Hewlett Packard
Enterprise

HPE Security ArcSight ESM

Software Version: 7.0

ESM 7.0 Release Notes

April 13, 2018

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

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

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://community.softwaregrp.com/t5/Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228

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

Welcome to ESM 7.0

ArcSight Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. ESM is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

ESM includes the Correlation Optimized Retention and Retrieval (CORR) Engine, a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches.

What's New in This Release

This topic describes the new features and enhancements added in ESM 7.0.

ArcSight Command Center Enhancements

Security Operation Center (SOC) Manager

The SOC Manager enables an administrative user to see case metric data details.

See the topic "Using the Security Operation Center (SOC) Manager" in the *Arcsight Command Center User's Guide* for details.

Security Operation Center (SOC) Dashboard

The SOC Dashboard enables an administrative user to see the sources and distribution of events. It includes a geographic map visualization of the top source addresses and top destination addresses of events, with details on events, rules, and assets.

See the topic "Using the Security Operation Center (SOC) Dashboard" in the *Arcsight Command Center User's Guide* for details.

Cluster View Dashboard

The Cluster View Dashboard displays a cluster and its component nodes. This dashboard is view-only, and enables you to get a quick look at the health of your cluster. Note, the *ESM Administrator's Guide* might refer to the Distributed Correlation Dashboard, which is actually the Cluster View Dashboard.

See the topic "Using the Cluster View Dashboard" in the *Arcsight Command Center User's Guide* for details.

Case History for Viewing Updates and Notes

The Case History pop-up lists updates related to a case, filtered by date or user who modified, in descending order.

See the topic "Viewing Updates and Notes in Case History" in the *Arcsight Command Center User's Guide* for details.

Assign Cases to a User Group

In addition to individual users as case owners, you can now assign user groups as case owners. A new field, `Owner Groups`, is added to the Assign section of the Attributes subtab of the Case Editor Initial tab.

See the topic "Creating or Editing a Case" in the *Arcsight Command Center User's Guide* for details.

Dark Theme Support in Entire ArcSight Command Center

Changes the Command Center display from the default light to dark theme. The dark theme reduces glare from the screen, providing visual comfort in dark room environments. It is now supported throughout the entire ArcSight Command Center.

See the topic "Basic Navigation" in the *Arcsight Command Center User's Guide* for details.

Session Timeout Can Be Disabled

A Session Timeout button has been added to the user information. The default is **On**; click the button to turn session timeout off.

See the topic "Basic Navigation" in the *ArcSight Command Center User's Guide* for details on these fields.

Case Management Fields in the ArcSight Command Center

The fields `Reason for Closure` and `Category of Situation` are now on the Ticket section of the Attributes subtab of the Case Editor Initial Tab.

See the topic "Entering Case Attributes" in the *ArcSight Console Guide* for details on these fields.

Enhanced Geo Map

The Geo Map has been enhanced and is fully supported in both default and dark themes.

Text entry for multiple-field searches for ArcSight Investigate searches

From an event list, you can select **ArcSight Investigate Multiple Fields**. You can now enter the field's name in the **Search Fields** field. If present, the matching field is selected for you, which you then add to your list of fields to search.

See the topic, "Accessing ArcSight Investigate or ArcSight Investigate Search from an Event List" in the *ArcSight Command Center User's Guide*.

ArcSight Console Enhancements

Create an active channel of correlation events

If you right-click a standard rule, you can select **Create channel with filter**. This option creates a temporary channel populated with correlation events generated by that rule.

Read the topic, "Viewing Rules and their Correlation Events" in the *ArcSight Console User's Guide*.

Visually Enhanced Charts and Graphs

The pie and bar charts, and geo and event graphs, have been visually enhanced.

Cluster View icon on the Console toolbar

The Console toolbar contains the Cluster View icon to show the health of your distributed correlation cluster, based on icon color. It provides the link to the Cluster View dashboard on the ArcSight Command Center.

Refer to the topic, "Checking the Status of the Distributed Correlation Cluster" in the *ArcSight Console User's Guide*. See also the topic "Using the Distributed Correlation Dashboard" in the *Arcsight Command Center User's Guide*.

Text entry for ArcSight Investigate multiple-field searches

From an active channel or event details panel, you can select **ArcSight Investigate Multiple Fields**. You can now enter the field's name in the **Search Fields** field. If present, the matching field is selected for you, which you then add to your list of fields to search.

Read the topic, "Running ArcSight Investigate Searches" in the *ArcSight Console User's Guide*.

Distributed Correlation

ESM now supports distributed correlation, a mode in which you deploy multiple instances of correlators and aggregators to increase processing speed and provide failover processing. These instances reside in a grouping (a cluster) on one or more machines (nodes in the cluster).

You set up distributed correlation during installation and configuration. There is a new installation procedure specifically for distributed correlation. See "Using the Configuration Wizard - Distributed Correlation Mode", in the *ESM Installation Guide*.

Note: The default mode of ESM is now known as compact mode, to distinguish it from the new distributed correlation mode. Distributed correlation mode is not available on the appliance.

See "Distributed Correlation Mode" on page 16 under Usage Notes.

Refer to the topic "Distributed Correlation in ESM" in *ESM 101* for concepts and background information on distributed correlation.

Read the chapter "Installing and Configuring Distributed Correlation Mode for ESM" in the *ESM Installation Guide* for details on installing and setting up a distributed correlation cluster.

See the topics "Managing Distributed Correlation" and "Configuring Distributed Correlation" in the *ESM Administrator's Guide* for details on distributed correlation cluster management and configuration.

ESM Event Data Transfer Tool Now Provided with ESM

The ESM Event Data Transfer Tool is now provided as part of the ESM installation. It is no longer available as a separate software download.

There are changes to tool setup and memory recommendations. Otherwise, the tool functions exactly as it did when it was an separate software application.

The documentation for the tool now resides in the *ESM Administrator's Guide*. The text in the *ESM Administrator's Guide* supersedes the entire *HPE Security Arcsight ESM Event Data Transfer Tool User's Guide*.

See "Event Data Transfer Tool" in Appendix C in the *ESM Administrator's Guide*.

Cases

Enhanced Case Editor UI

The Case Editor user interface on the ArcSight Console was redesigned for ease of use. Only the basic options for attribute setting are exposed up front, and optional attributes are available through the More Options widget. A button bar with icons has replaced the old tabs/subtabs design. Refer to the topic, "Case Management and Queries," in the *ArcSight Console Guide*.

Any previous customizations on the Case Editor UI will migrate smoothly. Restoring customizations is a post-upgrade task. If you made changes to the UI, refer to the topic, "Restore Cases User Interface Customization" in the *ESM Upgrade Guide* to ensure that your changes are properly integrated with ESM 7.0.

Case Ownership by User Group

In addition to individual users as case owners, you can now assign user groups as case owners. A new field, `Owner Groups`, is added to the Attributes panel of the Case Editor UI.

Attaching dashboard, data monitor, or query viewer image to the case

Previously, you had to save the image to a file and then attach the file to the case - a two-step process. In this release, you can add the resource directly to the case.

Refer to the topic, "Attaching a Data Monitor, Dashboard, or Query Viewer to a Case" in the *ArcSight Console User's Guide*.

Integration with ServiceNow® IT Service Management (ITSM)

You can now export ESM cases to ServiceNow® ITSM from ServiceNow, Inc. Enter integration parameters during ESM installation or run Manager setup after initial install. Export case data from the ArcSight Console.

Refer to the topic, "Using External Case Management Systems" in the *ArcSight Console User's Guide*.

Verifying the Downloaded Installation Software

HPE provides a digital public key to enable you to verify that the signed software you received is indeed from HPE and has not been manipulated in any way by a third party.

Visit the following site for information and instructions:

https://h22253.www2.hpe.com/ecommerce/efulfillment/digitalSignIn.do

Upgrade Support

Direct upgrade to ESM 7.0 is supported from ESM 6.11.0, with or without Patch 1. Upgrade to the latest supported patch before upgrading to ESM 7.0. Refer to the *ESM Upgrade Guide* for more details.

For details on supported platforms, refer to the HPE ArcSight ESM Support Matrix available on Protect 724 (https://community.softwaregrp.com/t5/ESM-and-ESM-Express/ArcSight-ESM-Support-Matrix/ta-p/1587254).

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_2018201.

Vulnerability Updates

This release includes recent vulnerability mappings from the February 2018 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2983	updated Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT
Enterasys Dragon IDS	updated CVE
Cisco Secure IDS S1007	updated CVE
Juniper IDP update 3027	updated Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT, MSKB
McAfee Intrushield	updated Bugtraq, X-Force, MSSB, Faultline, CVE, Nessus, CERT
TippingPoint UnityOne DV9057	updated Bugtraq
IBM Security Host Protection for Desktops 3370	updated CVE
IBM Security Host Protection for Servers (Unix) 36.115	updated CVE
IBM Security Host Protection for Servers (Windows) 3370	updated CVE
IBM Proventia Network IPS XPU 36.115	updated CVE
IBM Proventia Network MFS XPU 36.115	updated CVE
IBM Proventia Server IPS for Linux technology 36.115	updated CVE
IBM RealSecure Server Sensor XPU 36.115	updated CVE
McAfee HIPS 7.0	updated CVE

Supported Versions for Distributed Searches

Distributed searches are supported only on ESM peers of the same version.

The only version that supports IPv6 connectivity and IPv6 data search is ESM 6.11.0 and above.

For more information about distributed searches, look at the *ArcSight Command Center User’s Guide* topic “Searching Peers (Distributed Search).”

Supported Platforms

See the ESM Support Matrix document available on Protect 724 (ESM Support Matrix) for details on ESM 7.0 platform and browser support.

Supported Languages

These languages are supported by ESM:

- English
- French
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean
- Russian

Support for ActivClient Issues

This information is provided as a courtesy to customers who are also using ActivClient and CAC cards for ESM authentication purposes. Problems may arise from multiple versions of ActivClient and CAC cards that have not been tested by HPE.

ActivClient releases are typically more frequent than ESM releases. In case of ActivClient issues, contact the ActivClient vendor for resolution. If you would like HPE ArcSight support to assist with monitoring the resolution; or have HPE ArcSight Support assist with opening a ticket with ActivClient Support, ActivClient will require us to have documentation from you that you are providing permission to HPE ArcSight Support to assist with monitoring the ActivClient case. Send the permission to us through email.

To the best of our knowledge, below is the information for logging a ticket with ActivClient Support. Note that the information may not be updated. Always check with your vendor for the latest information.

- For US Government customers, you can open a new ticket by sending an email to support-usa@actividentity.com.
- For other customers, you can open a new ticket by sending an email to support@actividentity.com

The following are typically required when you open a ticket with ActivClient Support:

1. Attach the ActivClient logs and diagnostics in the AI incident for review. The AI team will then send these logs to their Engineering team located in France. They need permission to view the log files (as per CFIUS requirements).
2. Collect any error messages displayed, as well as a Java console capture.
3. Provide findings from Advanced Diagnostics:
   a. Insert the SmartCard.
   b. Right-click the **ActivClient** icon in the lower right system tray.
   c. Select **Advanced Diagnostics**.
   d. Click **Diagnose** while the SmartCard inserted. Wait for the diagnostics to complete.
   e. Select **File > Save As** to save the information to a file.
   f. Send this file along with your ActivClient support request.
4. Provide information from ActiveClient logs:
   a. Open the ActivClient Console.
   b. Select **Tools > Advanced > Enable Logging**.
   c. Note the location of the log files. These are typically in `C:\Program Files\Common Files\ActivIdentity\Logs` or `C:\Program Files (x86)\Common Files\ActivIdentity\Logs`
   d. Restart the computer.
   e. Reproduce the issue.
   f. Provide all files generated in the logging directory along with your ActivClient support request.

Important:

As claimed by the vendor, all generated log files you provide to ActivClient Support to diagnose issues do not contain personally identifiable information that is considered sensitive. You are advised to check with the vendor about the specifics, to ensure that the content being transmitted does not include private information. For example, you should know what types of information are considered sensitive, and therefore not traced.

Usage Notes

ArcSight Command Center

Event search on FireFox ESR 52.6.0 using dark theme

If you are using the FireFox ESR 52.6.0 browser to do event searches on the ArcSight Command Center, note that with the dark theme, some drop-down menus are shown in daylight theme. The options, however, are readable even in dark theme.

Scroll Bar Issues with Google Chrome and Apple Safari

When using the Chrome or Safari browser to use the ArcSight Command Center, scroll bars may appear inside the data grid on the Storage Mapping tab when the page is loaded for the first time. Adding another row eliminates the scroll bars. Subsequently, adding or deleting rows works as expected.

To avoid this issue, use either Internet Explorer or Firefox.

Viewing Secure Operations Center Dashboard Using Edge Browser on Windows 10

If you observe that the SOC dashboard on Windows 10 does not display correctly in Edge (especially on high EPS systems), use IE 11, Chrome, or Firefox instead.

Using IE Browser on Windows 2016

Following are problems seen on the Command Center in this environment:

- Active channels and some options in the Administration menu will not load if you are using IE on Windows 2016.
- Fonts are showing as Times New Roman with IE 11.

Make sure that you use these browser settings:

- Enable cookies, and
- *Do not set* Internet Zone Security setting to High. Set it to Medium using your standard IE settings menu. If IE does not allow you to do it, use the Custom level option. Also add the ACC's URL to the list of trusted sites.

Refer to your browser documentation for instructions.

ArcSight Console

ArcSight Console Dark Theme

On the ArcSight Console, you can switch from the default daylight theme to dark theme. The dark theme is to reduce glare if you are using the Console in a dark room environment.

The following views are problematic on the dark theme in all operating systems:

Viewer Type	
Charts in Geo and Political views	When viewed in the dark theme, fonts on the charts are not visible.
Hierarchy maps	The Up and Down buttons are hard to see.

For the above, use the daylight theme instead.

Events from Event Broker

If you are viewing events on an active channel, you can double-click a specific event to get more event details from the Event Inspector.

One of the details you can select on Event Inspector is Agent ID. If you click Agent ID, you may get the following message:

```
Unable to load resource as this event was likely consumed via Event Broker
```

This is expected behavior. There is no associated resource for events consumed from Event Broker.

Using Windows 10

The ArcSight Console for ESM 7.0 is supported on Windows 10.

- The recommended processors for Windows 10 are either Intel Xeon x5670 or Intel Core i7.
- Use Internet Explorer as your preferred browser. This preference is set during Console installation time; or after Console installation using the User Preferences setting for Program Preferences.

  See also "Using the Edge Browser" on page 20 for related information.
- In ESM distributed mode, FIPS is not supported for use with ArcSight Console.

Oversized Pie Charts on Dashboards

On the Console, depending on the number of pie charts displayed on the dashboard, the charts may be cut off due to the window size or charts appear too small to read. Try changing the dashboard layout to Tab view, to view Data Monitor or Query Viewer stats.

ArcSight Console in FIPS Mode

You cannot use ArcSight Console in FIPS mode on Windows 10 or on a Mac.

Limit on Dashboards Being Viewed

The ArcSight Console may run out of Java memory if you are viewing dashboards above the limit, which is 15 dashboards. For Windows 10 in particular, limit from 7 to 10 dashboards. If you must view dashboards over the limit, try switching to classic charts in the Console's Preferences menu, under Global Options.

The number of dashboards you can view on the Console is directly proportional to the memory for the Console system.

If you want to view more dashboards than the limit:

1. Increase the memory size.
2. In the Console's installation directory, modify `/current/config/console.properties` by adding this property:

   ```
   console.ui.maxDashBoard=<new limit>
   ```

Follow instructions in the topic, "Managing and Changing Properties File Settings" in the *ESM Administrator's Guide*.

Distributed Correlation Mode

Configuration Changes Require Restart of All Services

After making any configuration changes in distributed mode, such as adding a node to a cluster, stop then start all services.

Active List Updates in Distributed Correlation

If you encounter a rule that is triggering excessively, where the rule's conditions include a `NOT In ActiveList` condition, especially if one or more of the rule's actions adds the relevant data to the active list that is being checked, you may need to consider other options for this condition. For example, try using the `OnFirstEvent` instead of `OnEveryEvent` trigger.

Similarly, if you have a pair of rules: the first rule populates a list, and the second rule depends on data being on that list, and both rules are expected to operate on the same event, the list may not be updated by the first rule in time for the second rule to trigger as expected.

Note that the order of rule processing is not guaranteed, so this scenario is not guaranteed to work in Compact Mode, either. If both rules are not expected to operate on the same event, but the events arrive too closely together, the second rule may still not trigger due to the active list not having yet been updated.

Services are not Started During an ESM Distributed Correlation Installation

Services do not automatically start during an ESM installation in distributed correlation mode, and the `setup_services.sh` command does not start services either. In that context, **setup_services.sh** performs set up of the services only. In this case, start services using `/etc/init.d/arcsight_services start` on the persistor node after configuring all services. Services are started as a part of installation in compact mode. See the *ESM Installation Guide* for details.

Stop and Start All Services if a Major Service is Stopped

In distributed mode, if a major service is stopped, stop all other services (`/etc/init.d/arcsight_services stop all`) and start them again (`/etc/init.d/arcsight_services start all`) as the user **arcsight** from the persistor node.

Major services include:

- aggregator
- correlator
- dcache
- manager
- mbus_control
- mbus_data
- repo

Otherwise you may see reduction in event processing speed.

Major services typically stop in these cases:

- Node reboots, or High Availability Failovers
- When you bring down one of the above services for administrative purposes.

If the ESM Console or Control Center cannot connect to ESM, you can confirm that a stopping and starting all services is necessary by running

```
/etc/init.d/arcsight_services status manager
```

If this command reports that Manager is `unavailable` or `initializing`, you should stop and start all processes.

Stopping Message Bus Services

Unlike other services, message bus control services can be stopped **only** from the persistor node. Also, when you run `/etc/init.d/arcsight_services stop mbus_control<#>` from the persistor, it will stop all instances of message bus data.

Hierarchy Map Data Monitor in Distributed Correlation - Not Recommended

The Hierarchy Map data monitor is performance intensive, therefore it is not recommended in distributed mode.

Converting IPv4 to IPv6 in Distributed Correlation Mode - Consult Professional Services

If you decide to convert your machine from IPv4 to IPv6, and your system is In distributed correlation mode, you must consult professional services. It is not recommended that you attempt this conversion yourself.

Data Monitor Filters

In distributed correlation ESM, optimization of data monitor filters is not supported.

Distributed Cache Inconsistency

In some cases, distributed cache nodes may lose contact with each other. This can occur due to network interruptions or as the result of heavily-loaded system. If this happens, not all data is shared between correlators, aggregators, and the persistor. As a result, some data monitors and dashboards will show no data, and there may be a possible drop in EPS.

To fix this, you must identify the distributed cache (dcache) instance(s) that are causing the problem and need to be restarted. Note that if the distributed cache becomes inconsistent, you will see `Connection to DC` in right upper corner of ArcSight Command Center Cluster View dashboard shown in red.

To restore the state of distributed cache cluster:

1. Go the ArcSight Command Center and navigate to the Cluster View Dashboard.
2. Check the audit events on the dashboard, and look for the service name **DCache connection is down**. There will be an associated service message, **"Hazelcast cluster is inconsistent . . . "**.
3. Hover your mouse pointer over the **"Hazelcast cluster is inconsistent . . . "** service message, and you will see the identity of the service that is causing the issue. For example:

```
Hazelcast cluster is inconsistent with repository. Check/restart
standalone DCache instances: [dcache2@<hostname>]
```

   In this example the name of the distributed cache instance that is causing the issue is *dcache2*. The hostname is the name of the machine in the cluster on which that particular distributed cache instance resides.

4. Restart the services. For example:

   ```
   /etc/init.d/arcsight_services stop dcache2
   ```

   ```
   /etc/init.d/arcsight_services start dcache2
   ```

Prevent Excessive Logging - Distributed Correlation Only

In a distributed correlation environment, excessive logging can occur in aggregator instance, correlator instance, and server logs. Example log messages you could see in this case (generally numerous `INFO` and `WARN` messages):

```
[2018-03-30 09:27:16,402][WARN ]
[default.com.arcsight.common.sessionlist.tuple.SessionTupleMap] SL NewSL
still overflowing after pruning, evicting keys
[2018-03-30 09:27:16,402][WARN ]
[default.com.arcsight.common.sessionlist.tuple.SessionTupleMap] SL NewSL
after evicting 1 keys, count = 10005
[2018-03-30 09:27:16,403][INFO ]
[default.com.arcsight.common.sessionlist.tuple.SessionTupleMap] Pruning
session tuple map now (NewSL- nonoverlapping) Size = 10006, capacity = 10000
[2018-03-30 09:27:16,403][WARN ]
[default.com.arcsight.common.sessionlist.tuple.SessionTupleMap] SL NewSL
still overflowing after pruning, evicting keys
[2018-03-30 09:27:33,732][WARN ]
[default.com.arcsight.common.sessionlist.SessionListCache] Attempt to delete
entry that does not exist:DefaultTuple[accept_7460385]
[2018-03-30 09:27:33,733][WARN ]
[default.com.arcsight.common.sessionlist.SessionListCache] Attempt to delete
entry that does not exist:DefaultTuple[accept_9904399]
```

This can cause logs to roll over quickly, which can result in the loss of desired log information.

To prevent excessive logging:

1. Locate the property files for all aggregator instances, all correlator instances, and the server.

   ```
   /opt/arcsight/var/config/aggregator<all_instances>/aggregator.properties
   ```

   ```
   /opt/arcsight/var/config/correlator<all_instances>/correlator.properties
   ```

```
/opt/arcsight/manager/config/server.properties
```

2. As user *arcsight*, in all instances of `aggregator.properties`, all instances of `correlator.properties`, and in `server.propertes`, set these properties to the parameter value **3**:

   ```
   log.channel.file.property.class.com.arcsight.common.sessionlist.SessionListCache=3
   ```

   ```
   log.channel.file.property.class.com.arcsight.common.sessionlist.tuple.SessionTupleMap=3
   ```

3. Restart all services:

   ```
   /etc/init.d/arcsight_services stop all
   ```

   ```
   /etc/init.d/arcsight_services start all
   ```

Large Lists and Multi-Mapped Active Lists with Over 10,000 Entries Per Key - Not Supported

Large lists (those with over 1 million entries) are not supported on a distributed correlation system. Also, multi-mapped active lists with more than 10,000 entries per key are not supported.

Using the Edge Browser

- The ArcSight Console Help does not support Edge as the preferred browser. See also "Using Windows 10" on page 15 for related information.
- The Tools command does not work with the Edge browser due to a certificate issue.
- On the ArcSight Console and ArcSight Command Center, viewing PDF reports on the Edge browser is not supported. Either view the PDF report in Internet Explorer, or output the report in HTML format.

Oversized Event Graphs

In both the ArcSight Console and ArcSight Command Center, if you are viewing the Event Graph dashboard and there are too many events, the graph will be too large to fit the display.

If this happens, reduce the number of events in the data monitor used by the dashboard. You do this by refining the filter used by the data monitor.

Full Text Search

By default, ESM supports full text search. This enables you to search on any word of any text field of any event. Disk space is required for storing events for full text search, approximately 40 to 50% more than if full text search were disabled.

The feature is controlled by the property:

```
fulltext.search.enabled
```

If you want to disable full text search, enter this setting in server.properties:

```
fulltext.search.enabled=false
```

Then restart the Manager. For important details on editing properties files, refer to the topic, "Managing and Changing Properties File Settings" in the *ESM Administrator's Guide*.

Resource Validation

Resource validators for IP and MAC address data have been tightened. After an upgrade from 6.9.1, any resources containing incorrect IP addresses or address ranges will be invalidated. The same goes for non-unique MAC addresses. You need to rebuild the invalidated resource with the correct address formats.

You should also look at ESM packages created in previous releases, which may contain assets with the wrong address formats. Imported assets with the wrong address formats are invalidated. These should be fixed after they are imported.

For information on supported IP address range formats, refer to the *ArcSight Console User's Guide*'s topic on "IP Address Ranges."

ESM Peer Certification for Content Synchronization

Peering for ESM content synchronization is automatically mutual, so a group of peers may be enabled from a single Manager. Content Management is certified with up to five subscribers, with one additional Manager as a publisher.

> **Caution:** For ESM content synchronization, only ESM peers of the same version are supported. Application of Service Packs, Patches and Hotfixes alter version numbers. You should carefully consider the impact to synchronization during change management.

For information about content management, refer to the following:

- "Creating or Editing Packages" and "Supported Package Resources for Content Synchronization" in the *ArcSight Console User's Guide*

- "Content Management" and "Configuring Peers" in the *ArcSight Command Center User's Guide*

ESM and Logger Connectivity

ESM in pure IPv6 mode will not connect with Logger 6.3 or earlier releases.

Actor Model Import Connector

The Actor Model Import Connector for Microsoft Active Directory allows you to develop a model import connector to import actor model data. The Actor Model Import Connector for Microsoft Active Directory to install for ESM 7.0 is version 7.7.0.8047.0. This new connector can be configured in a dual stack or pure IPv6 environment. Refer to the *Actor Model Import Connector for Microsoft Active Directory Configuration Guide*.

See the ESM Support Matrix document available on the Protect 724 site for details on ESM 7.0 supported platforms.

> **Caution:** Install and use the Actor Model Import Connector for Microsoft Active Directory that is provided with the ESM 7.0 release. That is the version of the connector that is tested and certified to work with ESM 7.0. Do not use previously-supplied versions of the Actor Model Import Connector for Microsoft Active Directory with ESM 7.0.

Asset Model Import FlexConnector

The Asset Model Import FlexConnector supports the ability to create and manage the Asset Model within ESM. The Asset Model Import FlexConnector allows you to develop a model import connector to import asset model data from a file. This enables you to create and maintain ESM Network Model data and keep the data in sync with the data in your Asset Management system. The Asset Model Import FlexConnector to install for ESM 7.0 is version 7.7.0.8048.0. This new connector can be configured in a dual stack or pure IPv6 environment. Refer to the *Asset Model Import FlexConnector Developer's Guide*.

Earlier Asset Model Import Connector versions enabled the creation of IPv4 assets. This new version enables the creation of both IPv4 and IPv6 assets.

See the ESM Support Matrix document available on the Protect 724 site for details on 7.0 supported platforms.

> **Caution:** Install and use the Asset Model Import FlexConnector that is provided with the ESM 7.0 release. That is the version of the connector that is tested and certified to work with ESM 7.0. Do not use previously-supplied versions of the Asset Model Import FlexConnector with ESM 7.0.

Forwarding Connector

The ArcSight Forwarding Connector can receive events from a source Manager and then send them to a secondary destination Manager, an ArcSight Logger, or a non-ESM destination. Only the Linux executable applies to ESM 7.0.

The Forwarding Connector is capable of forwarding events with IPv4 or IPv6 addresses. If the destination ESM supports both IPv4 and IPv6 addresses, then the address fields like Attacker, Source, Target, and so on, will be used. If the destination does not support IPv6 addresses, then the deviceCustomIPv6Address fields 1-4 will be used.

See the ESM Support Matrix document for Forwarding Connector version on ESM 7.0.

90Meter Cards and Firefox Browser

If you are using Firefox 45.1.1 with 90Meter cards for authentication, you may encounter an error stating that `x86\litpkcs11.dll` is not supported. If this occurs, contact the 90Meter vendor's support for additional assistance in configuring Firefox to resolve this issue.

> **Caution:** Do not use Firefox 45 and later with Windows 8.1 Enterprise. Use Firefox v38.0.1 ESR instead.

For information on 90Meter cards supported in ESM releases, refer to the ESM Support Matrix.

Running ArcSight Investigate Searches

ESM has a set of supported browsers in the ESM Support Matrix. These refer only to browsers for use with the ArcSight Command Center. If you are running ArcSight Investigate searches, use only the browsers mentioned in the section "ESM Support of Other ArcSight Products/Components" in the ESM Support Matrix. Locate the line item for ArcSight Investigate.

General search instructions

- If the search query is on an empty field that is an Integer or Number data type, the query should be of the format

  `<FieldName> = '',Null`

  For example

  sourcePort = '',Null
- When launching ArcSight Investigate integration command, use the default port 443, unless the port is configured differently.
- If you are a non-administrator user in ArcSight Investigate, you may not be authorized to view

certain field values. If you are searching such fields, you will see an Unknown column error. If you are a non-administrator user in ArcSight Investigate and you are not authorized to execute a search query, you will see an error that says you are not authorized.

- If you open multiple browser sessions for ArcSight Investigate searches, you will eventually observe slowness in browser response. The threshold is from 5 to 6 sessions. If you open more than that, you should close some browsers.
- ArcSight Investigate search results are case-insensitive. That is by design.

Searching for Attacker Address and Target Address Based on Originator

This information applies to ArcSight Investigate searches executed from the ArcSight Console and from the ArcSight Command Center. The ESM derived fields Attacker Address and Target Address are not found in ArcSight Investigate. Instead, ArcSight Investigate uses the primary fields Source Address and Destination Address.

Assume these values for the following fields:

```
Attacker Address = 1.1.1.1
Target Address = 2.2.2.2
Source Address = 1.1.1.1
Destination Address = 2.2.2.2
```

If the Originator is	And you are searching	ArcSight Investigate returns
Source	Attacker Address 1.1.1.1	sourceAddress = 1.1.1.1
Source	Target Address 2.2.2.2	destinationAddress = 2.2.2.2
Destination	Attacker Address 2.2.2.2	destinationAddress = 2.2.2.2
Destination	Target Address 1.1.1.1	sourceAddress = 1.1.1.1

Searching for empty fields

This information applies to ArcSight Investigate searches executed from the ArcSight Console and from the ArcSight Command Center.

If the empty field type in ESM is	Example	Use this search syntax in ArcSight Investigate
String	Name	`Name=' ', Null` **Note:** Use two single quotes without spaces after the equal sign.
Integer or Number	SourcePort	`SourcePort=' ', Null`

Permission for searches

- If you are a non-administrator user in ArcSight Investigate, you may not be authorized to view certain field values. If you are searching such fields, you will see an `Unknown column` error.

- If you are a non-administrator user in ArcSight Investigate and you are not authorized to execute a search query, you will see an error that says you are not authorized.

For more information, refer to the *ArcSight Investigate Administrator's Guide*.

Search error due to complex characters

Some field values with complex characters may instruct you to fix the query manually.

When invoking ArcSight Investigate searches from ESM with values that contain both single and double quotes, truncate the value in the ArcSight Investigate Search Input after the second quote symbol. For example, if you ESM value of the Name field is:

```
my_esm_value'with"single'and"double_quotes
```

and it got inserted into Investigate as:

```
Name = 'my_esm_value'with"single'and"double_quotes
```

then truncate it after the single quote:

```
Name= 'my_esm_value'
```

and replace = with starts with:

```
Name starts with 'my_esm_value'
```

Supported ESM fields

Below is a list of ESM fields that are supported in ArcSight Investigate searches. For ESM fields that are not on this list, the right-click Investigate options are disabled.

List of ESM Fields Supported in ArcSight Investigate Searches

ESM Fieldname
agentAddress
agentDnsDomain
agentHostName
agentMacAddress
agentTranslatedAddress
agentType
agentVersion
applicationProtocol
bytesIn
bytesOut
categoryDeviceGroup

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
categoryDeviceType
categoryObject
categoryOutcome
categorySignificance
categoryTechnique
destinationAddress
destinationDnsDomain
destinationHostName
destinationMacAddress
destinationNtDomain
destinationPort
destinationProcessId
destinationProcessName
destinationServiceName
destinationTranslatedAddress
destinationTranslatedPort
destinationUserId
destinationUserName
destinationUserPrivileges
deviceAction
deviceAddress
deviceCustomFloatingPoint1
deviceCustomFloatingPoint2
deviceCustomFloatingPoint3
deviceCustomFloatingPoint4
deviceCustomIPv6Address1
deviceCustomIPv6Address2
deviceCustomIPv6Address3
deviceCustomIPv6Address4
deviceCustomNumber1

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
deviceCustomNumber2
deviceCustomNumber3
deviceCustomString1
deviceCustomString2
deviceCustomString3
deviceCustomString4
deviceCustomString5
deviceCustomString6
deviceDnsDomain
deviceDomain
deviceEventCategory
deviceEventClassId
deviceExternalId
deviceFacility
deviceHostName
deviceInboundInterface
deviceMacAddress
deviceNtDomain
deviceOutboundInterface
deviceProcessId
deviceProcessName
deviceProduct
deviceSeverity
deviceTranslatedAddress
deviceVendor
deviceVersion
eventOutcome
fileHash
fileId
fileName

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
filePath
filePermission
fileSize
fileType
flexNumber1
flexNumber2
flexString1
flexString2
name
oldFileHash
oldFileId
oldFileName
oldFilePath
oldFilePermission
oldFileSize
oldFileType
requestClientApplication
requestMethod
requestUrl
sourceAddress
sourceDnsDomain
sourceHostName
sourceMacAddress
sourceNtDomain
sourcePort
sourceProcessId
sourceProcessName
sourceServiceName
sourceTranslatedAddress
sourceTranslatedPort

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
sourceUserId
sourceUserName
sourceUserPrivileges
transportProtocol

SSL Configuration Properties Moved to esm.properties

SSL configuration properties have been moved from `$ARCSIGHT_HOME/config/server.properties` to `$ARCSIGHT_HOME/config/esm.properties`.

ESM Log Files Moved to `/opt/arcsight/var/logs`

ESM log files have moved from `/opt/arcsight/manager/logs` to `/opt/arcsight/var/logs`.

Post Upgrade - Install ArcSight SocView and ClusterView Packages

The content packages are installed automatically when you perform a new ESM installation (ClusterView content package is installed if you are using ESM in distributed mode). However, when you upgrade your ESM system, the content packages are not installed automatically. You can install these packages from the ArcSight Console any time after the upgrade.

For instructions on installing ESM packages, refer to the topic "Installing or Uninstalling Packages" in the *ArcSight Console User's Guide*.

High Availability - Spectre and Meltdown Patches Required for RHEL 6.9 and 7.3 and CentOS 6.9

For HA, you must have the Spectre and Meltdown patches installed on RHEL 6.9 or 7.3, or on CentOS 6.9.

> **Note:** HA does not support CentOS 7.3 for ESM 7.0.

To check for these patches:

To verify that you have the patches on RHEL and CentOS 6.9, check the kernel version:

```
# uname -r
```

```
2.6.32-696.20.1.el6.x86_64
```

This kernel version or greater indicates you have the Spectre and Meltdown patches.

To verify that you have the patches on RHEL 7.3, check the kernel version:

```
# uname -r
```

```
3.10.0-514.36.5.el7.x86_64
```

This kernel version or greater indicates you have the Spectre and Meltdown patches.

`arcsight_services restart` No Longer Supported

The command:

```
/etc/init.d/arcsight_services restart <service>
```

is no longer supported.

To start services, use a combination of stopping the individual service, and then start all services. For example, to restart the Manager, you must stop the Manager, and then start all services.

In this example, the commands are:

1. Stop the Manager:

   ```
   /etc/init.d/arcsight_services stop manager
   ```

2. Start all services:

   ```
   /etc/init.d/arcsight_services start all
   ```

Rule Recovery Timeout Possible During High EPS

Checkpoint rule recovery can timeout if high EPS occurs. To attempt to prevent this timeout, set the `rules.recovery.time-limit` property in `server.properties` to a higher recovery time limit. This will enable the server to continue to load events from the database for checkpoint. The default value for the `rules.recovery.time-limit` property is 120 seconds (two minutes).

Note that the timeout can still occur after increase the value of the `rules.recovery.time-limit` property, due to overall system load, high EPS, or a large number of rules. Also, the Manager will take longer to start up if the recovery time limit is increased.

For details on editing the `server.properties` file, see the "Editing Properties Files" topic in the ESM Administrator's Guide.

Unsupported Features in This Release

This information applies to ESM Software and ESM Express with ESM 7.0.

The following features are not available in this release:

- Logs sent with sendlogs from ArcSight Command Center do not include logs from a distributed ESM setup.
- Conversion from default (non-FIPS) to FIPS SuiteB mode is *not* supported in compact or distributed ESM.
    - A FIPS-140 setup *can* be upgraded to compact ESM, and from there, conversion to distributed ESM is supported.
    - Conversion from default (non-FIPS) to FIPS 140 mode *is* supported only in compact ESM.
    - Conversion from default (non-FIPS) distributed ESM to FIPS 140 distributed ESM is *not* supported.
- Pattern Discovery is not supported in distributed ESM; fewer events are processed compared to compact mode.
- Hierarchy Map data monitor is not supported in distributed ESM
- Partially cached active lists run out of memory.
- Optimization of data monitor filters is not supported in distributed ESM. It still works in compact ESM.

The following features are not supported in this release and are no longer available.

- Event Reconciliation and Session Reconciliation data monitors are deprecated and removed from ArcSight Console. They are listed in the Console after ESM upgrade but these data monitors are no longer available.
- Superindexes
- TRM integration commands from the ArcSight Console
- The NSP device listener as a Destination option in the Forwarding Connector
- The Java Authentication and Authorization Service (JAAS) external authentication mechanism
- ArcSight IdentityView Solution
- Integration with HPE OM and HPE OMi is no longer supported. The rule action to send commands to HP Openview Operations is no longer supported. The related audit event, `rule:314`, has been removed. HPE OM and HPE OMi are no longer supported as destinations for the Forwarding Connector.

The following are not supported in this release:

- SUSE Linux
- ESM 6.x Migration Tool, G7 to G9 ESM Express appliance
- ESM 6.x Migration Tool, G8 to G9 ESM Express appliance
- Resource Migration from ESM 5.x
- Hadoop Connector
- ArcSight Risk Insight
- Reputation Security Monitor (RepSM) 1.5x Solution, including use of RepSM Model Import Connector 7.1.7.7607.0
- Integration with HPE Service Manager, including use of the ArcSM connector
- Threat Central Solution, including use of Threat Central Model Import Connector
- Integration with Remedy ticketing software

Using external authenticators in pure IPv6 environment is not supported

If Active Directory, LDAP, or RADIUS is installed in a pure IPv6 environment, communications are *not* supported with ESM in pure IPv6 or dual stack environment.

However, if Active Directory, LDAP, or Radius is installed in dual stack, communications *are* supported with ESM in pure IPv6 or dual stack environment.

The following integrations are not supported in a pure IPv6 environment:

- External links to Console Help
- ArcSight Investigate 2.10 and Event Broker 2.20 do not support being deployed in an IPv6 only environment. These products support event data that contains IPv6 addresses, however.

ESM Integrations:

The following ESM integrations are not supported. If you are using any of the following, *do not upgrade* to ESM 7.0:

- Integration with iDefense. Do not run the `idefensesetup` command to launch the iDefense wizard.
- Integration with BMC Remedy, including use of the ArcRemedyClient connector
- Integration with Risk Insight

ESM Service Layer APIs:

The following deprecated methods have been removed from the ESM Service Layer APIs:

- public List insertResources(List resources, int relationshipType, R parent) throws ServiceException;
- public List findAll() throws ServiceException; public boolean containsDirectMemberByName1(String groupId, String targetId, String name) throws ServiceException;
- public boolean containsDirectMemberByNameOrAlias1(String groupId, String targetId, String alias, String name) throws ServiceException;
- public boolean containsDirectMemberByName(String groupId, String targetId) throws ServiceException;

Fixed Issues

The following issues are fixed in this release.

Analytics

Issue	Description
NGS-26715	In ESM distributed mode, the property settings for rule engine optimization are no longer limited to server.properties. Changes must be additionally entered in the correlator.properties. In addition to information stored in server.log, information is also stored in correlator.log. For more details, in the ArcSight Console User's Guide, see the topic, "Specifying Rule Conditions" under Rules Authoring.
NGS-24731	In some cases, duplicate event IDs can occur. This issue has been fixed.
NGS-23500	HTML reports embedded in email were not displaying Unicode Standard characters appropriately. This issue has been fixed.
NGS-23188	Correlation performance could be negatively impacted when datamonitor.event.buffer.size is small. Thread allocation has been corrected to prevent this.
NGS-22810	A synchronization problem resulted in Session Lists failing to purge and ConcurrentModificationExceptions in the logs. This issue has been fixed.
NGS-22398	The change of the Field Set used by Rule Action has caused the previous events' values to be lost. This issue has been fixed.

ArcSight Console

Issue	Description
NGS-26204	Previously, user could link to root groups like All Cases and this would cause the system to crash. Now, this linking cannot occur.
NGS-26072	Sorting on any fields in the active channel can result in performance issues. A Console property, console.ui.channel.disable.sorting, is provided so that sorting on any field is disabled except for End Time or Manager Receipt Time. This is documented in the ArcSight Console User's Guide, in the topic Best Practices to Optimize Channel Performance.
NGS-25146	Previously, ESM had a restriction on Console logins from hosts with certain fully qualified domain names. That restriction no longer exists.
NGS-25030	The image editor now fully supports dark theme.
NGS-24928	If you launch the Arcsight Investigate integration command from a blank field (a field with an empty value) in either the ArcSight Console or ArcSight Command Center, Arcsight Investigate 1.01 and ArcSight Investigate 1.10 display no data results. Workaround: Change the search condition value for the blank field in the ArcSight Investigate search window. For ArcSight Investigate 1.01: '',NONE for string value; 0,NONE for Integer value For ArcSight Investigate 1.10: '',NULL for string value; 0,NULL for Integer value
NGS-24422	The following are issues with the ArcSight Console when it is set to the dark theme. In some areas, the issues are visual only and will not affect functionality. 1. The Print option in the Geographic Event Graph data monitor is not supported. 2. For the Last State data monitor added to the dashboard, configure and color chooser are not supported. 3. In Hierarchy Map data monitor added to dashboard, color chooser is disabled. 4. Use Case and Network Model Wizard are not supported. 5. Print rule definition option from the Rules resource tree will not be in dark theme.; 6. Advanced options for circular layout of resource graph will not be in dark theme. 7. Hide Empty Triggers button shows font in white color after selection. This happens only in Windows Server 2012R2. 8. Mouse over on menu bar will not be in dark theme. 9. Drop down arrows in some dialogs will not be in dark theme.

Issue	Description
NGS-23877	When using dual monitors (multiple displays), the monitors displayed vertically (not side by side), and the pop up menu displayed in the wrong monitor. This issue has been fixed.
NGS-23868	Fixed issue where Print Spooler service needs to be running in Windows for Console to start. Now no need to have Print Spooler service running.
NGS-23800	Console in Windows 8.1 the CPU will jump to around 55% from 35%. Apart from this there will not be any other side affects.
NGS-23640	ArcSight Investigate searches on the Severity field may not work in some cases. ESM enhances the value received from the connector, and thus the value may not be same in ESM as it is in ArcSight Investigate.
NGS-23563	Issues with search commands containing special characters. Workaround: When a content-based ArcSight investigate command is launched containing values with special characters (such as the ampersand), be sure to enclose these values in single quotes in the ArcSight Investigate search query before executing the search.
NGS-23535	ActivClient 7.1.0.168 works on Windows 10; while this version of ActivClient is no longer available, ActivClient 7.1.0.190 was verified and worked. Note that the verification was completed for the Console and FireFox browsers. The verification for Internet Explorer and Chrome browsers was not possible due to lack of CAC cards.
NGS-22979	Due to a limitation in storage space, sending over a certain amount of characters to the ESM Storage System caused the input to be trimmed without any user warning. To address this, an error message has been added in order to notify the user whenever the data they are inputting in the case editor breaks the permitted limit.
NGS-22141	Non-administrators can now see who owns cases and who locked them. The Cases resource is exposed in the Console and in the ArcSight Command Center. Note that this feature can be disabled by setting the Console property console.ui.case.owners.lockedby.visible.to.all to false.
NGS-21410	When editing a session list, setting the field 'Entry Expiration Time' to a value of 24 days or higher caused the user interface to display negative values that did not correspond to expectations. To workaround this, a limit of 24 days (576 hours) has been established. If the user attempts to enter a value higher than the limit, a message displays the error and the field is reset. Optionally a value of -1 is used to represent unlimited time.
NGS-21258	This feature request would improve ease of use when customizing ESM to process large or complex reports.

ArcSight Manager

Issue	Description
NGS-26710	The Manager does not display or store custom zones correctly when aggregation is enabled. This issue has been fixed.
NGS-26229	Configuration of ESM's Certificate Revocation management to use LDAP would result in an error in the logs. This issue is now fixed, however functionality of CRLs via LDAP is not guaranteed.
NGS-24943	As a result of a velocity library upgrade, the velocity log file was missing. For the Manager: 1. Velocity.log is located in the following folder: /opt/arcsight/var/logs/manager/default *For distributed mode, velocity.log is under: - /opt/arcsight/var/logs/manager/default - /opt/arcsight/var/logs/correlator - /opt/arcsight/var/logs/aggregator 2. By default, the logging is on Warn level. The level can be changed to Info or Debug by setting the property in (Arcsight_Home)/config/velocity.properties (requires restart): esm.runtime.log.logsystem.avalon.level=debug *For distributed mode, the change has to be made on all nodes. For the ArcSight Console: 1. Velocity log is located in the following folder: (Console_home)\current\logs 2. By default, the logging is on Warn level. The level can be changed to Info or Debug by setting the property in (Console_Home)/current/config/velocity.properties (requires restart): esm.runtime.log.logsystem.avalon.level=debug;
NGS-24725	Asset auto-creation did not work. The cause was that the group versionID was not changed, even though the name was modified. This was fixed by modifying the group versionID.
NGS-24435	In compact mode, multi-mapped active lists that contained a large number of entries under a single key could cause lists to load slowly and result in a long interval during manager startup. This issue has been fixed.

Issue	Description
NGS-24408	The behavior of email notifications for empty reports is clarified. The default behavior is for email report notifications to be sent whether or not the report had data. The property setting to customize this behavior is with the property setting, report.scheduler.notify_empty_reports If set to false, email notifications are not sent for empty reports. This property is described in the topic, Setting Default and Custom Report Parameters in the ArcSight Console User's Guide. See the description of the Email To report parameter.
NGS-23567	Customers want the ability to search for Cases using a REST API. A different approach was proposed and agreed upon by the customer: the Case Search functionality has been provided via integration with ServiceNow, an external Case Management System.
NGS-23463	When events were manually annotated, the annotation time used was that of the Console. This caused issues if there was a discrepancy between the operating system clock on the Console machine and the operating system clock on the Manager server. As a result, annotation modification time could be earlier than event MRT. The annotation time is now that of the operating system clock on the Manager server.
NGS-23454	The notification tables stopped being purged when the table grew large when numerous notifications were run. This issue has been fixed.
NGS-23321	In some cases, after restarting Manager the arc_event_annotation table was corrupted. This issue has been fixed.
NGS-23052	A user account with a password containing an ampersand could not login to the manage.jsp. This issue has been fixed.
NGS-22470	In rare cases, the upgrade of the High Availability feature may report it was successful when it actually failed. This issue has been fixed.
NGS-22379	The import operations of resource archives containing a Case with originalAgentMacAddress field populated were failing due to an XML parsing error. This issue has been fixed.
NGS-21656	A rule is not fired when the condition contains special characters. The correct way to use a special character like [is to escape the character.

Issue	Description
NGS-16198	Customers could not import content packages greater than 100MB. Workaround: To import content packages greater than 100MB, set the following properties in the server.properties file with the values shown: persist.file.size.total.max=200 persist.file.size.max=200 Note: In distributed mode, the persistor node must be restarted after you set this parameter.
NGS-14963	The server warning message, limit of agent threads was exceeded, is now sent to the error notification email address (as long that that address is provided).
NGS-14055	Using the script export_system_tables.sh displayed the username and password information used for this process. This data should not be exposed. A new parameter was introduced for this script to hide the username and password information. Workaround: To hide these values, add the word "hidden" as the fifth parameter when executing this script.

CORR-Engine

Issue	Description
NGS-26189	Preservecaseevent.sh scripts, which moved case events from arc_event table to arc_event_p table in the Oracle database have been removed and are not supported.
NGS-24425	When large number of events were sent to ESM, this could cause a corrupted data chunk due to a BufferUnderflowException and a BufferOverflowException. As a result, some event fields such as Request Url could not be displayed in ArcSight Command Center and the Console. This issue has been fixed.
NGS-21427	For killing long running MySQL queries it is recommended to use the KILL statement (do not confuse this with the UNIX kill command). MySQL's statement will add a flag for the query to be stopped in one of the next thread's cycles which can take a while to execute. In case of a stalled thread in which the MySQL's KILL command could not stop the query, a MySQL restart is needed.

Command Center

Issue	Description
NGS-26699	The cases dashlet will load a maximum of 500 cases. If the user has more than 500 cases, the cases beyond the 500 maximum are ignored. Workaround: View cases in the Case Resource browser, which has higher limit.
NGS-25933	Note that in older versions of the Mozilla Firefox browser, the intersection of a latitude 0 degrees and a longitude 0 degrees is represented in scientific notation.
NGS-25623	On the ArcSight Command Center, there are no saved searches on the user interface, even if the files are showing in /opt/arcsight/logger/userdata/logger/user/logger/data/savedsearch. The 'Saved Searches Files' tab in 'Saved Searches' option of the 'Administration' menu now displays the correct files for all cases.
NGS-24937	Data Monitors in the ArcSight Command Center do not display the data collection start time and the data last received time. Data Monitors and Query Viewers now display Data time range and last refresh time in footer of Data dashlet.
NGS-23702	A user logging into the ArcSight Command Center may be disconnected frequently when there is a inconsistency of time between components of ESM. This issue has been fixed.
NGS-23701	A user logging in the ArcSight Command Center may be disconnected frequently when there is a inconsistency of time between components of ESM. This issue has been fixed.
NGS-23546	A user logging in the ArcSight Command Center may be disconnected frequently when there is a inconsistency of time between components of ESM. This issue has been fixed.
NGS-23137	OTP session for Logger integration command does not work the first time, but works fine next time. The session will time out as usual, then the user needs to log in again to continue.
NGS-20016	All tabs in the Saved Searches option of the Administration menu show only the records created or generated by the current logged in user. Before, other user data was displayed as well. This issue has been fixed.
NGS-15018	The ArcSight Command Center was showing End Time as epoch if in the query the "Display Name" heading is not "End Time". End Time is now displayed in a readable format.
NGS-10943	Added a login banner dialog in the ArcSight Command Center to display the text from the file specified in the "auth.login.banner" property in server.properties. This same login banner setting also applies to ArcSight Console. The server property is described in the ESM Administrator's Guide. See the topic "Setting up a Custom Login Banner."

Installation and Upgrade

Issue	Description
NGS-24323	The install-time check for a "localhost" entry in /etc/hosts correctly handles more variations of tabs and spaces.
NGS-23575	ESM server can crash with too many connections as process limits get reset on reboot. Workaround: The following steps need to be run as root user: /opt/arcsight/manager/bin/remove_services.sh #before install/uninstall /opt/arcsight/manager/bin/setup_services.sh #after install/uninstall
NGS-22158	The Remote Authentication Dial-In User Service (RADIUS) protocol RFC 2865 is now supported.

Open Issues

This release contains the following open issues.

Analytics

Issue	Description
ESM-49283	When defining filters, for a hostname to be properly interpreted from the Request URL, the host name needs to be enclosed either within // (double slash) and / (single slash); or within // (double slash) and : (colon). For example: https://hostname.example.com:8443 Such an event is retrieved correctly with the Request Url Host Is Not Null filter. Do not use a filter with a condition that says Request Url Host != Null because != makes the filter invalid.
ESM-39405	If you create a report whose name contains Chinese characters, and then send the report as a PDF attachment, the received email does not display the attachment's name correctly. The content of the report is correct; only the email attachment field that displays the name of the attachment is affected.
NGS-27142	When a system is heavily loaded, and in rare cases, the update on rules actions are not propagated to aggregators.
NGS-27117	In distributed mode join rules may fire multiple times even though trigger set for taking action in First Threshold.
NGS-27069	In ESM 7.0 distributed mode, the event annotation fields will not show up in DMs. Also, such fields cannot be used in the standard and joined Rules.
NGS-27045	HTML reports embedded in email were not displaying Unicode Standard characters appropriately.

Issue	Description
NGS-26720	If you move a rule group from the Real-time Rules folder to another folder (and delete from Real-time Rules), and then you schedule that new rule group, when rules in this new group are triggered, you will notice that the generated correlation events show the wrong information: the URI is still remembered as the old Real-time Rules folder instead of the new URI.
NGS-26663	On distributed ESM, when the cluster is installed or started up, the Event Throughput dashboard takes some time to display the graph on the top.
NGS-26380	In the Last State data monitor, the Override Status and Remove Entry options are not working correctly.
NGS-26376	In some cases, a Rule Action that create a new Case may fail to append a Note to the newly created Case. If this happens, an audit event (Device Event Class = rule:306) will incorrectly state that creating a Case failed. In reality, the Case is successfully created; however, it will not have a Note appended to it.
NGS-25756	An ESM system that uses Partially Cached Active Lists (PCALs) runs out of memory in distributed mode. Workaround:; If you have PCALs in your content and need to use them in distributed mode, you can: 1. Export the PCALs to a package (use the "export" format). 2. Extract the PCAL package's (.arb file) XML file. 3. Edit the XML to replace all occurrences of <partialCache>true</partialCache> with <partialCache>false</partialCache> 4. Change the versionID for the package resource and all PCALs you modified (you can simply change the last character of the version ID to another character). 5. Reconstitute the package (put your updated XML file back in). 6. Import the updated package and check to make sure the modified active lists are no longer partially cached. For examples on editing the XML files for ArcSight packages, see https://hpe-sec.com/foswiki/bin/view/ArcSightActivate/TActivateCustomerBaseTemplates#XML_Hacking_Method
NGS-24957	The GetSessionData function that uses sessionlist with multiple keys may show an incorrect result.
NGS-7181	Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.

ArcSight Console

Issue	Description
NGS-27187	Sometimes the notifications view may not render properly. Workaround: Close the notifications view and open it again.
NGS-27091	Drill down from stacked bar charts does not work as expected.

Issue	Description
NGS-27081	Performing Arcsight Investigate multiple search action from channel while data is loading may not launch Investigate Application. Pause the channel and then perform the action.
NGS-27004	For queries to work for non-administrators, the user group needs R (read) access to the /All Filters/ArcSight System group.
NGS-26915	The "Analyze Channel" option on the channel's right-click menu might be disabled sometimes on the bar chart or pie chart. On the second attempt, the option will be enabled.
NGS-26842	After ArcSight Console upgrade, if you notice that channels or dashboards are not displaying in the upgraded version, then copy the user's ast file from the previous version ArcSight Console home to the new version's ArcSight Console home. Now, previously opened views such as channels or dashboards display.
NGS-26291	To remove automatically created filters for agents add this property: console.ui.delete.agent.filters=true in the console.properties file. This property will not affect filters that were moved, or if the name or event condition has been modified.
NGS-26022	Using the ArcSight Console on macOS High Sierra 10.13 in IPv6 environment is not supported. In this case, use macOS Sierra 10.12.
NGS-25631	Unlike the ArcSight Console, which prevents the import of packages that already exist in the system, the Package Push operation of the Content Management feature in the ArcSight Command Center does not verify that a package exists on Subscribers. In some cases, pushing a modified package can cause resource corruption.
NGS-23639	When you start ArcSight Investigate from ESM on string based fields containing leading or trailing spaces, the search will fail. Workaround: In such cases, manually fix the spaces before or after the value.
NGS-23554	If you launch the Arcsight Investigate integration command from a blank field (a field with an empty value) in either the ArcSight Console or the ArcSight Command Center, Arcsight Investigate 1.01 displays no data results. Workaround: Change the search field value to: ",NONE for string value; 0,NONE for Integer value
NGS-23489	If two users each have a Console installed on the same Linux machine and they both try to upgrade, the first upgrade will succeed but the second will fail with the error /tmp/exportfile.pkcs12 (Permission denied). Workaround: Delete the file /tmp/exportfile.pkcs12 and re-run consolesetup for the second user to transfer settings again.
NGS-23444	When ArcSight Console is in dark theme and you run the arcsight replayfilegen command, you will have difficulty following instructions on the Wizard. Workaround: Run the command when the ArcSight Console is in the default theme.

Issue	Description
NGS-23214	In FIPS mode, if you have used changepassword to encrypt either ssl.keystore.password or ssl.truststore.password, and then you run consolesetup, check config/client.properties to make sure that you do not have entries for both. ssl.keystore.password ssl.keystore.password.encrypted and likewise for ssl.truststore.password. If you do, please remove the entry that is not encrypted. If you do not do this, then the ESM console may not run properly.
NGS-23207	The ArcSight Console will not work in FIPS mode with SSL and ca-signed if installed on Windows 7 Professional.
NGS-23198	The ArcSight Console does not check Certificate Revocation Lists to determine if a CA-signed manager certificate has been revoked by the Certificate Authority.
NGS-22659	When you open two dashboards (All Monitored Devices and Critical Monitored Devices) while the Console is set to dark theme in /All Dashboards/ArcSight Administration/Devices/ and exit or close, you are prompted to save them even when no changes are made. Workaround: Select Yes and save the dashboards. The next time you open and close these dashboards, you do not get the save prompt.
NGS-21831	The InSubnet condition strictly enforces the use of the wildcard asterisk "*". For example, a filter like 10.10. is invalid, and 10.10.*.* is valid. Old content that uses inSubnet without a supported format (2-address, or CIDR, or wildcard) will need to use a supported format.
NGS-19880	On Linux, mouse interaction with ArcSight Console after maximizing may not respond as expected. Workaround: Instead of maximizing, drag corners of ArcSight Console to resize to fill desktop.
NGS-17864	On some systems, the Show Event Details option on an eventID in a Query viewer does not show event details like EventID, Start time, ManagerReceipt Time. Workaround: Open the event in an Active channel first and then view the event using Query viewer using Show Event Details. In some cases, restarting of the ArcSight Console also solves the issue.
NGS-17863	In an MSSP environment, under certain circumstances a tenant may notice event(s) which should match the user group's Access Control List settings for Events, but these events will be stuck in Loading Event... state in the Active Channel. Workaround: Add the Customer Name column to the Active Channel and the events will load successfully.

Issue	Description
NGS-15686	When using Logger Integration Commands, authentication on Logger 5.3 SP1 will fail when using password authentication. Workaround: Configure Logger and Integration Commands for one-time passwords.
NGS-15119	An entry's Creation Time value is not being displayed properly in the ArcSight Console.
NGS-14002	If a report is run with a parameter on an annotation, the report result will be empty.
NGS-13829	Stages resources that should be locked as system content and are editable from the ArcSight Console, on the resource Navigator > Stages resource tree. Do not edit or move these stages resources, as doing so might cause the Manager to become unusable. The system content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.
NGS-11153	The ArcSight Console starts successfully, but with the error message: Cannot find sree properties in /home/arcsight/Console/current/reports/sree.properties. Workaround: Ignore this message.
NGS-8630	Not all drill-downs will be valid. A drill-down definition can be based on all available attributes, but when viewing a query viewer in a chart, not all attributes will be displayed. So a drill-down definition based on an attribute that is NOT part of a chart view will be invalid. In that case, the query viewer must be viewed in a table.
NGS-7173	The Console may become temporarily unresponsive for a few seconds when working with large active and session lists.
NGS-5981	When annotating groups of events, the count of events which the Console indicates were updated may not reflect the correct number of updated event records.
NGS-1088	If a regular or inline filter with the condition "Event Annotation Flags Is NOT NULL" is applied to an active channel, the active channel will not load all of the matching events. The Event Annotation Flags is a bit-mapped field and should never be NULL. The correct filter condition is: EventAnnotationFlags != 0

ArcSight Manager

Issue	Description
ESM-51070	Connector statistics file to be processed correctly on Managers other than the primary destination Manager. Related content such as the rule Connector Discovered or Updated will be impacted.
ESM-48068	After asset auto-creation, if the Manager does not restart and the server.std.log shows a message about a "conflicting device with the same hostname/ipaddress <resource id>", then two assets have the same resourceId. This conflict has to be resolved before starting the Manager.
ESM-47625	When exporting a case or other resource, the Creation Time is changed to the time of the export.
ESM-46699	Updating a Trend by refreshing it works only once. Subsequently, the trend does not refresh with updated information.
ESM-30008	Installing an exported package from a bundle occasionally results in the following error: Install Failed: Resource in broker is newer than modified resource. Workaround: Re-import the package.
NGS-27111	Similar to the previous versions, ESM 7.0 expects ET in a local time zone when receiving event data from Connectors and Event Broker. However, CEB pods use UTC time for ET when submitting events to Event Broker. When consuming such events, ESM may not show them in the sliding Active Channels based on ET as the ET time of those events is out of the Active Channels time intervals. Switching Active Channels to MRT instead of ET helps.
NGS-26944	If you run the sendlogs command from command line or from the ArcSight Console when you log in as an admin user, you can find the Local logs option at the second panel after choosing the option Change/Review setting (before gathering logs). You only have this choice if you log in as an admin user. Note: as a non-admin user, you can only choose the sanitizer mode, which has three choices: NO-sanitizer, IP-only sanitizer, full sanitizer including IP, hostname, and email address.
NGS-26917	When a system is first setup or installed, the audit events are generated as soon as Manager is started. In distributed mode, due to the time it takes for all the components to come up, the audit events not displayed by the dashboard displaying the status. When Manager is restarted, or a failover is done, audit events are processed by the distributed cluster and the correct status is displayed in the dashboard.
NGS-26846	In ESM distributed mode, when lags on topics start growing, look at Partial Match data monitor to find high Partial Match rules and tune them or disable them.
NGS-26452	If a rule is disabled by the system in a correlator or an aggregator, and then if you stop the correlator or aggregator immediately, the rule will not be reactivated by the system even by restarting the correlator or aggregator. Workaround: Do not stop the correlator or aggregator immediately after the rule is disabled by the system.
NGS-26237	In ESM distributed mode, System Monitor and System Monitor Attribute data monitors display information from the persistor node. They do not have access to information from nodes running correlators or aggregators.

Issue	Description
NGS-26217	When running the arcsight correlationsetup wizard, if the user terminates the wizard without completing the configuration of a correlator or aggregator instance, the service id generated for that instance will not be used for future instances. Service ids are unique to each instance. In this case, there is no negative side effect on the functionality of the system.
NGS-25604	Some reports may run more slowly in ESM distributed mode as compared to compact mode.
NGS-25518	Connections from ESM services to Event Broker and to Message Bus can fail intermittently from various causes, including networking issues, operating system resource contention, Kafka and ZooKeeper processing loads, or ESM service instance processing. Some failures resolve automatically as resources become available or processes work through data spikes. Other failures can result in persistent problems that require manual intervention. Failures may be more frequent with heavily-loaded systems, intra-cluster networks with high traffic, or high event rates. A common recommendation for Kafka operations is to run Kafka on a system with low disk i/o traffic. Following this recommendation may improve stability and performance of ESM message bus data and message bus control instances in a cluster. Some indications of these failures are:</p> 1. Manager, correlator, or aggregator log a WARN message if they try to read messages from message bus and the read does not complete as expected. Examples of these messages: consumer handled a wakeup() after <time stuck> ms - poll(<poll timeout>) may have been stuck These messages include an ID for the reader with a number at the end. If the message is being logged and the number is over 100, a problem may exist. If the message is frequent and the number is over 1000, a problem exists and manual recovery is needed. This problem can be resolved by restarting the affected service instance. Keep in mind any requirements to stop and start related instances in a controlled sequence. 2. Message Bus data instances (Kafka processes) log errors and warnings when replication falls too far behind. This is more likely on busy servers and busy networks. The problem normally resolves as replication catches up. If it does not resolve, it may be necessary to add servers, or manage network resources, or reduce EPS. 3. A node that is running a message bus control instance requires the instance be stopped before the operating system is shut down or rebooted. If the operating system is stopped without stopping message bus control, topic data may be corrupted. In some cases, Kafka can recover from this corruption. If Kafka cannot recover, shut down ESM, delete ESM's topics in message bus, and start ESM again. This procedure deletes in-flight event data and re-creates the topics. A future version of Kafka may resolve this problem. Locations for logs: Log output for message bus data instances: /opt/arcsight/var/logs/mbus_data*/kafka.log* Log output for message bus control instances: /opt/arcsight/var/logs/mbus_control*/zookeeper.log*

Issue	Description
NGS-23503	If the Manager certificate is changed for any reason, such as an IP address change, hostname change, expired certificate, or IPv6 reconfiguration, the newly-generated Manager certificate must be imported on all clients as stated in the section Changing the Hostname of Your Machine in the ESM Administrator's Guide. But there are problems that may occur while attempting to replace a source Manager certificate on a Forwarding Connector. A deleted source Manager certificate may reappear in the Forwarding Connector truststore unless it is deleted from two separate truststores. Workaround: Use the following procedure when the certificate of a source ESM Manager of a Forwarding Connector has changed: 1. Export the new Manager certificate from the source Manager. 2. Delete the old Manager certificate in the Forwarding Connector from both FIPS and non-FIPS truststores using the following sample commands. (Command samples are derived from the SmartConnector 7.5 User's Guide. The certificate alias and keystore password will vary based on your installation.) jre/bin/keytool -keystore jre/lib/security/cacerts -delete -storepass changeit -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388" jre/bin/keytool -keystore user/agent/fips/bcfips_ks -storetype BCFKS -storepass change -delete -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -J-Djava.security.egd=<a href="file:/dev/urandom" class="external-link" rel="nofollow">file:/dev/urandom</a> -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388" 3. Import the source Manager certificate into Forwarding Connector truststore (SmartConnector User Guide) 4. Run agentsetup on Forwarding Connector to re-register the destination Managers to the connector. The full alias of the Manager certificate may be found by running the keytool command with the -list option using the following sample: jre/bin/keytool -keystore jre/lib/security/cacerts -list -storepass changeit
NGS-23341	If you see Event Broker the connection audit event status go up and down continuously, it is likely that there is some issue with either the topic that ESM is consuming or with the Event Broker connected to ESM. Ensure that the Event Broker is running properly.
NGS-14860	Multiple failure messages are generated in logger_web.out.log when stopping arcsight services. These messages can be ignored.
NGS-14437	In some cases when permission is not properly set or an account was improperly moved from a lower level to a higher level of access control list, then the error message Not allowed to read 01000100010001001 (All Users) Error Messages is written to logs.

Issue	Description
NGS-14260	If some resource on the primary (for example, memory, or CPU) is temporarily exhausted, it may be necessary to reboot the primary to recover HA control completely. Symptoms during the resource exhaustion can include: 1. ESM running very slowly. 2. Cannot make a new SSH connection to the system. ESM will run normally after the resource exhaustion ends. But the following continuing symptoms may be seen: 1. HA will not failover via arcsight_cluster prefer or arcsight_cluster offline. 2. HA may report that the resources "ESM", "Filesystem", and "Service IP" are Stopped, when they evidently are running normally. If these symptoms are seen together, the primary system should be rebooted.
NGS-12105	The annotation stage name default value (Queued) is displayed in the active channel, but this value name does not display in the query viewer or in a report. Other non-default values (for example, Initial or Follow-Up) are displayed correctly in the query viewer or report.
NGS-9734	In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.
NGS-9109	An incorrect OID is provided for ArcSight SNMP Trap. A third party package causes the OID for the trap to be translated incorrectly.
NGS-8926	If there is a Forwarding Connector running between a source Manager and any destination, and a correlation event occurs on the source Manager, then the Forwarding Connector will forward the correlation event and its associated correlated events to the destination. However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database. As a result, if there is any correlation content on the source Manager looking for the value EventAnnotationFlags=correlated, the content will not be matched or triggered.
NGS-3825	If the field size of an event exceeds 32 KB, that event does not persist.
NGS-1937	The archive tool occasionally fails to import entries into an active list due to transient errors. In such situations, you might not see errors, but the list is not populated. Workaround: Re-import the same package.
NGS-172	Base events are not automatically annotated after rules trigger. Workaround: Set logger.base-event-annotation.enabled=true in server.properties.

CORR-Engine

Issue	Description
NGS-27158	In rare cases, a rule can have the wrong base event (on the first event trigger) when a second rule which matches any events and has aggregation 100/second in a high EPS system.
NGS-14477	Space-based retention cleans up same day data, but even after increasing the space, the system does not recognize that the space has been increased until midnight.
NGS-14041	Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the Ignore Case option, which rely on the UPPER function.
NGS-11080	When offline event archives are restored to another system using the restorearchives command, the event annotations are not restored. The offline archives are not affected.
NGS-4837	With certain long running queries, a deadlock might occur in the JDBC driver. You might notice decreased throughput. If you suspect this deadlock, request a thread dump through manage.jsp and determine if the end of the dump specifically indicates deadlock. Workaround: If a deadlock does occur and is an issue for you, restart the Manager to resume normal operations.
NGS-4790	To resolve a "database full" condition, free up space in the ArcSight System Storage Space. Workaround: 1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend. 2. Reduce the retention period of specific trends. By default, trends retain 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time the trend runs. 3. Examine the contents of your session lists. Data is not usually removed from session lists. Running bin/arcsight dropSLPartitions -h will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.

Command Center

Issue	Description
NGS-27190	The range for finished cases is defined by socmetrics.finished.cases.lower.end and socmetrics.finished.cases.higher.end in server.properties. When the value for finished cases is in the defined range, this value displays in gray, indicating it is in range. When the value is less than the defined range, it is displayed in red; when the value is greater than the range, it is displayed in blue.
NGS-27160	Drilldown does not work for Last State Data Monitor in the ArcSight Command Center in Tile view. On double click of entry an unexpected error occurs. Workaround: Switch to Table view to create drilldown in entries.
NGS-27116	The Cluster View dashboard may not reflect properly the service status if correlator or aggregator lags are large. This caused by Cluster View dashboard audit events using the same path as other events, and, if there is a large lag, audit event delivery is possibly also delayed.
NGS-27089	When Health of Distributed Correlation is bad, where-in Aggregator Lag is bad or no connection to Mbus or Dcache, Aggregator Lag in the Cluster View Dashboard fluctuates between very high number and 0. When it gets response it shows actual value.
NGS-26382	When a case is expanded in Security Operations Center metrics grid view, full history may not be displayed. Workaround: In this situations, view the history in the Cases editor by clicking the case.
NGS-26357	While viewing dashboards in the ArcSight Command Center, charts might appear small. Workaround: Refresh the page for proper rendering.
NGS-23549	The Tools dialog appears truncated at the top of the window when you are selecting the first 5 row options of the grid. This occurs when the IP Address value is in IPv6 format.
NGS-23437	If you set a background image to a dashboard in the ArcSight Console, this image is not set to the same dashboard when it is viewed in the ArcSight Command Center.

NGS-23429	Reports run in HTML format from ArcSight Command Center containing charts do not show up in the report output when the server is configured with the following properties, which save report output in database:
	vfs.report.provider.scheme=db
	vfs.report.provider.class=com.arcsight.common.vfs.database.ArcDatabaseFileProvider
	vfs.report.provider.base=db://reports/archive
	Workaround:
	Run the report in PDF format.

Issue	Description
NGS-23105	If the Manager has a CA signed certificate, and the certificate is signed with the SHA1 algorithm, the ArcSight Command Center may not work on the Microsoft Internet Explorer or Google Chrome browsers. CA signed certificates signed with SHA256 or SHA384 are recommended.
NGS-22583	The Condition Summary is not formatted in color codes and also does not display the field Display Name when a drilldown is created based on active channel.
NGS-22573	The ArcSight Command Center User's Guide states that FIPS Suite B Mode is not supported for peering or content management. The Administration->Content Management and Administration->Peers menu items are disabled if the server is running in FIPS Suite B mode. However, the aforementioned menus are enabled if the Manager from which you initiate peering is not in FIPS Suite B mode, even if the target of the peer relationship is in FIPS Suite B mode. This is an unsupported configuration. But the ArcSight Command Center does not have visibility into the FIPS mode of the target Manager so it cannot disable the menu item. Note that peering and content management are not supported if either manager in the peer relationship is in FIPS Suite B mode.
NGS-22085	In the ArcSight Command Center, for Query viewers, Stacked Bar chart will not be supported if Y axis or Z-axis are not aggregated fields. In such cases user has to view in Table format.
NGS-21986	Viewing the Last N events data monitor in the ArcSight Command Center which contains numerous variable fields (based on an overlapping Session List) may cause a Java Script unresponsive error. Workaround: Limit the data monitor to six variable fields with 10 rows, or split the fields by creating one or more data monitors.
NGS-21930	If an event storage group is full and, at the same time, the Daylight Saving Time to standard-time transition occurs, the space retention process may get stuck. As a result, the Manager will start reporting a no space available error and event flow will stop. Workaround: On the ArcSight Command Center: 1. Select Storage Management. 2. Select the Storage group's retention period. 3. Change the retention period so that the archive job status of the date of Daylight Saving Time to standard time transition will be changed to offline and re-change the retention period back to original value.
NGS-20458	The search parameter | regex "#" will cause the search query to fail and will throw a 503 service request error. Once the page gets a 503 error, it does not leave this state. Workaround: Refresh the page (press F5).
NGS-20280	The WHERE operator is not supported in user-defined fields.
NGS-19267	You cannot restrict access to cases by user in the ArcSight Command Center.

Issue	Description
NGS-17407	If the system has too many notifications, the ArcSight Command Center will not show notification counts in the notification view. Workaround: Stop the Manager, delete unused notifications such as undeliverable or old pending notifications, and start the Manager.
NGS-14900	There is a rare case that may cause confusion in channel event data visualization screen, if the event interval is less than 1 minute apart. The depending charting library, d3.js, is not able to handle this minute rounding case.
NGS-13926	The stages available in the ArcSight Console Stage drop-down list do not always display in the ArcSight Command Center active channel. The stage Follow-Up is available in the ArcSight Console Annotation Stage drop-down list, but does not display in the Annotation Stage drop-down list in ArcSight Command Center - Active Cannels.
NGS-8530	In the ArcSight Command Center event search feature, some expected fields are missing from exported search results. For example, if you search for events, click Export Results, and check All Fields in the Export Options page, then click Export and download the exported results, then only some basic fields are listed, such as endTime, Name, sourceAddress. Workaround: In the ArcSight Command Center search page, after a search is completed click Export. Instead of selecting the checkbox to include All Fields, enter a comma-separated list of fields in the text area provided.
NGS-7912	In peer search, the search result is not refreshed responsively if one peer node has high hits, or the system is busy due to high ingestion rate or multiple searches running.
NGS-7891	In an ArcSight Command Center Search, queries using some operators, such as eval, rename, replace, rex, and regex, may not return the correct results when searching the following types of fields: - IPv4 fields such as sourceAddress - MAC address fields such as destinationMacAddress - IPv6 fields such as dvc_custom_ipv6_address1 - Geo Location fields such as dest_geo_latitude - agentSeverity and locality fields; For example the following queries may not return the correct results: ... | replace Low with notToWorry in agentSeverity ... | replace Local with localevents in locality

Issue	Description
NGS-7594	In the ArcSight Command Center, after search results are exported and the session times out, you will see a logout message in the export window. Workaround: When this occurs:; 1. Close the export window.; 2. Log in to ArcSight Command Center again. 3. Continue with the search.
NGS-7584	Fixed issue where a condition in a case query group with owner = <username> will return an error while viewing cases of a case query group in any user interface. Now search group will display cases for set username.
NGS-6886	When a system has several peers and a peer stops responding, some pages in the ArcSight Command Center user interface might become slow to display. The delay happens regardless of the reason the peer system stopped responding. Workaround: Identify the peer that is not responding and remove its peer relationship on the Administration > Peers page, Peer Configuration tab. You can re-add the peer later, when it is back in service.
NGS-6812	The ESM server log and the Logger server log may contain messages that say "...NotSerializableException: ...PeerLoggerRequestDestination". These messages do not indicate an active problem, and can be ignored.

Connector Management

Issue	Description
NGS-22669	When events are sent to ESM by an Event Broker, payload information cannot be retrieved for the corresponding event.

Connectors

Issue	Description
NGS-23179	The command ./arcsight agent tempca -i in connector version 7.5.0.7983.0 in FIPS SuiteB mode will throw an exception. Update the connector to a version later than version 7.5 where this might be addressed.
NGS-13049	When upgrading the Forwarding Connector, two fatal exception messages will appear, regarding [agents [0].arcsightuser] and [agents[0].arcsightpassword]. Workaround: Ignore these messages.

Issue	Description
NGS-12407	Annotation flag indicating forwarded' may not get set when forwarding events from ESM.
NGS-1423	Upgrading a connector running on Windows from the ArcSight Console will fail if any process is using the connector's current folder. Workaround: 1. Make sure there are no files in the connector's "current" folder open. 2. Start the connector by using Start > Programs > Connector Programs. Do not start the connectors using the "arcsight agents" command.

Installation and Upgrade

Issue	Description
NGS-26959	After doing an upgrade to ESM HA 7.0, you may see messages like the following: myhost.mydomain.com: 2018-02-27 13:51:16 ERROR - Cluster did not come up after upgrade See the status output above this message myhost.mydomain.com: 2018-02-27 13:51:16 This may be a transient problem - check status again in a few minutes. when HA is actually up and running. Check for the line: Disk: SyncSource UpToDate/Inconsistent which indicates that the secondary is synchronizing with the primary. You can continue the upgrade procedure while this goes on.
NGS-26913	Occasionally, in distributed mode, the output from /etc/init.d/arcsight_services version may not be correct for a node if this information has recently changed (for example if a node has been converted from compact mode, or converted to HA). This can be corrected by running the following command on the node that has the incorrect information: /etc/init.d/arcsight_services setLocalBuildVersions This will correctly display the version information on all nodes.
NGS-26898	In ESM distributed mode, if network instability occurs, topics may not be listed in message bus and correlators and aggregators do not appear to be consuming any events. A restart of the cluster using stop all/start all will get the cluster back to normal.
NGS-26661	The log message Could not convert table(s) arc_trend_xxxxxx without column details in arc_db_table_schema in the upgrade log means the table schema for arc_trend_xxxxxx could not be found from schema table. ESM could not perform upgrade on table arc_trend_xxxxxx.

Issue	Description
NGS-21995	On upgrade, due to resource validators for IP Address data, any resource containing incorrect IP Addresses or IP Ranges will be invalidated and the conditions may be cleared. Workaround: Rebuild the invalidated resource after the upgrade.
NGS-21133	;During ESM upgrade, if the fully qualified domain name (FQDN) does not resolve to the IP Address of the ESM host, the upgrade process might freeze and finally fail. Workaround: If this is the case, check the upgrade log file /opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log if it contains this message: "Starting Apache...httpd: Could not open configuration file /opt/arcsight/logger/current/local/apache/conf/httpd.conf: No such file or directory Failed to start. Stopping APS...APS was not running." To prevent this failure, make sure the fully qualified domain name is configured properly on the ESM host before starting the upgrade.
NGS-19862	Before installing ESM, verify that the system has a configured hostname that resolves to a local IP address.
NGS-14188	ArcSight Console installation on non-English path in Windows machines fails to configure the ArcSight Console. Workaround: Use English filenames in installation paths. Or run ArcSight Console configuration after installation finished by running the consolesetup script from the ArcSight Console ..\current\bin directory.
NGS-7497	Console installation on localized path works in some Windows 7 machines, but not in others. Workaround: Due to the inconsistent behavior in Windows 7 machines, use English filenames only in installation paths. Local language names in paths may cause installation to fail in certain Windows 7 environments.
NGS-3839	Occasionally, the First Boot Wizard may fail to proceed due to some errors. Workaround: If this happens, terminate the process. After checking the logs and correcting the errors, follow the clean up instruction in the ESM Installation Guide and re-launch the installer.
NGS-2783	When a Forwarding Connector is installed, Superconnectors group is created under Custom Users Groups group. In addition, No Events enforcing filter is replaced by a specific event filter. After the upgrade, No Events enforcing filter will be reinstated meaning that no events will be forwarded from the Manager to the destination. Workaround: Remove the No Events enforcing filter.

Localization

Issue	Description
NGS-26414	In localized environments, some of counts in the Security Operation Center view are not updated properly.
NGS-23004	On a system with the Simplified Chinese locale, after the import of a case package created in English locale, the properties of the case may have default values instead of the entered values. This issue exists in both the ArcSight Command Center and the ArcSight Console.
NGS-22991	In Simplified Chinese and Traditional Chinese, if you create a data monitor with the type HourlyCount and view it in tile format, its display will hang with no data displayed.
NGS-22600	On a Traditional Chinese Installation, when you display the Top Value Count dashboard, the Stacking Area, Area,Scatter Plot, and Line options show no data. Data displays in the Bar, Pie, and Stacking Bar options.
NGS-22568	In Traditional Chinese the function LengthOf may display incorrect values and/or produce the wrong filter results.
NGS-21872	If you retrieve logs via the Command Center on an ESM localized to other than English, the ArcSight Command Center will not inform you when the logs have been retrieved. Workaround: Go to the log retrieval page; you will find your newly generated logs.

Pattern Discovery

Issue	Description
NGS-26694	In ESM distributed mode, Pattern Discovery is processing fewer events as compared to compact mode ESM.

Reports

Issue	Description
NGS-20509	Peer reports fail when Logger is peered with ESM 6.8c and onwards. This happens because the database type of the event field arc_sourceAddress is different for Logger and ESM.

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 system, click the link above and an email window opens with the following information in the subject line:

Feedback on ESM 7.0 Release Notes (ESM 7.0)

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 arc-doc@hpe.com.

We appreciate your feedback!