate, NewTime)

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 3	ProcessId
Destination process Name	ProcessName
Message	'This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.'

Event Id 4618

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A monitored security event pattern has occurred.'
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetUserDomain
Device NT Domain	TargetUserDomain
Message	'This event is generated when Windows is configured to generate alerts in accordance with the Common Criteria Security Audit Analysis requirements (FAU_SAA) and an auditable event pattern occurs.'

Event Id 4621

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.'
Device Custom Number 2	CrashOnAuditFail value.
Message	'This event is logged after a system reboots following CarshOnAuditFail.'

Event Id 4622

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security package has been loaded by the Local Security Authority.'
File Path	SecurityPackageName
Device Custom String 5	SecurityPackageName

Event Id 4624

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An account was successfully logged on.'
Additional data	TargetOutboundUserName
Additional data	TargetOutboundDomainName
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination Process Name	ProcessName
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom String 1	ImpersonationLevel
Device Custom String 3	ProcessId
Device Custom String 4	RestrictedAdminMode
Device Process Name	LogonProcessName
Device Custom String 6	LogonGuid
Source Host Name	One of (IpAddress, 'localhost')
Source Port	IpPort
Device Custom String 5	AuthenticationPackageName
Device Custom Number 1	LogonType
File Type	VirtualAccount

Micro Focus ArcSight ESM Field	Device-Specific Field
File ID	TargetLinkedLogonId
File Name	ElevatedToken
Message	'This event is generated when a logon session is created. It is generated on the computer that was accessed.'

Event Id 4625

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An account failed to log on.'
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Destination Process Name	ProcessName
Destination NT Domain	TargetDomainName
Device Custom String 1	SubStatus
Device Custom String 3	ProcessId
Reason	FailureReason
Device Process Name	LogonProcessName
Destination User ID	' '
Source Host Name	WorkstationName
Source Port	IpPort
Source Process Name	ProcessId
Device Custom String 4	FailureReason
Device Custom String 5	AuthenticationPackageName

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	LogonType
Destination UserName	TargetUserName
Message	<p>'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'

Event Id 4626

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'User/Device claims information.'
Device NT Domain	SubjectDomainName
Destination User Name	TargetUserName
Destination User ID	TargetLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Device Custom Number 1	LogonType
Message	<p>'The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit User/Device claims subcategory is configured and the user's logon token contains user/device claims information. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.'</p>

Event Id 4627

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Group membership information.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom Number 1	LogonType
Device Custom Number 2	EventIdx

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	EventCountTotal
Device Custom String 1	GroupMembership
Message	<p>'This event is generated when the Audit Group Membership subcategory is configured. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.'</p>

Event Id 4634

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An account was logged off.'
Destination User ID	TargetLogonId
Device Custom Number 1	LogonType
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName
Message	<p>'This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.'</p>

Event Id 4646

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IKE DoS-prevention mode started.'

Event Id 4647

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'User initiated logoff.'
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName
Message	'This event is generated when a logoff is initiated but the token reference count is not zero and the logon session cannot be destroyed. No further user-initiated activity can occur. This event can be interpreted as a logoff event.'

Event Id 4648

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A logon was attempted using explicit credentials.'
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Destination Process Name	ProcessName
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device Custom String 6	TargetLogonGuid (Logon GUID)
Device Custom String 3	ProcessId (Process ID)
Source Port	IpPort
Destination User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Message	'This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.'
Device Custom String 5	TargetServerName

Event Id 4649

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A replay attack was detected.'
Source Host Name	WorkstationName
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Device Custom String 5	AuthenticationPackage
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.'

Event Id 4650

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.'

Event Id 4651

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

Event Id4652

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason

Event Id4653

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason

Event Id 4654

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalPort
Destination Address	RemoteAddress
Destination Port	RemotePort
Message	FailureReason

Event Id 4655

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association ended.'
Source Address	LocalAddress

Event Id 4656

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 3	ProcessId
Device Custom String 1	AccessList
Device NT Domain	SubjectDomainName
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Privileges	PrivilegeList
File ID	HandleId
File Name	ObjectName
File Type	ObjectType

Event Id 4657

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A registry value was modified.'
Device Custom String 6	ObjectValueName
Device Action	OperationType
Old File Type	OldValueType
Device Custom String 4	OldValue
File Type	NewValueType

Micro Focus ArcSight ESM Field	Device-Specific Field
File ID	HandleId
File Name	ObjectName
Device Custom String 5	NewValue
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4658

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The handle to an object was closed.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4659

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested with intent to delete.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId

Micro Focus ArcSight ESM Field	Device-Specific Field
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4660

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An object was detected.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4661

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested.'
Device Custom String 1	AccessList
Destination User Privileges	PrivilegeList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4662

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 1	One of (AccessList, AccessMask)
Device Custom String 5	ObjectType
Device Custom String 6	Properties
Device NT Domain	SubjectDomainName
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Name	'An operation was performed on an object.'

Event Id 4663

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to access an object.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)

Event Id 4664

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to create a hard link.'
Destination User ID	SubjectLogonId
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4665

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to create an application client context.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

Event Id 4666

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An application attempted an operation.'
File Name	ObjectName

Event Id 4667

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An application client context was deleted.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

Event Id 4668

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An application was initialized.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

Event Id 4670

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Permissions on an object were changed.'
Device Custom String 4	OldSd
Device Custom String 5	NewSd
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Name	ObjectName

Event Id 4671

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An application attempted to access a blocked ordinal through the TBS.'
Destination User ID	CallerLogonId
Destination User Name	One of (CallerUserName, CallerUserSid)
Destination NT Domain	CallerDomainName
Device NT Domain	CallerDomainName

Event Id 4672

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Special privileges assigned to new logon.'
Destination User privileges	PrivilegeList
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4673

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A privileged service was called.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination Process Name	ProcessName

Event Id 4674

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An operation was attempted on a privileged object.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Privileges	PrivilegeList
Device Custom String 3	ProcessId
File ID	HandleId

Event Id 4675

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'SIDs were filtered.'

Event Id 4688

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A new process has been created.'
Destination User Name	One of (SubjectUserName, SubjectUserSid, TargetUserName, TargetUserSid)
Destination NT Domain	One of (SubjectDomainName, desinationNtDomain)
Destination User ID	One of (SubjectLogonId, TargetLogonId)
Device Custom String 1	MandatoryLabel
Device Custom String 3	NewProcessId
Device Custom String 6	TokenElevationType
Device Custom String 5	ProcessId
Device Custom String 4	CommandLine
Destination Process Name	NewProcessName
Device NT Domain	SubjectDomainName
File Path	ParentProcessName
Message	'Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.Type 1 is a full token with no privileges removed or groups disabled. Type 2 is an elevated token with no privileges removed or groups disabled.Type 3 is a limited token with administrative privileges removed and administrative groups disabled.'

Event Id 4689

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A process has exited.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Device Custom String 4	Status
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4690

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to duplicate a handle to an object.'
Old File ID	SourceHandleId
Device Custom String 5	SourceProcessId
File ID	TargetHandleId
Device Custom String 3	TargetProcessId
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4691

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Indirect access to an object was requested.'
Destination User ID	SubjectLogonId
Device Custom String 1	AccessMask

Micro Focus ArcSight ESM Field	Device-Specific Field
File Type	ObjectType
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4692

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Backup of data protection master key was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4693

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Recovery of data protection master key was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4694

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Protection of auditable protected data was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4695

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Unprotection of auditable protected data was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4696

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A primary token was assigned to process.'
Device Custom String 3	TargetProcessId
Destination Process Name	TargetProcessName
Device Custom String 5	ProcessId
Source Process Name	ProcessName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device NT Domain	SubjectDomainName

Event ID 4697

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A service was installed in the system.'
File Path	ServiceFileName
File Type	ServiceType

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 5	ServiceStartType
Device Custom String 6	ServiceAccount
Destination User ID	SubjectLogonId
Destination Service Name	ServiceName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4698

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was created.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4699

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was deleted.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4700

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was enabled.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4701

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was disabled.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4702

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was updated.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4703

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A token right was adjusted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Destination Process Name	ProcessName
Device Custom String 3	ProcessId
Device Custom String 1	EnabledPrivilegeList
Device Custom String 4	DisabledPrivilegeList
Message	'A token right was adjusted.'

Event Id 4704

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user right was assigned.'
Source User Name	One of (SubjectUserSid, SubjectUserName)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4705

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user right was removed.'
Source User Name	One of (SubjectUserSid, SubjectUserName)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4706

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A new trust was created to a domain.'
Device Custom String 6	One of (DomainName, DomainSid)
Device Custom String 5	TdoType (Trust Type)
Device Custom String 3	TdoDirection (Trust Direction)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4707

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A trust to a domain was removed.'
Device Custom String 6	One of (DomainName, DomainSid)
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4709

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services was started.'

Event Id 4710

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The IPsec Policy Agent service was disabled.'

Event Id 4711

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.'

Event Id 4712

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Policy Agent encountered a potentially serious failure.'

Event Id 4713

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Kerberos policy was changed.'
Message	All of ((KerberosPolicyChange, "", "(—' means no changes, otherwise each change is shown as: (Parameter Name): (new value) (old value))
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4714

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Data Recovery Agent group policy for Encrypting File System (EFS) has changed. The new changes have been applied.'
Message	All of (EfsPolicyChange, " ", "Changes Made('--' means no changes, otherwise each change is shown as:(Parameter Name): (new value) (old value))")
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4715

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The audit policy (SACL) on an object was changed.'
Device Custom String 6	NewSd
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4716

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Trusted domain information was modified.'
Device Custom String 6	One of (DomainName, DomainSid)

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 5	TdoType (Trust Type)
Device Custom String 3	TdoDirection (Trust Direction)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4717

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'System security access was granted to an account.'
Source User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	AccessGranted

Event Id 4718

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'System security access was removed from an account.'
Source User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	TargetSid
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	AccessRemoved

Event Id 4719

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'System audit policy was changed.'
Device Custom String 5	SubcategoryId
Device Custom String 6	CategoryId
Device Action	AuditPolicyChanges
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4720

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4722

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was enabled.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event Id 4723

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to change an account's password.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4724

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to reset an account's password.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName

Micro Focus ArcSight ESM Field	Device-Specific Field
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event Id 4725

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was disabled.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event Id 4726

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4727

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privilege	PrivilegeList

Event Id 4728

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4729

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4730

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4731

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4732

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4733

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4734

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4735

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4737

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4738

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device Custom String 4	OldUacValue (Old User Account Control Value)
Device Custom String 5	NewUacValue (New User Account Control Value)
Device Custom String 6	UserAccountControl (Change in User Account Control)
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4739

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Domain Policy was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination NT Domain	DomainName
Destination User Name	' '
Destination User ID	' '
Message	DomainPolicyChanged
Device Custom String 6	Changed Attributes
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4740

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was locked out.'
Destination User Name	TargetUserName
Source Host Name	TargetDomainName
Destination NT Domain	TargetSid
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event ID 4741

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A computer account was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4742

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A computer account was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	' '
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Device Custom Date1	PasswordLastSet
Device Custom Date1 Label	Password Last Set

Event ID 4743

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A computer account was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4744

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4745

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4746

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4747

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4748

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4749

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4750

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4751

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4752

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4753

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4754

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4755

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4756

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4757

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4758

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4759

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4760

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4761

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4762

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4763

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4764

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A group's type was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Device Custom String 5	GroupTypeChange
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4765

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'SID History was added to an account.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	SourceUserName
Destination User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4766

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt to add SID History to an account failed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	SourceUserName
Destination User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4767

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user account was unlocked.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event ID 4768

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos authentication ticket (TGT) was requested.'
Source Address	IpAddress

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 3	IpAddress (Client Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device Custom String 4	Status
Device Custom String 5	PreAuthType
Source Port	IpPort
Destination Service Name	ServiceName
Message	'Certificate information is only provided if a certificate was used for pre-authentication.Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.'

Event ID 4769

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was requested.'
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 3	IpAddress (Client Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination Service Name	ServiceName
Device Custom String 6	LogonGuid
Device Custom String 5	TicketEncryptionType ("Ticket Encryption Type")
Source Port	IpPort
Device Custom String 4	Status

Micro Focus ArcSight ESM Field	Device-Specific Field
Message	'This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.'
File Name	ServiceSid
Device Custom String 1	TicketOptions ("Ticket Options")

Event ID 4770

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was renewed.'
Device Custom String 3	IpAddress (Client Address)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination Service Name	ServiceName
Source Port	IpPort
Message	'Ticket options and encryption types are defined in RFC 4120.'

Event ID 4771

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Kerberos pre-authentication failed.'
Device Custom String 3	IpAddress (Client Address)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetSid
Destination Service Name	ServiceName

Micro Focus ArcSight ESM Field	Device-Specific Field
Reason	Status
Source Port	IpPort
Device Custom String 4	Status
Message	'Certificate information is only provided if a certificate was used for pre-authentication.Pre-authentication types, ticket options and failure codes are defined in RFC 4120.If the ticket was malformed or damaged during transit and could not be decrypted, then many fields in this event might not be present.'

Event ID 4772

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos authentication ticket request failed.'
Device Custom String 3	IpAddress (Client Address)
Source Port	IpPort
Destination Service Name	ServiceName
Device Custom String 4	FailureCode
Message	'Ticket options and failure codes are defined in RFC 4120.'

Event ID 4773

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket request failed.'
Device Custom String 3	IpAddress (Client Address)
Source Port	IpPort
Destination Service Name	ServiceName
Device Custom String 4	FailureCode
Message	'Ticket options and failure codes are defined in RFC 4120.'

Event ID 4774

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An account was mapped for logon.'
Destination User Name	MappedName
Device Custom String 5	One of (MappedName, MappingBy)

Event ID 4775

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An account could not be mapped for logon.'
Destination User Name	MappingBy
Device Custom String 5	ClientUserName

Event ID 4776

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The domain controller attempted to validate the credentials for an account.'
Destination User Name	TargetUserName
Reason	Status
Source Host Name	Workstation
Device Custom String 4	Status
Device Custom String 5	PackageName

Event ID 4777

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The domain controller failed to validate the credentials for an account.'
Destination User Name	TargetUserName

Micro Focus ArcSight ESM Field	Device-Specific Field
Source Host Name	Workstation
Device Custom String 4	Status
Device Custom String 5	ClientUserName

Event ID 4778

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A session was reconnected to a Window Station.'
Device Custom String 6	SessionName
Source Host Name	ClientName
Source Address	ClientAddress
Destination User ID	LogonID
Destination User Name	AccountName
Destination NT Domain	AccountDomain
Device NT Domain	Account Domain
Message	'This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching.'

Event ID 4779

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A session was disconnected from a Window Station.'
Device Custom String 6	SessionName
Source Host Name	ClientName
Source Address	ClientAddress
Destination User ID	LogonID
Destination User Name	AccountName
Destination NT Domain	AccountDomain
Device NT Domain	Account Domain
Message	'This event is generated when a user disconnects from an existing Terminal Services session, or when a user switches away from an existing desktop using Fast User Switching.'

Event ID 4780

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The ACL was set on accounts which are members of administrators group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'Every hour, the Windows domain controller that holds the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role compares the ACL on all security principal accounts (users, groups, and machine accounts) present for its domain in Active Directory and that are in administrative groups against the ACL on the AdminSDHolder object. If the ACL on the principal account differs from the ACL on the AdminSDHolder object, then the ACL on the principal account is reset to match the ACL on the AdminSDHolder object and this event is generated.'

Event ID 4781

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The name of an account was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	OldTargetUserName
Device Custom String 6	NewTargetUserName
Destination NT Domain	TargetDomainName

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4782

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The password hash account was accessed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

Event ID 4783

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4784

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4785

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4786

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4787

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A non-member was added to a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.'

Event ID 4788

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A non-member was removed from a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.'

Event ID 4789

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was deleted.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4790

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An LDAP query group was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4791

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4792

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An LDAP query group was deleted.'
Source User Name	SubjectUserName

Micro Focus ArcSight ESM Field	Device-Specific Field
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event ID 4793

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Password Policy Checking API was called.'
Source Host Name	Workstation
Source User Name	TargetUserName
Device Custom String 4	Stataus
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4794

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to set the Directory Services Restore Modeadministrator password.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4797

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to query the existence of a blank password for an account.'
Source Host Name	Workstation
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event ID 4798

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A user's local group membership was enumerated.'
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
File Name	CallerProcessId
File Path	CallerProcessName
Message	'A user's local group membership was enumerated.'

Event ID 4799

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group membership was enumerated.'
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName

Micro Focus ArcSight ESM Field	Device-Specific Field
Source User ID	SubjectLogonId
File Name	CallerProcessId
File Path	CallerProcessName
Message	'A security-enabled local group membership was enumerated.'

Event ID 4800

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The workstation was locked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

Event ID 4801

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The workstation was unlocked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

Event ID 4802

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The screen saver was invoked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

Event ID 4803

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The screen saver was dismissed.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

Event ID 4816

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'RPC detected an integrity violation while decrypting an incoming message.'

Event ID 4817

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Auditing settings on object were changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File Type	ObjectType
File Name	ObjectName

Event ID 4818

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Proposed Central Access Policy does not grant in the same access permissions as the current Central Access Policy.'
Destination Process ID	ProcessId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Type	ObjectType
File Name	ObjectName
Destination Process Name	ProcessName

Event ID 4819

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Central Access Policies on the machine have been changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File Type	ObjectType
Device NT Domain	SubjectDomainName

Event ID 4820

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos Ticket-granting ticket \\(TGT\\) was denied because the device does not meet the access control restrictions.'
Source User Name	TargetUserName
Source DNS Domain	TargetDomainName
Source User ID	TargetSid

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 5	ServiceSid
Device Custom String 1	All of (PreAuthType,, Status, TicketEncryptionType, TicketOptions)
Source Address	IpAddress
Device Custom String 4	All of (CertIssuerName,CertSerialNumber, CertThumbprint)
Device Custom String 3	SiloName
Device Custom String 6	PolicyName
Destination Service Name	ServiceName
Source Port	IpPort
Message	'Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.'

Event ID 4821

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.'
Source User Name	TargetUserName
Source DNS Domain	TargetDomainName
Destination Process ID	ServiceSid
Device Custom String 1	All of (Status, TicketEncryptionType, TicketOptions, TransitedServices)
Source Address	IpAddress
Source User ID	LogonGuid
Device Custom String 5	SiloName
Device Custom String 6	PolicyName
Source Port	IpPort

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Device Custom String 4	Status
Message	'This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.'

Event ID 4822

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'NTLM authentication failed because the account was a member of the Protected User group.'
Reason	Status
Device Custom String 4	Status
Destination User Name	AccountName

Event ID 4823

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'NTLM authentication failed because access control restrictions are required.'
Reason	Status
Device Custom String 5	SiloName
Device Custom String 6	PolicyName
Device Custom String 4	Status
Destination User Name	AccountName

Event ID 4824

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.'
Source User Name	TargetUserName
Source User ID	TargetSid
Device Custom String 1	All of (PreAuthType, Status, TicketOptions)
Source Address	IpAddress
Device Custom String 4	All of (CertIssuerName, CertSerialNumber, CertThumbprint)
Source Port	IpPort
Destination Service Name	ServiceName

Event ID 4826

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Boot Configuration Data loaded.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Message	'Boot Configuration Data loaded.'
Additional data	LoadOptions
Additional data	AdvancedOptions
Additional data	ConfigAccessPolicy
Additional data	RemoteEventLogging
Additional data	KernelDebug
Additional data	VsmLaunchType
Additional data	TestSigning
Additional data	FlightSigning
Additional data	DisableIntegrityChecks

Micro Focus ArcSight ESM Field	Device-Specific Field
Additional data	HypervisorLoadOptions
Additional data	HypervisorLaunchType
Additional data	HypervisorDebug

Event ID 4864

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A namespace collision was detected.'

Event ID 4865

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was added.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4866

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was removed.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event ID 4867

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was modified.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4868

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The certificate manager denied a pending certificate request.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4869

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a resubmitted certificate request.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4870

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services revoked a certificate.'
Destination User ID	SubjectLogonId
Device Custom String 4	RevocationReason
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4871

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to publish the certificate revocation list (CRL).'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4872

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to publish the certificate revocation list (CRL).'

Event Id 4873

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A certificate request extension changed.'
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4874

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'One or more certificate request attributes changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4875

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to shutdown.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4876

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services backup started.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4877

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services backup completed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4878

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services restore started.'

Event Id 4879

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services restore completed.'

Event Id 4880

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services started.'

Event Id 4881

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services stopped.'

Event Id 4882

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The security permissions for Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4883

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services retrieved an archived key.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4884

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services imported a certificate into its database.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4885

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The audit filter for Certificate Services changed.'
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4886

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a certificate request.'

Event Id 4887

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services approved a certificate request and issued a certificate.'

Event Id 4888

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services denied a certificate request.'

Event Id 4889

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services set th status of a certificate request to pending.'

Event Id 4890

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The certificate manager settings for Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4891

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A configuration entry changed in Certificate Services.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4892

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A property of Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4893

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services archived a key.'

Event Id 4894

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services imported and archived a key.'

Event Id 4895

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services published the CA certificate toActive Directory Domain Services.'

Event Id 4896

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'One or more rows have been deleted from the certificate database.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4897

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Role separation enabled.'

Event Id 4898

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services loaded a template.'

Event Id 4899

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Certificate Services template was updated.'

Event Id 4900

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services template security was updated.'

Event Id 4902

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Per-user audit policy table was created.'
Device Custom Number 3	PuaCount
Device Custom Number 6	PuaPolicyId

Event Id 4904

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to register a security event source.'
Device Custom String 6	AuditSourceName
Device Custom String 5	EventSourceId
Device Custom String 3	ProcessId
Destination Process Name	ProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4905

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to unregister a security event source.'
Device Custom String 6	AuditSourceName
Device Custom String 5	EventSourceId
Device Custom String 3	ProcessId
Destination Process Name	ProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4906

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The CrashOnAuditFail value has changed.'
Device Custom Number 2	CrashOnAuditFailValue

Event Id 4907

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Auditing settings on object were changed.'
Device Custom String 5	ObjectType
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4908

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Special Groups Logon table modified.'
Device Custom String 6	SidList
Message	'This event is generated when the list of special groups is updated in the registry or through security policy. The updated list of special groups is indicated in the event.'

Event Id 4909

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The local policy settings for the TBS were changed.'

Event Id 4910

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The group policy settings for the TBS were changed.'

Event Id 4911

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Resource attributes of the object were changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination Process ID	ProcessId
Destination Process Name	ProcessName

Event Id 4912

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Per User Audit Policy was changed.'
Device Custom String 6	TargetUserSid
Device Custom String 5	SubcategoryId
Device Action	AuditPolicyChanges
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4913

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Central Access Policy on the object was changed.'
Destination User Name	One of (SubjectUserName,SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination process ID	ProcessId
Destination process Name	ProcessName

Event Id 4928

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was established.'

Event Id 4929

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was removed.'

Event Id 4930

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was modified.'

Event Id 4931

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica destination naming context was modified.'

Event Id 4932

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Synchronization of a replica of an Active Directory naming context has begun.'

Event Id 4933

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Synchronization of a replica of an Active Directory naming context has ended.'

Event Id 4934

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Attributes of an Active Directory object were replicated.'

Event Id 4935

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Replication failure begins.'

Event Id 4936

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Replication failure ends.'

Event Id 4937

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A lingering object was removed from a replica.'

Event Id 4944

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following policy was active when the Windows Firewall started..'

Event Id 4945

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A rule was listed when the Windows Firewall started.'

Event Id 4946

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was added.'

Event Id 4947

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was modified.'

Event Id 4948

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was deleted.'

Event Id 4949

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall settings were restored to the default values.'

Event Id 4950

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 4	SettingType
Device Custom String 5	SettingValue
Name	'A Windows Firewall setting has changed.'

Event Id 4951

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A rule has been ignored because its major version number was not recognized by Windows Firewall.'

Event Id 4952

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.'

Event Id 4953

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A rule has been ignored by Windows Firewall because it could not parse the rule.'
Device Custom String 4	ReasonForRejection

Event Id 4954

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall Group Policy settings has changed. The new settings have been applied.'

Event Id 4956

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall has changed the active profile.'

Event Id 4957

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall did not apply the following rule.'
Device Custom String 6	RuleName
Device Custom String 4	RuleAttr (Error Information)

Event Id 4958

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.'
Device Custom String 4	Error

Event Id 4960

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.'

Event Id 4961

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.'

Event Id 4962

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.'

Event Id 4963

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.'

Event Id 4964

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Special groups have been assigned to a new login.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom String 3	TargetLogonGuid
Device Custom String 6	SidList
Device NT Domain	SubjectDomainName

Event Id 4965

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.'

Event Id 4976

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event Id 4977

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event Id 4978

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event Id 4979

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'

Event Id 4980

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'

Event Id 4981

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

Event Id 4982

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

Event Id 4983

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason
Device Custom String 4	Failure

Event Id 4984

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason
Device Custom String 4	Failure

Event Id 4985

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The state of a transaction has changed.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5024

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service has started successfully.'

Event Id 5025

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service has been stopped.'

Event Id 5027

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.'
Device Custom String 4	ErrorCode

Event Id 5028

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.'
Device Custom String 4	ErrorCode

Event Id 5029

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.'
Device Custom String 4	ErrorCode

Event Id 5030

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service failed to start.'
Device Custom String 4	ErrorCode

Event Id 5031

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service blocked an application from accepting incoming connections on the network.'

Event Id 5032

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.'
Device Custom String 4	ErrorCode

Event Id 5033

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver has started successfully.'
Message	" "

Event Id 5034

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver has been stopped.'

Event Id 5035

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver failed to start.'
Device Custom String 4	ErrorCode

Event Id 5037

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver detected critical runtime error. Terminating.'
Device Custom String 4	ErrorCode

Event Id 5038

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.'

Event Id 5039

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A registry key was virtualized.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5040

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was added.'

Event Id 5041

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was modified.'

Event Id 5042

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was deleted.'

Event Id 5043

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was added.'

Event Id 5044

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was modified.'

Event Id 5045

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was deleted.'

Event Id 5046

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was added.'

Event Id 5047

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was modified.'

Event Id 5048

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was deleted.'

Event Id 5049

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Security Association was deleted.'

Event Id 5050

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE) interface was rejected because this API is not supported on Windows Vista. This has most likely occurred due to a program which is incompatible with Windows Vista. Please contact the program's manufacturer to make sure you have a Windows Vista compatible program version.'

Event Id 5051

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A file was virtualized.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5056

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic self test was performed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5057

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic primitive operation failed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	Reason
Reason	ReturnCode

Event Id 5058

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Key file operation.'
File Name	KeyName
File Type	KeyType
File Path	KeyFilePath
Device Action	Operation
Device Custom Date 1	ClientCreationTime
Device Custom String 1	ProviderName
Device Custom String 3	AlogorithmName

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 4	ReturnCode
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Source Process Id	ClientProcessId

Event Id 5059

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Key migration operation.'
File Name	KeyName
File Type	KeyType
Device Action	Operation
Device Custom String 4	ReturnCode
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5060

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Verification operation failed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5061

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Cryptographic operation.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5062

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A kernel-mode cryptographic self test was performed.'

Event Id 5063

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic provider operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5064

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic context operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5065

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic context modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5066

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5067

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5068

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function provider operation was attempted.'
Destination User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5069

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function property operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5070

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function property modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5071

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Key access denied by Microsoft key distribution service.'
Device Custom String 5	SecurityDescriptor
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5120

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'OCSP Responder Service Started.'

Event Id 5121

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'OCSP Responder Service Stopped.'

Event Id 5122

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Configuration entry changed in the OCSP Responder Service.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5123

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A configuration entry changed in the OCSP Responder Service.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5124

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A security setting was updated on OCSP Responder Service.'

Event Id 5125

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A request was submitted to OCSP Responder Service.'

Event Id 5126

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Signing Certificate was automatically updated by the OCSP Responder Service.'

Event Id 5127

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The OCSP Revocation provider successfully updated the revocation information.'

Event Id 5136

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was modified.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	OperationType

Event Id 5137

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was created.'
Device Custom String 6	ObjectDN

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5138

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was undeleted.'
Device Custom String 6	NewObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5139

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was moved.'
Device Custom String 6	NewObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5140

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A network share object was accessed.'
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
File Path	ShareName
File Type	ObjectType
Device Custom String 6	ShareName
Device Custom String 1	AccessList
Source Port	IpPort
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5141

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was deleted.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5142

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A network share object was added.'
File Path	ShareName
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event Id 5143

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A network share object was modified.'
File Path	ShareName
Device Custom String 5	ObjectType
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event Id 5144

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A network share object was deleted.'
File Path	ShareName
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event Id 5145

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A network share object was checked to see whether client can be granted desired access.'
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Source Port	IpPort
Device Custom String 6	ShareName
File Path	ShareLocalPath
File Name	RelativeTargetName

Event Id 5146

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a packet.'
Device Direction	Direction
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Destination Address	DestAddress

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Source Port	SourceSwitchPort
Destination Port	DestinationvSwitchPort

Event Id 5147

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A more restrictive Windows Filtering Platform filter has blocked a packet.'
Device Direction	Direction
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Destination Address	DestAddress
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Source Port	SourceSwitchPort
Destination Port	DestinationvSwitchPort

Event Id 5152

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform blocked a packet.'
Source Address	SourceAddress
Source Port	SourcePort
Destination Address	DestAddress
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5153

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A more restrictive Windows Filtering Platform filter has blocked a packet.'
Source Port	SourcePort
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5154

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering platform has permitted an application or service to listen on a port for incoming connections.'
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort
File Name	Application
File Path	Application
File Type	Application

Event Id 5155

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.'
Source Port	SourcePort
File Name	Application
File Path	Application
File Type	Application

Event Id 5156

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has allowed a connection.'
Device Direction	Direction
Source Address	One of (SourceAddress)
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort
Destination Address	One of (DestAddress)
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Destination Port	DestPort
Transport Protocol	Protocol
File Name	Application
File Path	Application
File Type	Application

Event Id 5157

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a connection.'
Source Port	SourcePort
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5158

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has permitted a bind to a local port.'
Source Address	SourceAddress

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort
File Name	Application
File Path	Application
File Type	Application

Event Id 5159

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a bind to a local port.'
Source Process ID	ProcessId
File Name	Application
File Path	Application
File Type	Application
Source Address	SourceAddress
Destination Address	SourceAddress
Transport Protocol	Protocol
Device Custom Number 2	FilterRTID
Device Custom String 6	LayerName
Device Custom Number 3	LayerRTID
Source Port	SourcePort

Event Id 5168

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Spn check for SMB/SMB2 fails.'
Destination User Name	' '
Source User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	' '
Source NT Domain	SubjectDomainName
Destination User ID	' '

Micro Focus ArcSight ESM Field	Device-Specific Field
Source User ID	SubjectLogonId
Destination Service Name	SpnName
Device Custom String 4	ErrorCode
Device NT Domain	SubjectDomainName
Reason	ErrorCode

Event Id 5376

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom Date 1	ProcessCreationTime
Device NT Domain	SubjectDomainName
File Path	BackupFileName
Message	'This event occurs when a user backs up their own Credential Manager credentials. A user (even an Administrator) cannot back up the credentials of an account other than his own.'
Name	'Credential Manager credentials were backed up.'
Source Process ID	ClientProcessId

Event Id 5377

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Path	BackupFileName

Micro Focus ArcSight ESM Field	Device-Specific Field
Message	'This event occurs when a user restores his Credential Manager credentials from a backup. A user (even an Administrator) cannot restore the credentials of an account other than his own.'
Name	'Credential Manager credentials were restored from a backup.'
Source Process ID	ClientProcessId

Event Id 5378

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The requested credentials delegation was disallowed by policy.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5379

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination Process Name	TargetName
Device Custom Date 1	ProcessCreationTime
Device Custom Number 1	Type
Device Custom Number 2	CountOfCredentialsReturned
Device Custom String 3	ReadOperation
Reason	ReturnCode
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5380

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 2	CountOfCredentialsReturned
Device Custom String 4	SchemaFriendlyName
Request Context	SearchString
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5381

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 2	CountOfCredentialsReturned
Device Custom Number 3	Flags
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5382

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 3	Flags
Device Custom String 4	SchemaFriendlyName
Device Custom String 5	PackageSid
Device Custom String 6	Identity

Micro Focus ArcSight ESM Field	Device-Specific Field
Reason	ReturnCode
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5440

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following callout was present when the Windows Filtering Platform Base Filtering Engine started.'

Event Id 5441

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following filter was present when the Windows Filtering Platform Base Filtering Engine started.'

Event Id 5442

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following provider was present when the Windows Filtering Platform Base Filtering Engine started.'

Event Id 5443

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.'

Event Id 5444

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.'

Event Id 5446

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform callout has been changed.'
Destination User Name	One of (UserName, UserSid)

Event Id 5447

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform filter has been changed.'
Destination User Name	One of (UserName, UserSid)

Event Id 5448

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform provider has been changed.'
Destination User Name	One of (UserName, UserSid)

Event Id 5449

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform provider context has been changed.'
Destination User Name	One of (UserName, UserSid)

Event Id 5450

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform sub-layer has been changed.'
Destination User Name	One of (UserName, UserSid)

Event Id 5451

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode security association was established.'
Source Address	LocalAddress
Source Port	LocalPort
Destination Address	RemoteAddress
Destination Port	RemotePort

Event Id 5452

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode security association ended.'
Source Address	LocalAddress
Source Port	LocalPort
Destination Address	RemoteAddress
Destination Port	RemotePort

Event Id 5453

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.'

Event Id 5456

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied Active Directory storage IPsec policy on the computer.'

Event Id 5457

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.'

Event Id 5458

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied locally cached copy of Active Directory storage IPsec on the computer.'

Event Id 5459

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.'
Device Custom String 4	Error

Event Id 5460

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied local registry storage IPsec policy on the computer.'

Event Id 5461

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply local registry storage IPsec policy on the computer.'
Device Custom String 4	Error

Event Id 5462

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.'
Device Custom String 4	Error

Event Id 5463

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine Polled for changes to the active IPsec policy and detected no changes.'

Event Id 5464

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.'

Event Id 5465

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.'

Event Id 5466

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.'

Event Id 5467

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.'

Event Id 5468

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.'

Event Id 5471

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine loaded local storage IPsec policy on the computer.'

Event Id 5472

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to load local storage IPsec policy on the computer.'
Device Custom String 4	Error

Event Id 5473

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine loaded directory storage IPsec policy on the computer.'

Event Id 5474

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to load directory storage IPsec policy on the computer.'
Device Custom String 4	Error

Event Id 5477

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to add quick mode filter.'
Device Custom String 4	Error

Event Id 5478

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has started successfully.'

Event Id 5479

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.'

Event Id 5480

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.'

Event Id 5483

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services failed to initialize RPC server. IPsec Services could not be started.'
Device Custom String 4	Error

Event Id 5484

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.'
Device Custom String 4	Error

Event Id 5632

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A request was made to authenticate to a wireless network.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, Identity)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	One of (ReasonCode, ErrorCode)
Reason	One of (EAPErrorCode, EAPReasonCode, ErrorCode, both (ReasonText, ReasonCode))

Event Id 5633

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A request was made to authenticate to a wired network.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, Identity)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Outbound Interface	InterfaceName
Device Custom String 4	One of (ReasonCode, ErrorCode)
Reason	One of (ErrorCode, both (ReasonText, ReasonCode))

Event Id 5712

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Remote Procedure Call (RPC) was attempted.'
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5888

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An object in the COM+ Catalog was modified.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name

Event Id 5889

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An object was deleted from the COM+ Catalog.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name
Message	'This event occurs when an object is deleted from the COM+ catalog.'

Event Id 5890

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'An object was added to the COM+ Catalog.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name

Event Id 6144

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Security policy in the group policy objects has been applied successfully.'

Event Id 6145

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'One or more errors occurred while processing security policy I nthe group policy objects.'
Device Custom String 4	ErrorCode

Event Id 6272

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user.'
Destination User Name	SubjectUserName

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Destination Address	NASIPv4Address
Destination Port	NASPort
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

Event Id 6273

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Destination Address	NASIPv4Address
Destination Port	NASPort
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 4	Reason
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier

Event Id 6274

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the request for a user. . Contact the Network Policy Server administrator for more information.'

Event Id 6275

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the accounting request for a user. . Contact the Network Policy Server administrator for more information.'

Event Id 6276

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server quarantined a user. . Contact the Network Policy Server administrator for more information.'

Event Id 6277

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy . Contact the Network Policy Server administrator for more information.'

Event Id 6278

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted full access to a user because the host met the defined health policy.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Source User Name	SubjectMachineName

Micro Focus ArcSight ESM Field	Device-Specific Field
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Destination Address	NASIPv4Address
Destination Port	NASPort
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

Event Id 6279

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server locked the user account due to repeated failed authentication attempts.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName

Event Id 6280

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server unlocked the user account.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName

Event Id 6281

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Code Integrity determined that the page hashes or an image file are not valid.'
File Path	Param1
Message	'The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.'

Event Id 6409

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'BranchCache: A service connection point object could not be parsed.'

Event Id 6410

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Code integrity determined that a file does not meet the security requirements to load into a process.'
Message	'This could be due to the use of shared sections or other issues.'
File Name	param1

Event Id 6416

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A new external device was recognized by the system.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
File ID	ClassId
Device Custom String 1	VendorIds

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 4	CompatibleIds
Device Custom String 5	LocationInformation
Message	'A new external device was recognized by the system.'

Event Id 8191

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Highest System-Defined Audit Message Value.'

Mappings for Microsoft OAlerts

Event Id 300

ArcSight ESM Field	Device-Specific Field
Name	Microsoft Office Alerts
Device Product	OAlerts
File Type	%1
Message	%2
Device Version	%4

Mappings for DNS Client Operational

Event Id 1015

ArcSight Field	Vendor Field
Name	"Name resolution timed out after the DNS server did not respond"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 1016

ArcSight Field	Vendor Field
Name	"A name not found error was returned"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 1017

ArcSight Field	Vendor Field
Name	"The DNS server's response to a query"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 3006

ArcSight Field	Vendor Field
Name	"DNS query is called"
Device Custom String 1	QueryName
Device Custom String 5	ServerList
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	InterfaceIndex

Event Id 3008

ArcSight Field	Vendor Field
Name	"DNS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults

ArcSight Field	Vendor Field
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	QueryStatus

Event Id 3009

ArcSight Field	Vendor Field
Name	"Network query initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress
Device Dns Domain	DNSServerAddress

Event Id 3010

ArcSight Field	Vendor Field
Name	"DNS Query sent to DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress

Event Id 3011

ArcSight Field	Vendor Field
Name	"Received response from DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress
Event Outcome	ResponseStatus

Event Id 3012

ArcSight Field	Vendor Field
Name	"NETBIOS query is initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress

Event Id 3013

ArcSight Field	Vendor Field
Name	"NETBIOS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Event Outcome	Status

Event Id 3014

ArcSight Field	Vendor Field
Name	"NETBIOS query is pending"
Device Custom String 1	QueryName

Event Id 3016

ArcSight Field	Vendor Field
Name	"Cache lookup called"
Device Custom String 1	QueryName
Device Custom Number 2	QueryType
Device Custom Number 3	InterfaceIndex

Event Id 3018

ArcSight Field	Vendor Field
Name	"Cache lookup for name"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions

Event Id 3019

ArcSight Field	Vendor Field
Name	"Query wire called"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Custom Number 2	NetworkIndex
Device Custom Number 3	InterfaceIndex

Event Id 3020

ArcSight Field	Vendor Field
Name	"Query response for name"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	NetworkIndex
Device Custom Number 3	InterfaceIndex
Event Outcome	Status

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
Account Logon	Credential Validation	4774	An account was mapped for logon.
	Credential Validation	4775	An account could not be mapped for logon.
	Credential Validation	4776	The domain controller attempted to validate the credentials for an account.
	Credential Validation	4777	The domain controller failed to validate the credentials for an account.
	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.
	Kerberos Authentication Service	4771	Kerberos pre-authentication failed.
	Kerberos Authentication Service	4772	A Kerberos authentication ticket request failed.
	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.
	Kerberos Service Ticket Operations	4770	A Kerberos service ticket was renewed.

Category	Subcategory	ID	Message Summary
Account Management	Application Group Management	4783	A basic application group was created.
		4784	A basic application group was changed.
		4785	A member was added to a basic application group.
		4786	A member was removed from a basic application group.
		4787	A non-member was added to a basic application group.
		4788	A non-member was removed from a basic application group.
		4789	A basic application group was deleted.
		4790	An LDAP query group was created.
	Computer Account Management	4742	A computer account was changed.
		4743	A computer account was deleted.
Account Management	Distribution Group Management	4744	A security-disabled local group was created.
		4745	A security-disabled local group was changed.
		4746	A member was added to a security-disabled local group.
		4747	A member was removed from a security-disabled local group.
		4748	A security-disabled local group was deleted.
		4749	A security-disabled global group was created.
		4750	A security-disabled global group was changed.
		4751	A member was added to a security-disabled global group.
		4752	A member was removed from a security-disabled global group.
		4753	A security-disabled global group was deleted.
		4759	A security-disabled universal group was created.
		4760	A security-disabled universal group was changed.
		4761	A member was added to a security-disabled universal group.
		4762	A member was removed from a security-disabled universal group.
		4763	A security-disabled universal group was deleted.

Category	Subcategory	ID	Message Summary
Account Management	Other Account Management Events	4782	The password hash an account was accessed.
		4793	The Password Policy Checking API was called.
		4797	An attempt was made to query the existence of a blank password for an account.
Account Management	Security Group Management	4727	A security-enabled global group was created.
		4728	A member was added to a security-enabled global group.
		4729	A member was removed from a security-enabled global group.
		4730	A security-enabled global group was deleted.
		4731	A security-enabled local group was created.
		4732	A member was added to a security-enabled local group.
		4733	A member was removed from a security-enabled local group.
		4734	A security-enabled local group was deleted.
		4735	A security-enabled local group was changed.
		4737	A security-enabled global group was changed.
		4754	A security-enabled universal group was created.
		4755	A security-enabled universal group was changed.
		4756	A member was added to a security-enabled universal group.
		4757	A member was removed from a security-enabled universal group.
		4799	A security-enabled local group membership was enumerated
Account Management	User Account Management	4758	A security-enabled universal group was deleted.
		4764	A group's type was changed.

Category	Subcategory	ID	Message Summary
		4720	A user account was created.
		4722	A user account was enabled.
		4723	An attempt was made to change an account's password.
		4724	An attempt was made to reset an account's password.
		4725	A user account was disabled.
		4726	A user account was deleted.
		4738	A user account was changed.
		4740	A user account was locked out.
		4765	SID History was added to an account.
		4766	An attempt to add SID History to an account failed.
		4767	A user account was unlocked.
		4780	The ACL was set on accounts which are members of administrators groups.
		4781	The name of an account was changed:
		4794	An attempt was made to set the Directory Services Restore Mode.
		4798	A user's local group membership was enumerated.
		5376	Credential Manager credentials were backed up.
		5377	Credential Manager credentials were restored from a backup.
Detailed Tracking	DPAPI Activity	4692	Backup of data protection master key was attempted.
		4693	Recovery of data protection master key was attempted.
		4694	Protection of auditable protected data was attempted.
		4695	Unprotection of auditable protected data was attempted.
	Process Creation	4688	A new process has been created.
		4696	A primary token was assigned to process.
	Process Termination	4689	A process has exited.
	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.

Category	Subcategory	ID	Message Summary
DS Access	Detailed Directory Service Replication	4928	An Active Directory replica source naming context was established.
		4929	An Active Directory replica source naming context was removed.
		4930	An Active Directory replica source naming context was modified.
		4931	An Active Directory replica destination naming context was modified.
		4934	Attributes of an Active Directory object were replicated.
		4935	Replication failure begins.
		4936	Replication failure ends.
		4937	A lingering object was removed from a replica.
DS Access	Directory Service Access	4662	An operation was performed on an object.
	Directory Service Changes	5136	A directory service object was modified.
		5137	A directory service object was created.
		5138	A directory service object was undeleted.
		5139	A directory service object was moved.
		5141	A directory service object was deleted.
	Directory Service Replication	4932	Synchronization of a replica of an Active Directory naming context has begun.
		4933	Synchronization of a replica of an Active Directory naming context has ended.
Logon/Logoff	Account Lockout	4625	An account failed to logon
	IPsec Extended Mode	4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		4979	IPsec Main Mode and Extended Mode security associations were established.
		4980	
		4981	
		4982	
		4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Category	Subcategory	ID	Message Summary
		4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
Logon/Logoff	IPsec Main Mode	4646	IKE DoS-prevention mode started.
		4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
		4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
	IPsec Main Mode	4652	An IPsec Main Mode negotiation failed.
		4653	An IPsec Main Mode negotiation failed.
		4655	An IPsec Main Mode security association ended.
		4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5049	An IPsec Security Association was deleted.
		5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
	IPsec Quick Mode	4654	An IPsec Quick Mode negotiation failed.
		4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5451	An IPsec Quick Mode security association was established.
		5452	An IPsec Quick Mode security association ended.

Category	Subcategory	ID	Message Summary
Logon/Logoff	Logoff	4634	An account was logged off.
		4647	User initiated logoff.
	Logon	4624	An account was successfully logged on.
		4625	An account failed to log on.
		4626	User/Device claims information.
		4627	Group membership information.
		4648	A logon was attempted using explicit credentials.
		4675	SIDs were filtered.
	Network Policy Server	6272	Network Policy Server granted access to a user.
		6273	Network Policy Server denied access to a user.
		6274	Network Policy Server discarded the request for a user.
		6275	Network Policy Server discarded the accounting request for a user.
		6276	Network Policy Server quarantined a user.
		6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
		6278	Network Policy Server granted full access to a user because the host met the defined health policy.
		6279	Network Policy Server locked the user account due to repeated failed authentication attempts.
		6280	Network Policy Server unlocked the user account.

Category	Subcategory	ID	Message Summary
Logon/Logoff	Other Logon/Logoff Events	4649	A replay attack was detected.
		4778	A session was reconnected to a Window Station.
		4779	A session was disconnected from a Window Station.
		4800	The workstation was locked.
		4801	The workstation was unlocked.
		4802	The screen saver was invoked.
		4803	The screen saver was dismissed.
	Other Logon/Logoff Events	5378	The requested credentials delegation was disallowed by policy.
		5632	A request was made to authenticate to a wireless network.
		5633	A request was made to authenticate to a wired network.
	Special Logon	4964	Special groups have been assigned to a new logon.

Category	Subcategory	ID	Message Summary
Object Access	Application Generated	4665	An attempt was made to create an application client context.
		4666	An application attempted an operation:
		4667	An application client context was deleted.
		4668	An application was initialized.
	Central Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
	Certification Services	4868	The certificate manager denied a pending certificate request.
		4869	Certificate Services received a resubmitted certificate request.
		4870	Certificate Services revoked a certificate.
		4871	Certificate Services received a request to publish the certificate revocation list (CRL).
		4872	Certificate Services published the certificate revocation list (CRL).
		4873	A certificate request extension changed.
		4874	One or more certificate request attributes changed.
		4875	Certificate Services received a request to shutdown.
		4876	Certificate Services backup started.
		4877	Certificate Services backup completed.
		4878	Certificate Services restore started.
		4879	Certificate Services restore completed.
		4880	Certificate Services started.
		4881	Certificate Services stopped.
		4882	The security permissions for Certificate Services changed.

Category	Subcategory	ID	Message Summary
Object Access	Certification Services	4883	Certificate Services retrieved an archived key.
		4884	Certificate Services imported a certificate into its database.
		4885	The audit filter for Certificate Services changed.
		4886	Certificate Services received a certificate request.
		4887	Certificate Services approved a certificate request and issued a certificate.
		4888	Certificate Services denied a certificate request.
		4889	Certificate Services set the status of a certificate request to pending.
		4890	The certificate manager settings for Certificate Services changed.
		4891	A configuration entry changed in Certificate Services.
		4892	A property of Certificate Services changed.
		4893	Certificate Services archived a key.
		4894	Certificate Services imported and archived a key.
	Certification Services	4895	Certificate Services published the CA certificate to Active Directory Domain Services.
		4896	One or more rows have been deleted from the certificate database.
		4897	Role separation enabled.
		4898	Certificate Services loaded a template.

Category	Subcategory	ID	Message Summary
Object Access	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.
	File Share	5140	A network share object was accessed.
		5142	A network share object was added.
		5143	A network share object was modified.
		5144	A network share object was deleted.
		5168	Spn check for SMB/SMB2 failed.
	File System	4664	An attempt was made to create a hard link.
		4985	The state of a transaction has changed.
		5051	A file was virtualized.
	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
		5146	The Windows Filtering Platform has blocked a packet.
		5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5150	The Windows Filtering Platform has blocked a packet.
		5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
		5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
		5156	The Windows Filtering Platform has allowed a connection.
		5157	The Windows Filtering Platform has blocked a connection.
		5158	The Windows Filtering Platform has permitted a bind to a local port.
		5159	The Windows Filtering Platform has blocked a bind to a local port.
Object Access	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.
		5153	A more restrictive Windows Filtering Platform filter has blocked a packet.

Category	Subcategory	ID	Message Summary
Object Access	Handle Manipulation	4656	A handle to an object was requested.
		4658	The handle to an object was closed.
		4690	An attempt was made to duplicate a handle to an object.
Object Access	Other Object Access Events	4671	An application attempted to access a blocked ordinal through the TBS.
		4691	Indirect access to an object was requested.
		4698	A scheduled task was created.
		4699	A scheduled task was deleted.
		4700	A scheduled task was enabled.
		4701	A scheduled task was disabled.
		4702	A scheduled task was updated.
Object Access	Other Object Access Events	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
		5149	The DoS attack has subsided and normal processing is being resumed.
		5888	An object in the COM+ Catalog was modified.
		5889	An object was deleted from the COM+ Catalog.
		5890	An object was added to the COM+ Catalog.
Object Access	Registry	4657	A registry value was modified.
		5039	A registry key was virtualized.
Object Access	Special	4659	A handle to an object was requested with intent to delete.
		4660	An object was deleted.
		4661	A handle to an object was requested.
		4663	An attempt was made to access an object.

Category	Subcategory	ID	Message Summary
Policy Change	Audit Policy Change	4715	The audit policy (SACL) on an object was changed.
		4719	System audit policy was changed.
		4817	Auditing settings on an object were changed.
		4902	The Per-user audit policy table was created.
		4904	An attempt was made to register a security event source.
		4905	An attempt was made to unregister a security event source.
		4906	The CrashOnAuditFail value has changed.
		4907	Auditing settings on object were changed.
		4908	Special Groups Logon table modified.
		4912	Per User Audit Policy was changed.
Policy Change	Authentication Policy Change	4713	Kerberos policy was changed.
		4716	Trusted domain information was modified.
		4717	System security access was granted to an account.
		4718	System security access was removed from an account.
		4739	Domain Policy was changed.
		4864	A namespace collision was detected.
		4865	A trusted forest information entry was added.
		4866	A trusted forest information entry was removed.
		4867	A trusted forest information entry was modified.
		4703	A token right was adjusted.
Policy Change	Authorization Policy Change	4704	A user right was assigned.
		4705	A user right was removed.
		4706	A new trust was created to a domain.
		4707	A trust to a domain was removed.
		4714	Encrypted data recovery policy was changed.
		4911	Resource attributes of the object were changed.
		4913	Central Access Policy on the object was changed.
Policy Change	Filtering Platform Policy Change	4709	IPsec Services was started.

Category	Subcategory	ID	Message Summary
		4710	IPsec Services was disabled.
Policy Change	Filtering Platform Policy Change	4711	<p>May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine applied Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine applied local registry storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply local registry storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply some rules of the active IPsec policy on the computer.</p> <p>PAStore Engine failed to load directory storage IPsec policy on the computer.</p> <p>PAStore Engine loaded directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to load local storage IPsec policy on the computer.</p> <p>PAStore Engine loaded local storage IPsec policy on the computer.</p> <p>PAStore Engine polled for changes to the active IPsec policy and detected no changes.</p>

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	4712	IPsec Services encountered a potentially serious failure.
		5040	A change has been made to IPsec settings. An Authentication Set was added.
		5041	A change has been made to IPsec settings. An Authentication Set was modified.
		5042	A change has been made to IPsec settings. An Authentication Set was deleted.
		5043	A change has been made to IPsec settings. A Connection Security Rule was added.
		5044	A change has been made to IPsec settings. A Connection Security Rule was modified.
		5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.
		5046	A change has been made to IPsec settings. A Crypto Set was added.
		5047	A change has been made to IPsec settings. A Crypto Set was modified.
		5048	A change has been made to IPsec settings. A Crypto Set was deleted.
Policy Change	Filtering Platform Policy Change	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
		5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
		5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
		5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
		5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
		5446	A Windows Filtering Platform callout has been changed.
Policy Change	Filtering Platform Policy Change	5448	A Windows Filtering Platform provider has been changed.
		5449	A Windows Filtering Platform provider context has been changed.

Category	Subcategory	ID	Message Summary
		5450	A Windows Filtering Platform sub-layer has been changed.
		5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.
		5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
		5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
		5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
		5460	PAStore Engine applied local registry storage IPsec policy on the computer.
		5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.
		5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.
		5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.
		5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
		5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
		5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
		5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
		5471	PAStore Engine loaded local storage IPsec policy on the computer.
		5472	PAStore Engine failed to load local storage IPsec policy on the computer.
		5473	PAStore Engine loaded directory storage IPsec policy on the computer.
		5474	PAStore Engine failed to load directory storage IPsec policy on the computer.
		5477	PAStore Engine failed to add quick mode filter.

Category	Subcategory	ID	Message Summary
Policy Change	MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started.
		4945	A rule was listed when the Windows Firewall started.
		4946	A change has been made to Windows Firewall exception list. A rule was added.
		4947	A change has been made to Windows Firewall exception list. A rule was modified.
		4948	A change has been made to Windows Firewall exception list. A rule was deleted.
		4949	Windows Firewall settings were restored to the default values.
		4950	A Windows Firewall setting has changed.
		4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.
		4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
		4953	A rule has been ignored by Windows Firewall because it could not parse the rule.
		4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.
		4956	Windows Firewall has changed the active profile.
		4957	Windows Firewall did not apply the following rule:
		4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:

Category	Subcategory	ID	Message Summary
Policy Change	Other Policy Change Events	4819	Central Access Policies on the machine have been changed.
		4909	The local policy settings for the TBS were changed.
		4910	The group policy settings for the TBS were changed.
		5063	A cryptographic provider operation was attempted.
		5064	A cryptographic context operation was attempted.
		5065	A cryptographic context modification was attempted.
		5066	A cryptographic function operation was attempted.
		5067	A cryptographic function modification was attempted.
		5068	A cryptographic function provider operation was attempted.
		5069	A cryptographic function property operation was attempted.
		5070	A cryptographic function property modification was attempted.
		5447	A Windows Filtering Platform filter has been changed.
		6144	Security policy in the group policy objects has been applied successfully.
		6145	One or more errors occurred while processing security policy in the group policy objects.
Policy Change	Subcategory (special)	4670	Permissions on an object were changed.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4672	Special privileges assigned to new logon.
		4673	A privileged service was called.
		4674	An operation was attempted on a privileged object.
System	IPsec Driver	4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
		4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
		4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.

Category	Subcategory	ID	Message Summary
System	IPsec Driver	4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
		4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
		5478	IPsec Services has started successfully.
		5479	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
		5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
		5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.
		5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
		5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
System	Other System Events	4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
		4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.
		4822	NTLM authentication failed because the account was a member of the Protected User group.

Category	Subcategory	ID	Message Summary
System	Other System Events	4823	NTLM authentication failed because access control restrictions are required.
		4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
		4826	Boot Configuration Data Loaded.
		5024	The Windows Firewall Service has started successfully.
		5025	The Windows Firewall Service has been stopped.
		5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
System	Other System Events	5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
		5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
		5030	The Windows Firewall Service failed to start.
		5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
		5033	The Windows Firewall Driver has started successfully.
		5034	The Windows Firewall Driver has been stopped.
		5035	The Windows Firewall Driver failed to start.
		5037	The Windows Firewall Driver detected critical runtime error. Terminating.
		5058	Key file operation.
		5059	Key migration operation.
		6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
		6401	BranchCache: Received invalid data from a peer. Data discarded.
		6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.

Category	Subcategory	ID	Message Summary
System	Other System Events	6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.
		6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
		6405	BranchCache: %2 instance(s) of event id %1 occurred.
		6406	%1 registered to Windows Firewall to control filtering for the following: %2
		6407	1%
		6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2
System	Security State Change	4608	Windows is starting up.
		4609	Windows is shutting down.
		4616	The system time was changed.
		4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.
System	Security System Extension	4610	An authentication package has been loaded by the Local Security Authority. Native Connector: An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
		4611	This logon process will be trusted to submit logon requests.
		4614	A notification package has been loaded by the Security Account Manager.
		4622	A security package has been loaded by the Local Security Authority.
		4697	A service was installed in the system.

Category	Subcategory	ID	Message Summary
System	System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
		4615	Invalid use of LPC port.
		4618	A monitored security event pattern has occurred.
		4816	RPC detected an integrity violation while decrypting an incoming message.
		5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
		5056	A cryptographic self test was performed.
		5057	A cryptographic primitive operation failed.
		5060	Verification operation failed.
		5061	Cryptographic operation.
		5062	A kernel-mode cryptographic self test was performed.
		6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error

Appendix A. Types of Internal Events

The Windows Event Log – Native connector documents the following types of internal events:

- ["Specific Windows Security Event Mappings" below](#)
- [Collector Connected](#)
- [Collector Disconnected](#)
- [Collector Up](#)
- [Collector Down](#)
- [Collector Configuration Accepted](#)
- [Collector Status Updated](#)
- [Collector Event Collection Started](#)
- [Remote Agent Status](#)

Specific Windows Security Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The log file was cleared'
Message	concatenate('The ',Channel,' log file was cleared')
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName
File Type	Channel
File Path	BackupPath

1100

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The event logging service has shut down.'

1101

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Audit events have been dropped by the transport. The real time backup file was corrupt due to improper shutdown.'
Device Custom Number 3	Reason

1102

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The audit log was cleared.'
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination User ID	SubjectLogonId

1104

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The security log is now full'

1105

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Event log automatic backup.'
File Type	Channel
File Name	BackupPath

Collector Connected

Field	Description
Event Name	'Collector'
Device Event Category	'/Informational'
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Disconnected

Field	Description
Event Name	'Collector Disconnected'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Down

Field	Description
Event Name	'Collector Down'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Configuration Accepted

Collector Status for "Collector Configuration Accepted"

Field	Description
Event Name	'Collector Configuration Accepted'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Configuration Accepted”

Field	Description
Event Name	'Collector Configuration Accepted'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or 'Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Configuration Accepted”

Field	Description
Event Name	'Collector Configuration Accepted'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Status Updated

Collector Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3, depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Event Collection Started

Collector Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'

Field	Description
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<Event Collection SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>

Field	Description
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Up

Field	Description
Event Name	'Collector Up'
Device Event Category	'/Informational'
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Appendix B. Microsoft Windows Event Log Native Connector and Unified Features Comparison

This topic compares the SmartConnector for Microsoft Windows Event Log - Native to the SmartConnector for Microsoft Windows Event Log - Unified.

The Native connector is ArcSight's Windows Event Log collection SmartConnector. It uses native Microsoft technology and has broad capabilities, but can be installed only on Windows systems.

The Unified connector is ArcSight's legacy Windows Event Log collection SmartConnector. It is a portable connector that can be installed on both Windows and Unix systems. This is achieved through a Java implementation of the Windows logging technology (JCIFS), which limits the connector to JCIFS technical capabilities.

Windows Event Log - Native and Unified Connector Features

Feature	Native Connector	Unified Connector
Scalability	Improved scalability. Uses "push" instead of "pull". Does not use round robin, does not "hang" on a device that is slow or unresponsive. There is no need to balance event sources.	Pulls events in a round robin sequence (round robin applies to hosts from which batches of events collected). Experiences delays when polling a slow or unresponsive source.
Pre-filtering	Performs pre-filtering on the sending server. This conserves bandwidth and enhance connector performance. For example, if you are interested only in logon failures (such as Event ID 4625), you do not need to get any other event to the connector.	Does not perform pre-filtering.
IPv6 Stack	Able to fully run on the IPv6 stack.	IPv6 stack not supported.
SMBv2 and SMBv3	Supports SMBv2 and SMBv3, providing enhanced security and better performance.	Limited to SMBv1.
Easier Configuration	Configuration is easier, with fewer windows and configuration options. One screen includes all of the configuration required in a typical implementation, including use of Windows Event Forwarding (WEF).	Configuration requires more windows and configuration options.

Feature	Native Connector	Unified Connector
Forwarded Events	Collects from ForwardedEvents log, which is the default when you setup a WEF subscription.	Collects remote logs only from the HardwareEvents event log, in addition to Security/Application/System.
Custom Event Logs	Can read events in any Windows event log, including AppLocker and Windows Defender events. The flex framework makes it easier to create custom parsers	Has limitations in reading Windows event logs, although there is a workaround for AppLocker events using WEF.
Operating Systems Supported for Connector Installation	Windows	Windows, Linux
Event Log Types	Security, System, Application event logs under "Windows Logs" and all event logs under "Applications and Services Logs"	Security, System, Application event logs under "Windows Logs"
Parser Support	Windows OS independent. Native does not need OS information for correct parsing, so configuring source host OS versions is optional.	Not Windows OS independent

SmartConnector for Windows Event Log - Native Limitations

- Runs only on Windows; it cannot be run on ArcSight Management Center, Connector Appliance, or Linux/Unix OS, although it can be remotely managed from ArcSight Management Center.
- Runs only on 64-bit OS.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Windows Event Native Smart Connector (ArcSight 8.2.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!