



ArcSight ESM

Software Version: 7.8

ESM 7.8 Release Notes

Document Release Date: August 2024

Software Release Date: August 2024

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2001-2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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://www.microfocus.com/documentation/arcsight/

Contents

- Welcome to ESM 7.8 6
 - What's New in This Release 6
 - Rules Authoring 6
 - Certificate Management 7
 - Updated Components 7
 - Standard Content 8
 - Verifying the Downloaded Installation Files 8
 - Upgrade Support 9
 - Upgrade Paths for ESM 9
 - Upgrade Paths for ESM with the Active Passive High Availability (APHA) Module 10
 - Geographical Information Update 11
 - Vulnerability Updates 11
 - Supported Versions for Distributed Searches 11
 - Supported Platforms 12
 - Supported Languages 12
 - Support for ActivClient Issues 12
 - Usage Notes 13
 - Improving Security in Default or FIPS 140-2 Mode 13
 - Active Lists and Rule Authoring 14
 - Required Workarounds for G10 Appliance 15
 - Uninstall the Chrony RPM 15
 - Remove Health-related RPMs 16
 - Configuring Connectors to Write to Transformation Hub 16
 - ArcSight Command Center 16
 - Scroll Bar Issues with Google Chrome and Apple Safari 16
 - Viewing Secure Operations Center Dashboard Using Edge Browser on Windows 10 16
 - ArcSight Console 17
 - Events from Transformation Hub 17
 - Using Windows 10 17
 - Oversized Pie Charts on Dashboards 17
 - Limit on Dashboards Being Viewed 17
 - Distributed Correlation Mode 18
 - Configuration Changes and Service Restarts Require Restart of All Services 18
 - Active List Updates in Distributed Correlation 18

Stopping Message Bus Services	19
Hierarchy Map Data Monitor in Distributed Correlation - Not Recommended	19
Converting IPv4 to IPv6 in Distributed Correlation Mode - Consult Professional Services	19
Distributed Cache Inconsistency	19
Large Lists Can Take Time to Load on Cluster Startup	20
Oversized Event Graphs	20
Full Text Search	20
ESM Peer Certification for Content Synchronization	21
Actor Model Import Connector	21
Asset Model Import FlexConnector	21
Forwarding Connector	22
Rule Recovery Timeout Possible During High EPS	22
Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations	23
Reference to SmartConnectors Not Updated (Customer URI)	23
Silent Install Does Not Trigger the Console Setup	23
Unsupported Features in This Release	25
Resolved Issues	27
General	27
ArcSight Console	29
ArcSight Manager	30
Command Center	30
ArcSight Fusion	30
Connectors	31
Installation and Upgrade	31
Open Issues	32
Installation and Upgrade	32
General	34
Analytics	35
ArcSight Console	35
ArcSight Manager	37
CORR-Engine	40
Command Center	41

ArcSight Fusion	43
Connector Management	44
Connectors	45
Active Passive High Availability Module	45
Localization	45
Publication Status	46
Send Documentation Feedback	47

Welcome to ESM 7.8

ArcSight Enterprise Security Manager (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.

Got an Idea? Want to request a new feature? Click [here](#) to visit the Ideas Exchange - the Open Text online portal for submitting feature requests.

What's New in This Release



Note: ArcSight Command Center in any ArcSight Platform version up to and including 24.2.1 is not supported when integrated with ESM 7.8. Other integration functionality between ESM 7.8 and any ArcSight Platform version up to and including 24.2.1 is supported. For information about disabling ArcSight Command Center in the ArcSight Platform, see the [Administrator's Guide for the ArcSight Platform](#) that corresponds to your deployment type: Off-Cloud, Azure, AWS, or GCP.

After you disable ArcSight Command Center, the related menus will be visible but will not work. To remove the menus, clear the cache and then log in again.

This topic describes the new features and enhancements in ESM 7.8.

Rules Authoring

Rules authoring is now available in the ArcSight Command Center.

When creating rules, you can:

- Use our new feature to create rules from recent events.
Use the latest event data to streamline rule creation. Select relevant fields to add them to the Condition Editor.
- For advanced users, use our full text query feature to swiftly build rules.
- Use the summary view in the Condition Editor to review configured rules and verify rule conditions.

To view a summary of the entire condition, collapse the root node. To view a summary of a condition branch, collapse the branch node.

The following functionality is not supported at this time:

- Advanced conditions such as matches Filter, InActivelist, In Asset

Basic rule conditions with simple queries is supported. For example:

```
( Name endswith Failed or ( bytesIn >= 100 and bytesOut >= 1 and priority > 5 ) )
```

```
Agent Address = '10.0.0.1' and Application Protocol = UDP
```

- Resources, resource references, and date time fields
- Field names as reference field values in conditions
- In, Between, and InGroup operators

For more information, see the [Command Center User Guide](#).

Certificate Management

ESM utilizes certificates to provide a secure connection between multiple components. These certificates may be self-signed (the default during installation) or signed by a certificate authority (CA). Prior to Certificate Management, the components of ESM would trust other components of ESM by having a copy of the certificate of the component they wish to trust. These certificates were communicated between components via the ESM repository or manually in the case of components like collectors. This means that when a component was configured with a new certificate, all components which desire trust with that component must be updated with a copy of that new certificate.

With Certificate Management, ESM still utilizes certificates to provide component trust, but slightly changes the generation of the certificates. With SSL certificates, a client can trust Certificate A because it trusts the certificate which signed Certificate A. This is how Certificate Management works. With Certificate Management enabled, all component certificates are signed by a root certificate. That root certificate is placed in the truststore of any component which requires a secure connection. Once the root certificate is in place in the truststore, any certificate signed by that root certificate will be trusted. This also means that any component will trust a new component certificate when that component's certificate is renewed. So, Certificate Management saves time because you do not have to update each certificate manually.

Updated guides for ESM 7.8 are available on the [ESM documentation page](#).

Updated Components

ESM 7.8 includes updates to the following components:

- HTTPD version to 2.4.62
- Java version to 8u422
- Tomcat version to 9.0.89

7.8 also includes upgrades to various other components.

Standard Content

ESM 7.8 installs, or upgrades to, version 4.4 of the following packages:

- /All Packages/ArcSight Foundation/Security Threat Monitoring
- /All Packages/ArcSight Foundation/Threat Intelligence Platform

For more information, see the [ArcSight Administration and ArcSight System Standard Content Guide](#) or the [Default Content 4.4 Release Notes](#).

Verifying the Downloaded Installation Files

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the [OpenText Downloads website](#) along with their associated signature files (*.sig).



Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the [OpenText Code Signing site](#). If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact OpenText Customer Support.

4. Begin the installation.

Upgrade Support

This section provides upgrade paths for:

- ESM
- ESM with the Active Passive High Availability (APHA) Module

Upgrade Paths for ESM

For ESM 7.5, 7.6, 7.6.4, 7.7 and release patches you can upgrade directly to ESM 7.8.

Upgrade paths for earlier versions are as follows:

- 7.4:
 - a. Upgrade to ESM 7.5.
 - b. Upgrade to ESM 7.8.
- 7.3:
 - a. Upgrade to ESM 7.5.
 - b. Upgrade to ESM 7.8.
- 7.2 Service Pack 1:
 - a. Upgrade to ESM 7.3.
 - b. Upgrade to ESM 7.5.
 - c. Upgrade to ESM 7.8.
- 7.0 Patch 1 and Patch 2:
 - a. Upgrade to ESM 7.2.
 - b. Upgrade to ESM 7.4.
 - c. Upgrade to ESM 7.5.
 - d. Upgrade to ESM 7.8.
- ESM 7.0:
 - a. Apply ESM 7.0 Patch 2.
 - b. Upgrade to ESM 7.2.
 - c. Upgrade to ESM 7.4.
 - d. Upgrade to ESM 7.5.
 - e. Upgrade to ESM 7.8.

- ESM 6.11, with or without patches:
 - a. Upgrade to ESM 7.0 Patch 1.
 - b. Upgrade to ESM 7.2.
 - c. Upgrade to ESM 7.4.
 - d. Upgrade to ESM 7.5.
 - e. Upgrade to ESM 7.8.

Upgrade Paths for ESM with the Active Passive High Availability (APHA) Module

For ESM 7.5, 7.6, 7.6.4, 7.7 and release patches you can upgrade directly to ESM 7.8.

Upgrade paths for earlier versions are as follows:

- Version 7.4 of ESM and the APHA module:
 - a. Upgrade ESM and the APHA module to version 7.5.
 - b. Upgrade ESM and the APHA module to version 7.8.
- Version 7.3 of ESM and the APHA module:
 - a. Upgrade ESM and the APHA module to version 7.5.
 - b. Upgrade ESM and the APHA module to version 7.8.
- Version 7.2 Service Pack 1 of ESM and the APHA module:
 - a. Upgrade ESM and the APHA module to version 7.3.
 - b. Upgrade ESM and the APHA module to version 7.5.
 - c. Upgrade ESM and the APHA module to version 7.8.
- Version 7.0 of ESM and the APHA module:
 - a. Upgrade ESM and the APHA module to version 7.0 Patch 2.
 - b. Upgrade ESM and the APHA module to version 7.2.
 - c. Upgrade ESM and the APHA module to version 7.4.
 - d. Upgrade ESM and the APHA module to version 7.5.
 - e. Upgrade ESM and the APHA module to version 7.8.
- Version 7.0 of the APHA module:
 - a. Upgrade the APHA module to version 7.2.
 - b. Upgrade the APHA module to version 7.4.
 - c. Upgrade ESM and the APHA module to version 7.5.
 - d. Upgrade ESM and the APHA module to version 7.8.



Note: Ensure you perform the upgrade from a local workstation or server, not over a VPN. If you perform the upgrade over a VPN, and the VPN is disconnected during the upgrade, the upgrade will fail. If you must use a VPN during the upgrade process, consider using a desktop sharing utility like the screen command on Linux to prevent terminating the upgrade session if the network disconnects.

For information about supported platforms, see the Technical Requirements on the [ESM documentation page](#).

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20240515.

Vulnerability Updates

This release includes recent vulnerability mappings from the May 2024 Update:

- Snort / Sourcefire 31470 updated CVE
- Juniper IDP update 3703 updated CVE
- McAfee Network Security Manager 11.10.14.4 updated CVE
- TippingPoint UnityOne DV9899 updated CVE
- Palo Alto Networks PAN-OS 10.0.8 updated CVE
- Fortinet Fortigate 5.2 Content 3.086 updated CVE

This release includes currency updates and addresses potential security vulnerabilities in third-party components such as Java and Apache HTTPD.

Supported Versions for Distributed Searches

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

The only versions that support IPv6 connectivity and data search are ESM 6.11.0 and above.

For more information about distributed searches, see the [ArcSight Command Center Users Guide](#).

Supported Platforms

For information about ESM 7.8 platform and browser support, see the Technical Requirements on the [ESM documentation page](#).

Supported Languages

These languages are supported by ESM:

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

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 OpenText.

ActivClient releases are typically more frequent than ESM releases. In case of ActivClient issues, contact the ActivClient vendor for resolution. If you would like OpenText ArcSight support to assist with monitoring the resolution, or have OpenText 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 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.

Usage Notes

This section contains the following topics:

Improving Security in Default or FIPS 140-2 Mode

For improved security, you can enable support for a stronger cipher (256-bit AES) on your ESM installation when you install the system in either default mode or FIPS 140-2 mode. If the communicating component supports it, the stronger cipher will be used for communications with ESM.

To enable support for a stronger cipher:

1. In compact mode or on all ESM nodes in distributed mode, open the `/opt/arcsight/manager/config/esm.properties` file and add the following line (or replace the existing entry, if already present):

```
servletcontainer.jetty311.socket.https.ciphersuites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```
2. In compact mode or on the ESM persistor node in distributed mode, open the `/opt/arcsight/logger/current/local/apache/conf/httpd.conf` file and add the following line (or replace the existing entry, if already present):

```
SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
```
3. In compact mode or on the ESM persistor node in distributed mode, open the `/opt/arcsight/logger/current/arcsight/logger/user/logger/logger.properties` file and add the following line (or replace the existing entry, if already present):

```
fips.ssl.enabledcsuites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```
4. If the `/opt/arcsight/manager/config/client.properties` file exists on any of the nodes, add the following line (or replace the existing entry, if already present):

```
ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```
5. On any system where you use an instance of the ESM Console to communicate with the ESM server where the cipher update is made, open the `CONSOLE_HOME/current/config/client.properties` file, and add the following line (or replace the existing entry, if already present):

```
ssl.cipher.suites=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
```
6. For connectors that communicate with the ESM Server, similar updates might be needed in the `agent.properties` file.
7. Restart services for the changes to take effect.

Active Lists and Rule Authoring

The ArcSight Platform includes a subset of the functionality that is available for active lists and rules in the ArcSight Command Center.

- **Active Lists** - Active lists allow you to track traffic with IP addresses of interest. While you can manually update active lists, their real value comes when you define them in conjunction with rules specifically tailored to interact with and populate the lists dynamically. Lists that are not rule-driven are empty or contain only manual entries that have not timed out.
- **Rules** - Creating rules involves defining the events the rule evaluates and thresholds for triggering the rule. Conditions define which events trigger the rule and thresholds

determine when a condition is met and a correlation event is generated. You can also create real-time rules and apply event-based conditions to rules.

For more information, see the [ESM Administrator's Guide](#).

Required Workarounds for G10 Appliance

The G10 appliance has the following known issues:

- The chrony RPM might override the ntp service on server restart.
- Health-related RPMs prevent High Availability mode from working and /opt from mounting.

The following workarounds remove the RPMs and ensure the appliance works correctly.

Uninstall the Chrony RPM

You can remove the chrony RPM before or after you perform the upgrade.

Before Upgrade

Prior to setting up the G10 ESM appliance, complete the following steps:

1. Log in to the appliance using default root credentials.
2. Immediately type `control-C` to interrupt the System First Boot Wizard (FBW) script.
3. In the shell prompt, type the following command:
`rpm -ev chrony`
4. Verify the `systemctl status chronyd` command displays "Unit chronyd.service could not be found."
5. Log out.
6. Log in again and resume normal FBW steps.

After Upgrade

If you have already set up your appliance, complete the following steps:

1. Run `systemctl stop chronyd`.
2. Run `systemctl disable chronyd`.
3. Run `rpm -ev chrony`.
4. Run `systemctl status chronyd`.
5. Stop all arcsight services with the following command:
`/etc/init.d/arcsight_services stop all`
6. Reboot the appliance.

Remove Health-related RPMs

If you are using the G10 appliance in Active-Passive High Availability mode, before you install High Availability, complete the following steps on both the servers:

1. To remove the mf-health package, run the following:

```
yum remove mf-health
```
2. To remove the hp folder from /opt, run the following:

```
rm -fR /opt/hp
```

Configuring Connectors to Write to Transformation Hub

If you configure a version 7.15 or 8.0 or later SmartConnector to write binary events to a Transformation Hub topic for consumption by ESM 7.8, select **ESM** for the content type and **7.2.x** for the ESM version.

ArcSight Command Center

Scroll Bar Issues with Google Chrome and Apple Safari

When using ArcSight Command Center with the Chrome browser, 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 Microsoft Edge 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 Chrome or Firefox instead.

ArcSight Console

This section contains the following topics:

Events from Transformation Hub

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 Transformation Hub
```

This is expected behavior. There is no associated resource for events consumed from Transformation Hub.

Using Windows 10

The ArcSight Console for ESM 7.8 is supported on Windows 10.

- The recommended processors for Windows 10 are either Intel Xeon x5670 or Intel Core i7.
- Use Microsoft Edge as your preferred browser. This preference is set during Console installation time; or after Console installation using the User Preferences setting for Program Preferences.
- You can install the ArcSight Console on Windows 10 using either IPv4 or IPv6. FIPS is supported with IPv4 but not IPv6.

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.

Limit on Dashboards Being Viewed

The ArcSight Console might run out of Java memory if you are viewing more than 15 dashboards. For Windows 10, limit the number of dashboards to 10. If you must view dashboards over the limit, try switching to classic charts from the **Preferences** menu, under **Global Options**.

The number of dashboards you can view in the console is directly proportional to the Java heap memory configuration for the console program.

If you want to view more dashboards than the limit:

1. Increase the Java heap memory size.
2. In the console's installation directory, modify `/current/config/console.properties` with the following property:

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

For more information, see the [ESM Administrator's Guide](#).

Distributed Correlation Mode

This section contains the following topics:

Configuration Changes and Service Restarts Require Restart of All Services

After making any configuration changes in distributed mode, such as adding a node to a cluster or needing to restart one of the services, stop and 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, refer to the new Cache Model setting **Write Synchronized** in the [ArcSight Console User's Guide](#).



Note: This option is effective at eliminating the redundant firing of Lightweight Rules where changing to `OnFirstEvent` trigger is not available. See below for performance implications you need to understand before changing the setting.

Similarly, if you have a pair of rules: the first rule populates a list, and the second rule depends on data in 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. The **Write Synchronized** setting ensures that a list update performed by a Lightweight Rule is visible to subsequent standard rules.



Note: The order of rule processing is not guaranteed unless the first rule is a Lightweight Rule, so this scenario might not 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 might still not trigger due to the active list not having yet been updated.

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.

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 a 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 to 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 inconsistency . . .**".

3. Hover your mouse pointer over the service message, and you will see the identity of the service that is causing the issue. For example:

```
Hazelcast cluster inconsistency. Some DCache instances are not accessible.
Restart them if they are running (split-brain), otherwise clear their
runtime records in repo using command "dcache-repo-records". Troubled
instances: dcache2@host3
```

In this example the name of the distributed cache instance that is causing the issue is *dcache2*. The hostname in this example is *host3*, and is the name of the machine in the cluster on which that particular distributed cache instance resides.

4. Restart the cluster.
5. (Conditional) If a standalone distributed cache instance did not properly shutdown or was abruptly disconnected (for example, due to a network problem) and is not accessible from the persister, run the following command to remove information repository records from non-responsive distributed cache instances:

```
bin/arcsight dcache-repo-records -r dcache2
```

This command cleans internal runtime records for *dcache2* in the information repository. The records are automatically reset by the instance, if it becomes available again (for example, after the network connection is restored).

Large Lists Can Take Time to Load on Cluster Startup

In a distributed cluster, when large lists (>1 million) are present, it can take some time, depending on the size of the list, for the lists to load and EPS to ramp up, on startup of the cluster. This release improves the load time, but you might still experience some impact.

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. Approximately 50 percent more disk space is required for storing events for full text search.

The feature is controlled by the property `fulltext.search.enabled`. If you want to disable full text search, enter the following in `server.properties` and then restart the Manager:

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

For more information about editing properties files, see the [ESM Administrator's Guide](#).

ESM Peer Certification for Content Synchronization

Peering for ESM content synchronization is automatically mutual, so a group of peers can 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. Consider the impact to synchronization during change management.

For more information about content management, see the [ArcSight Console User's Guide](#) and the [ArcSight Command Center Users Guide](#).

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. This connector can be configured in a dual stack or pure IPv6 environment. For more information, see the [Actor Model Import Connector for Microsoft Active Directory Configuration Guide](#). The Actor Model Import Connector for Microsoft Active Directory to install for ESM 7.8 is version 8.4.6.9375.0.

See the Technical Requirements on the [ESM documentation page](#) for information about ESM 7.8 supported platforms.



Caution: Install and use the Actor Model Import Connector for Microsoft Active Directory that is provided with the ESM 7.8 release. That is the version of the connector that is tested and certified to work with ESM 7.8. Do not use previously-supplied versions of the Actor Model Import Connector for Microsoft Active Directory with ESM 7.8.

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. This connector can be configured in a dual stack or pure IPv6 environment. For more information, see the [Asset Model Import FlexConnector Developer's Guide](#). The Asset Model Import FlexConnector to install for ESM 7.8 is version 8.4.6.9376.0.

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 Technical Requirements on the [ESM documentation page](#) for information about 7.8 supported platforms.



Caution: Install and use the Asset Model Import FlexConnector that is provided with the ESM 7.8 release. That is the version of the connector that is tested and certified to work with ESM 7.8. Do not use previously-supplied versions of the Asset Model Import FlexConnector with ESM 7.8.

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 7.8.

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 Technical Requirements on the [ESM documentation page](#) for the version that is supported with ESM 7.8.

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: Timeout can still occur after increasing 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 if you increase the recovery time limit.

For information about editing the `server.properties` file, see the [ESM Administrator's Guide](#).

Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations

The creation or deletion of mark similar configurations now generates audit events. You can add filters to view the audit events:

ID	Message	Priority
marksimilar:102	Mark similar configuration is created	Low
marksimilar:100	Mark similar configuration removed due to time window expiry	Low
marksimilar:100	Mark similar - all have been removed	Medium
marksimilar:100	Mark similar configuration removed due to error. Check server.log	High

Reference to SmartConnectors Not Updated (Customer URI)

When the customer object is renamed on the ArcSight Console, the associated reference to SmartConnectors (the Customer URI) is not updated with the new name. The Customer URI on the connector retains the old name. This is expected behavior and not an issue.

Silent Install Does Not Trigger the Console Setup

When in silent mode, the ArcSight Console installation program does not trigger the `consolesetup` step at the end of the installation. As a result, a default `console.properties` file is not generated during the installation.

Workaround:

1. Run the `consolesetup` wizard in recording mode to capture a silent response file. For example:

```
arcsight consolesetup -i recorderui -f console_silent.out
```

2. Use the response file `console_silent.out` to run `consolesetup` in silent mode. For example:

```
arcsight consolesetup -i silent -f <full path to console_silent.out>
```

This results in a `config/console.properties` file in the ArcSight Console installation.

Syntax:

The `consolesetup` command supports the following parameters:

```
consolesetup [-i <mode>] [-f <file>] [-g]
```

Parameters:

-i <mode>: modes are: console, silent, recorderui, swing

-f <file>: log file name (properties file in -i silent mode)

-g: generate sample properties file for -i silent mode

For more information about commands and parameters, see the [ESM Administrator's Guide](#).

Unsupported Features in This Release

This information applies to ESM Software and ESM Express.

The following features are not available in this release:

- Conversion from default (non-FIPS) to FIPS SuiteB mode is *not* supported in compact or distributed ESM:
 - 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.
- The `arcsight_services restart` command is no longer supported.

The following are not supported in this release:

- 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 Service Manager, including use of the ArcSM connector
- Threat Central Solution, including use of Threat Central Model Import Connector
- Integration with Remedy ticketing software
- Partially cached behavior is not supported on any data list in distributed mode, regardless of the size of the list. This includes:
 - Partially Cached Active Lists
 - Time Partitioned Active Lists
 - All Session Lists.



Note: These lists still function with in-memory data but no attempt is made to retrieve entries from the database.

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 environments.

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

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

External links to Console Help are not supported in an IPv6-only environment.

ESM Integrations:

The following ESM integrations are not supported. If you are using any of the following, *do not upgrade* to ESM 7.8:

- 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;`

Resolved Issues

This section provides information about issues that are either fixed in this release or resolved with a workaround.

General

Issue	Description
OCTCR331607096	<p>If FIPS Mode is enabled at the OS Level, an error output occurs when creating a root certificate on the Persistor Node.</p> <p>Workaround: To verify if FIPS mode is enabled at the OS level, run the following command:</p> <pre>fips-mode-setup --check</pre> <p>If FIPS mode is enabled at the OS level, while running firstbootsetup (for a distributed fresh install) or prepare_repo.sh (for a distributed upgrade) on the persistor node, the errors below can be safely ignored when the root certificate is getting created.</p> <p>Errors outputting keys and certificates 140178280273728:error:0607B0C8:digital envelope routines:EVP_CipherInit_ex:disabled for FIPS:crypto/evp/evp_enc.c:227:140178280273728:error:06074078:digital envelope routines:EVP_PBE_CipherInit:keygen failure:crypto/evp/evp_pbe.c:131:140178280273728:error:23077073:PKCS12 routines:PKCS12_pbe_crypt:pkcs12 algor cipherinit error:crypto/pkcs12/p12_decr.c:41:140178280273728:error:2306A075:PKCS12 routines:PKCS12_item_decrypt_d2i:pkcs12 pbe crypt error:crypto/pkcs12/p12_decr.c:94:</p>
OCTCR331605115	<p>The Initialize New Node Properties script does not work in cloud environments with key-based authentication.</p> <p>Workaround: Follow these steps:</p> <ol style="list-style-type: none">1. Configure Passwordless SSH manually between the persistor and non-persistor nodes, as the later execution of sshSetup script may fail with a permission denied error.2. Create the file esm.properties under /opt/arcsight/manager/config on each non-persistor nodes.3. Edit esm.properties added in step 2. and add the property fips.enabled=true/false depending on the persistor node's FIPS configuration.
OCTCR331607050	<p>Multiple warning messages appear while using the package, archive, and managerinventory command line utility during ESM Installation (both Compact and Distributed) in FIPS mode import.</p> <p>Workaround: Ignore the warning messages and proceed with your actions.</p>
OCTCR331451008	<p>During stop/start of the manager service, events are lost.</p> <p>Workaround:Software update in 7.8.</p>

Issue	Description
OCTCR331857054	<p>Active channel searching IP is slower than searching host name.</p> <p>Workaround:Software update in 7.8.</p>
<p>OCTCR331865009, OCTCR331764002</p>	<p>Issue upgrading Threat Intelligent Platform package (TIP) to v4.2</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1. As systemuser, login to the ArcSight Console. 2. Backup any customizations. 3. Delete: <ul style="list-style-type: none"> • /All Packages/ArcSight Foundation/Security Monitoring - Base - Active Lists (starting with this package it might happen that Security Threat Monitoring and Security Monitoring – Base will also be automatically deleted) • /All Packages/ArcSight Foundation/Threat Intelligence Platform • /All Packages/ArcSight Foundation/Security Threat Monitoring • /All Packages/ArcSight Foundation/Security Monitoring – Base 4. As systemuser, remove the following groups from all resource types (Rules, Reports, Trends, Queries, Templates, Query Viewer, Lists, Filters, Field sets, Dashboards): <ul style="list-style-type: none"> • ArcSight Foundation/Threat Intelligence Platform • ArcSight Foundation/Security Threat Monitoring • ArcSight Foundation/MITRE ATT&CK <div data-bbox="548 1058 1414 1142" style="border: 1px solid #ccc; border-radius: 5px; padding: 5px; margin: 10px 0;">  Note: Be sure to check the Unassigned folder. </div> 5. As systemuser, search for the following and remove instances: <ul style="list-style-type: none"> • Threat Intelligence Platform • Security Threat Monitoring • MITRE ATT&CK' 6. Execute <code>/bin/arcsight resvalidate</code> and remove invalid resources. 7. Using archive utility import archive tipfix.xml. For <host> you should set esm fqdn. For example: <code>/bin/arcsight archive -action import -m <host> -u admin -p <password> -f tipfix.xml</code>. 8. Stop all services: <code>/etc/init.d/arcsight_services stop all</code> 9. Run: <code>/etc/init.d/arcsight_services start mysqld</code>. 10. Start all services: <code>/etc/init.d/arcsight_services start all</code>. 11. Import Threat Intelligence Platform v4.3.
OCTCR331854067	<p>Certain types of filter changes would fail to work correctly.</p> <p>Workaround:Software update in 7.8.</p>
OCTCR331828028	<p>ESM was not ingesting events from Transformation Hub.</p> <p>Workaround:Software update in 7.7.</p>

Issue	Description
OCTCR33I829027	Mbus/Kafka Serialization Error in Correlator Workaround: Software update in 7.7.1.
OCTCR33I736002	Customer experiencing a velocity template issue. Workaround: <ol style="list-style-type: none"> 1. Stop all services: <code>/etc/init.d/arcsight_services stop all</code> 2. Add the following line to <code>/opt/arcsight/manager/config/velocity.properties</code> <code>velocity.engine.restricted.classes=</code> 3. Restart ESM: <code>/etc/init.d/arcsight_services start all</code>. <p>If empty value is not accepted by VelocityEngine, then change the setting to something like the following and restart ESM: <code>velocity.engine.restricted.classes=foo.bar</code>.</p>
OCTCR33I790002	ActiveChannel view field looks empty. Workaround: Software update in 7.7.
OCTCR33I715047	LoginEnable field on Swagger does not update via API. Workaround: Software update in 7.8.
OCTCR33I865063	When making API calls checking the status of a rule with variable it no longer shows the status of the rule is enabled or disabled. Workaround: Software update in 7.8.
OCTCR33I891108	API call always unsets 'deprecated' state of QueryViewer if the attribute 'deprecated' is not explicitly specified in API update request. Workaround: Software update in 7.8.

ArcSight Console

Issue	Description
OCTCR33I891189	Console doesn't show any Fields under Unassigned Group. Workaround: Software update in 7.8.

ArcSight Manager

Issue	Description
OCTCR33I611106	<p>During manager startup the following warnings can be found multiple times in <code>server.std.log</code> under <code>/opt/arcsight/var/logs/manager/default</code>: Failed to create KeyManager and BCFKS not found. This is for distributed FIPS mode installations only.</p> <p>Workaround: It can be safely ignored.</p>
OCTCR33I895031	<p>The <code>repoCA</code> folder of the distributed environment is not maintained/copied into the new manager folder during the upgrade from ESM 7.6.4 to 7.7 .</p> <p>Workaround: Copy the folder from the <code>manager.preUpgradeBackup</code> into <code>/opt/arcsight/manager</code>. If the customer has already run the last step of the upgrade, see "Completing Optional Post-Upgrade Tasks" in the Upgrade Guide.</p>

Command Center

Issue	Description
NGS-27696	The fill text in Events > Event Search for historical events displays properly.
NGS-32851	Fixed the false positive.
NGS-26382	SOC Manager Dashboard metrics grid view displays the full history.
NGS-19267	You can restrict access to cases by user in the ArcSight Command Center.
OCTCR33I876015	<p>After Upgrade, when clicking ESM - Command Center from Fusion, it shows blank page.</p> <p>Workaround:Software update in 7.7.</p>

ArcSight Fusion

Issue	Description
NGS-33393	The Case Breakdown widget legend renders correctly.
ANGUX-1059	When you change the title of the Active Lists widget, the filter settings for the widget no longer disappear.
ANGUX-1041	The dashboards will display correctly.
ANGUX-990	ESM Command Center will appear correctly.
ANGUX-838	You will no longer receive an error message.
ANGUX-776	The Case Breakdown widget displays data for the specified assigned owners or owner groups when you choose to group the data by Assigned Owner Group or Assigned Owner.

Connectors

Issue	Description
OCTCR33I234215	The error has been fixed.

Installation and Upgrade

Issue	Description
OCTCR33I610022	<p>Running the GUI installer can sometimes cause the firstboot wizard to exit prematurely with a timeout error.</p> <p>Workaround: When installing ESM 7.6.4 on a FIPS-enabled, distributed cluster, both the installer and first boot wizard need to be run in console mode, and not using the installer GUI on the non-persistor cluster nodes.</p>

Open Issues

This release contains the following open issues.

Installation and Upgrade

Issue	Description
OCTCR33I943037	<p>Upgrade to ESM 7.8 on a G10 appliance that is running Red Hat Enterprise Linux (RHEL) 8.8 fails with the following message:</p> <pre>Pre-Install check failed: Package numactl is required.</pre> <p>Workaround: Install the missing numactl-libs and numactl packages.</p>
OCTCR33I941104	<p>Upgrade or install ESM24.3(7.8) on Redhat Linux 9.2 fails with error message during the preflight check:</p> <pre>Pre-Install check failed: Package ncurses-compat-libs is required. Please exit the installer and install it first.</pre> <p>Workaround: Install the missing ncurses-compat-libs package.</p>
OCTCR33I345079	<p>Attempting to reinstall the Security Monitoring - Base package results in an error.</p> <p>Workaround: Before you reinstall the Security Monitoring - Base package, ensure you restart Manager first.</p>
OCTCR33I231637	<p>In some cases, an upgrade might fail with a message stating that the arcsight user does not own some files.</p> <p>Workaround: The message directs you to the file nonArcSightFiles.txt. If the files that are listed in nonArcSightFiles.txt are in a directory of the form /opt/arcsight/manager.preUpgradeBackup.NNNNNNNNNN (ending in a 10-digit number), change the ownership of the files to user arcsight and then re-run the upgrade. The upgrade should complete successfully.</p>

Issue	Description
OCTCR33I235092	<p>If you are upgrading in distributed mode, an automated step recreates the configurations of all <code>mbus_data</code> and <code>mbus_control</code> instances. If the cluster is busy with other upgrade processes, this automated step might fail on one or more nodes. If the step fails, there is no configuration directory for any affected <code>mbus</code> instances. As a result, the <code>mbus</code> instance cannot start.</p> <p>Workaround: Ensure <code>repo</code> is running, then complete the following steps:</p> <ol style="list-style-type: none"> 1. Log in to the affected node as <code>arcsight</code> user. 2. Go to <code>/opt/arcsight/manager</code>, and run the following command: <pre>bin/arcsight mbus-configure-instances</pre> <p>The command automatically locates the <code>mbus</code> instances on the current node and correctly configures them.</p> 3. Repeat these steps for all affected nodes. 4. From the persistor, run the following: <ul style="list-style-type: none"> • <code>/etc/init.d/arcsight_services stop</code> • <code>/etc/init.d/arcsight_services start</code>
NGS-26661	<p>The log message <code>Could not convert table(s) arc_trend_XXXXXX without column details in arc_db_table_schema</code> in the upgrade log means the table schema for <code>arc_trend_XXXXXX</code> could not be found from schema table. ESM could not perform upgrade on table <code>arc_trend_XXXXXX</code>.</p>
NGS-21995	<p>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.</p> <p>Workaround: Rebuild the invalidated resource after the upgrade.</p>
NGS-21133	<p>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.</p> <p>Workaround: If this is the case, check the upgrade log file <code>/opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log</code> to determine if it contains this message:</p> <pre>"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."</pre> <p>To prevent this failure, make sure the fully qualified domain name is configured properly on the ESM host before starting the upgrade.</p>
NGS-14188	<p>ArcSight Console installation on non-English path in Windows machines fails to configure the ArcSight Console.</p> <p>Workaround: Use English filenames in installation paths. Or run ArcSight Console configuration after installation finished by running the <code>consolesetup</code> script from the ArcSight Console <code>..\current\bin</code> directory.</p>

General

Issue	Description
OCTCR33I370003	<p>If you delete a rule in a folder from the ESM web application, retrieving rules from that folder returns a bad request.</p> <p>Workaround: Reload the resource again from the grid.</p> <p>Note: This issue has a unique Octane number: 905453.</p>
OCTCR33I935015	<p>During the installation of ArcSight Information Repository, multiple Failed to create KeyManager errors could be displayed. These occur as the repowizard is trying to load repokeystore.client.bcfs which does not exist yet and will be created during the process.</p> <p>Workaround: Once the store is created, no more error messages will be displayed. This issue does not affect first boot setup completion.</p>
OCTCR33I386094	<p>Setting the <code>jmx.rmi.enabled</code> property value in the <code>esm.properties</code> file affects only the correlator and aggregator services. The repo and mbus services do not recognize it.</p> <p>Workaround: To affect all services, use the <code>jmx.rmi.enabled</code> property value in the <code>esm.defaults.properties</code> file.</p>
OCTCR33I384086	<p>If your ESM environment is installed on either the CentOS 8.x or Redhat 8.x platforms, the <code>disasterrecovery</code> command does not work.</p> <p>Workaround: Prior to running the <code>disasterrecovery</code> command, create the following directory:</p> <pre>/opt/arcsight/logger/current/arcsight/logger/tmp/configs</pre> <p>After you create this directory, the <code>disasterrecovery</code> command works without error.</p>
NGS-33318	<p>If you start services on an APHA distributed mode persistor after installation or upgrade, ESM might attempt to move the repo instance on the persistor to another node. At the end of this process, you might receive the following message:</p> <pre>RESULT: repositup terminated abnormally.</pre> <p>Typically this message is incorrect and everything actually worked properly.</p> <p>To check, run the following:</p> <pre>/etc/init.d/arcsight_services statusByNode</pre> <p>Ensure that all repo instances are up, and that there are no repo instances on the persistor.</p>

Analytics

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-26380	In the Last State data monitor, the Override Status and Remove Entry options are not working correctly.
NGS-24957	The GetSessionData function that uses sessionlist with multiple keys may show an incorrect result.
OCTCR33I233579	In distributed mode, when a user deletes a list that a rule references, the rule is disabled but continues to fire.

ArcSight Console

Issue	Description
OCTCR33I386148	In the default Transformation Hub audit events active channel, as well as any custom audit event channels, the Device Event Class ID and Device Event Category columns incorrectly refer to Event Broker instead of Transformation Hub. This does not affect functionality in any way.
OCTCR33I235130	When you create a drill-down definition, you can base it all available attributes. When viewing a query viewer in a chart, however, not all attributes are visible. Drill-down definitions that use attributes that are not part of a chart view are invalid. Workaround: Use a table to view the query viewer.
NGS-29487	An issue with font rendering on Windows and Linux operating systems can affect how the Console displays resource names containing one or more "." characters. For example, the resource name is clipped in the resource tree or a resource name might extend over a nearby component on the screen. Workaround: Change the ESM Console font to one that does not demonstrate this behavior, such as Arial. To change the font for the ESM Console, go to Edit > Preferences , and select Global Options . Change the font to Arial, and apply the changes.

Issue	Description
NGS-29702	<p>If your local computer is in a different timezone than the ESM server, any event search attempts to use the local time instead of the server time. For example, if you create an Active Channel that uses the ESM server time, and then perform an event search, the event search uses the local time range. As a result, there is a mismatch and the event cannot be found.</p> <p>Workaround: When you perform an event search, specify the time zone for the ESM server.</p>
NGS-27091	<p>Drill down from stacked bar charts doesn't work as expected.</p>
NGS-26915	<p>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.</p>
NGS-25631	<p>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.</p>
NGS-23639	<p>When you start ArcSight Investigate from ESM on string based fields containing leading or trailing spaces, the search will fail.</p> <p>Workaround:</p> <p>In such cases, manually fix the spaces before or after the value.</p>
NGS-23554	<p>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.</p> <p>Workaround:</p> <p>Change the search field value to one of the following:</p> <ul style="list-style-type: none"> • String value: ' ', NONE • Integer value: 0, NONE
NGS-23489	<p>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).</p> <p>Workaround:</p> <p>Delete the file "/tmp/exportfile.pkcs12" and re-run consolesetup for the second user to transfer settings again.</p>
NGS-23444	<p>When ArcSight Console is in dark theme and you run the "arcsight replayfilegen" command, you will have difficulty following instructions on the Wizard.</p> <p>Workaround:</p> <p>Run the command when the ArcSight Console is in the default theme.</p>

Issue	Description
NGS-23214	<p>In FIPS mode, if you have used <code>changepassword</code> to encrypt either <code>ssl.keystore.password</code> or <code>ssl.truststore.password</code>, and then you run <code>consolesetup</code>, check <code>config/client.properties</code> to make sure that you do not have entries for both</p> <p><code>ssl.keystore.password</code></p> <p><code>ssl.keystore.password.encrypted</code></p> <p>and likewise for <code>ssl.truststore.password</code>. If you do, remove the entry that is not encrypted.</p> <p>If you do not do this, then the ArcSight Console might not run properly.</p>
NGS-22659	<p>When you open two dashboards (All Monitored Devices and Critical Monitored Devices) while the Console is set to dark theme in <code>/All Dashboards/ArcSight Administration/Devices/</code> and exit or close, you are prompted to save them even when no changes are made.</p> <p>Workaround:</p> <p>Select Yes and save the dashboards. The next time you open and close these dashboards, you do not get the save prompt.</p>
NGS-21831	<p>The <code>InSubnet</code> condition strictly enforces the use of the wildcard asterisk <code>"*"</code>. For example, a filter like <code>10.10.</code> is invalid, and <code>10.10.*.*</code> is valid.</p> <p>Old content that uses <code>inSubnet</code> without a supported format (2-address, or CIDR, or wildcard) will need to use a supported format.</p>
NGS-19880	<p>On Linux, mouse interaction with ArcSight Console after maximizing may not respond as expected.</p> <p>Workaround:</p> <p>Instead of maximizing, drag corners of ArcSight Console to resize to fill desktop.</p>

ArcSight Manager

Issue	Description
OCTCR33I231646	<p>If you uninstall the Security Monitoring - Base package, some resources will be unavailable, such as the variables related to MITRE ATT&CK.</p> <p>Workaround: Uninstall the Security Monitoring - Base - Active List package, and then reinstall both packages.</p>
NGS-26917	<p>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 are 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.</p>

Issue	Description
NGS-26217	When running the arcsight correlationsetup wizard, even if the user terminates the wizard without completing the configuration of a correlator or aggregator instance, the service id generated and reserved for that instance will not be used for future instances. This may result in 'gaps' in service ids of configured instances. There is no negative side effect on the functionality of the system due to this behavior.
NGS-25604	Some reports may run more slowly in ESM distributed mode as compared to compact mode.

Issue	Description
NGS-23503	<p>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.</p> <p>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.</p> <p>Workaround:</p> <p>Use the following procedure when the certificate of a source ESM Manager of a Forwarding Connector has changed:</p> <ol style="list-style-type: none"> 1. Export the new Manager certificate from the source Manager. 2. Change the directory to /opt/arcsight/fwdconn/current. 3. 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.) <pre>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"</pre> <pre>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-1.0.2.jar -J-Djava.security.egd=file:/dev/urandom -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388"</pre> 4. Import the source Manager certificate into Forwarding Connector truststore (SmartConnector User Guide) 5. Run the runagentsetup command on Forwarding Connector to re-register the destination Managers to the connector. <p>The full alias of the Manager certificate may be found by running the keytool command with the -list option using the following sample:</p> <pre>jre/bin/keytool -keystore jre/lib/security/cacerts -list -storepass changeit</pre>

Issue	Description
NGS-14260	<p>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:</p> <ol style="list-style-type: none"> 1. ESM running very slowly. 2. Cannot make a new SSH connection to the system. <p>ESM will run normally after the resource exhaustion ends. But the following continuing symptoms may be seen:</p> <ol style="list-style-type: none"> 1. HA will not failover via arcsight_cluster offline. 2. HA may report that the resources "ESM", "Filesystem", and "Service IP" are Stopped, when they evidently are running normally. <p>If these symptoms are seen together, the primary system should be rebooted.</p>

CORR-Engine

Issue	Description
NGS-33937	<p>In a very limited number of circumstances, if an active list configured with a very low capacity (less than 10,000) is at capacity (near 100%), a correlator or aggregator might fail to retain some of the list entries during initial load. To detect whether this is occurring, compare the number of entries loaded via the logs or manage.jsp between the persister and the aggregator or correlator.</p> <p>Workaround: If this issue occurs, you can resolve it by doing one of the following:</p> <ul style="list-style-type: none"> • Configure the list to a higher capacity. • Disable the list size management by setting <code>activelist.eviction.enabled=false</code> in <code>server.properties</code>. <p>Note: Setting the <code>activelist.eviction.enabled</code> property to false disables all internal size management for lists with cache model set to write-synchronized. It has no effect on other lists.</p>
OCTCR33I234098	<p>When you run a peer search with an ESM installation as a peer, ESM disregards the hit count limit.</p>
NGS-14477	<p>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.</p>

Command Center

Issue	Description
OCTCR33I907056	<p>ESM Certificate needs to be specifically imported into the browser if ESM is using self signed certificate and is OSP enabled.</p> <p>Workaround: Execute this url: <a href="https://<osp_host>/osp/a/default/auth/oauth2/.well-known/openid-configuration">https://<osp_host>/osp/a/default/auth/oauth2/.well-known/openid-configuration that imports certificate, then login to ACC.</p>
OCTCR33I364043	<p>If you use OSP Client Only Authentication in your environment, you might experience an issue where logging out of ArcSight Command Center does not log you out. Instead, your session will return you to the main ArcSight Command Center landing page and you remain logged in. This occurs when the IdP session timeout setting is larger than the OSP token expiration setting.</p> <p>Workaround: After you log out of ArcSight Command Center, close your browser.</p>
NGS-32858	<p>The MITRE Activity Dashboard might be blank, even if there is data in the Rules Triggered with Mitre ID Active List (/All Active Lists/ArcSight Foundation/MITRE ATT&CK/Rules Triggered).</p> <p>Workaround: Delete the row with empty values or manually update the row with the correct data.</p>
NGS-29702	<p>If your local computer is in a different timezone than the ESM server, any event search attempts to use the local time instead of the server time. For example, if you create an Active Channel that uses the ESM server time, and then perform an event search, the event search uses the local time range. As a result, there is a mismatch and the event cannot be found.</p> <p>Workaround: When you perform an event search, specify the time zone for the ESM server.</p>
OCTCR33I233578	<p>When you create a condition in a channel or an Active List, if the AND and OR operators are at the parent level, the filter summary does not include the OR.</p> <p>Workaround: Ensure there is only one operator at the parent level. You can then add other operators under the parent operator.</p>
OCTCR33I235091	<p>If license usage data is corrupted, the 45-median report will state, "No results were returned from the server."</p>
NGS-26357	<p>While viewing dashboards in the ArcSight Command Center, charts might appear small.</p> <p>Workaround: Refresh the page for proper rendering.</p>
NGS-23437	<p>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.</p>

Issue	Description
NGS-23429	<p>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:</p> <pre> vfs.report.provider.scheme=db vfs.report.provider.class=com.arcsight.common.vfs.database.ArcDatabaseFileProvider vfs.report.provider.base=db://reports/archive </pre> <p>Workaround: Run the report in PDF format.</p>
NGS-23105	<p>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.</p>
NGS-22583	<p>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.</p>
NGS-22573	<p>The ArcSight Command Center Users 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.</p> <p>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.</p> <p>Note that peering and content management are not supported if either manager in the peer relationship is in FIPS Suite B mode.</p>
NGS-21986	<p>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 JavaScript unresponsive error.</p> <p>Workaround: Limit the data monitor to six variable fields with 10 rows, or split the fields by creating one or more data monitors.</p>

Issue	Description
NGS-21930	<p>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.</p> <p>Workaround:</p> <p>On the ArcSight Command Center:</p> <ol style="list-style-type: none"> 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	<p>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.</p> <p>Workaround: Refresh the page (press F5).</p>
NGS-17407	<p>If the system has too many notifications, the ArcSight Command Center will not show notification counts in the notification view.</p> <p>Workaround: Stop the Manager, delete unused notifications such as undeliverable or old pending notifications, and start the Manager.</p>

ArcSight Fusion

Issue	Description
OCTCR33I409044	<p>ESM 7.6.4 allows you to install ESM, CDF, and a single Vertica node on the same computer. ESM 7.6.4 and CDF both support FIPS but the version of Vertica 11 included in the installer does not. If you attempt to perform an "all-in-one" installation on a computer with FIPS mode enabled, the installation procedure fails.</p> <p>Workaround:</p> <p>If you want to install everything on the same computer, disable FIPS mode on the computer and then specify non-FIPS mode in the installation program.</p> <p>If you want to run ESM 7.6.4 and CDF in FIPS mode, you can install them on one computer and connect to a separate non-FIPS Vertica installation.</p>
OCTCR33I376074	<p>When you attempt to disable the Track Rules with MITRE ID rule, the rule is not disabled.</p> <p>Workaround: Use the Console to disable the rule.</p>
ANGUX-971	<p>When running the install-single-node.sh script on a server that uses a non-English operating system, the installation process fails.</p> <p>Workaround: Change the operating system to English, then run the installation scripts. Upon a successful installation and deployment, change the operating system back to the original language.</p>

Issue	Description												
ANGUX-574	In Fusion, when you attempt to delete a dashboard whose title includes special characters, the Dashboard displays a success message but the deletion fails. Workaround: Rename the dashboard, then delete it.												
ANGUX-634	If you attempt to delete a large number of dashboards, such as 35 or more, the resulting message displays an error and does not specify which dashboards were deleted or not.												
Bug 1145490 Bug 1144088	<p>Known issues associated with RedHat can affect Fusion by causing sluggish performance and errors in the server log, particularly in a single-node deployment.</p> <ul style="list-style-type: none"> You might observe slow responses times and that some of the deployed pods enter the “CrashLoopBackoff” state. This issue tends to occur because of large quantities of calls to the NFS client. (Bug 1145490) When logging into Fusion, the server might send the user back to the login page, particularly after you first install Fusion. You would see the following type of error in the idi-web-app log: Unable to fetch user details from management after retrying, error: StatusCodeError: 401 (Bug 1144088) After logging into Fusion, you may be redirected to ADMIN > Account Groups page wherever you click on the user interface. (Bug 1144088) <p>Workaround:</p> <ol style="list-style-type: none"> Follow the instructions in RedHat Solution 3915571. Restart the User Management pod by performing the following: <ol style="list-style-type: none"> Get the User Management pod details: <pre>kubectl get pods --all-namespaces grep hercules-management</pre> <p>Example output:</p> <table border="1"> <thead> <tr> <th>NAMESPACE</th> <th>NAME</th> <th>READY</th> <th>STATUS</th> <th>RESTARTS</th> <th>AGE</th> </tr> </thead> <tbody> <tr> <td>arcsight-installer-p2d1t</td> <td>hercules-management-7f876b4978-9xk16</td> <td>2/2</td> <td>Running</td> <td>6</td> <td>10d</td> </tr> </tbody> </table> Delete the User Management pod: <pre>kubectl delete pod -n <namespace> <management pod name></pre> <p>Example:</p> <pre>kubectl delete pod -n arcsight-installer-p2d1t hercules-management-7f876b4978-9xk16</pre> <p>When you delete any pod, the pod will start automatically.</p> 	NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE	arcsight-installer-p2d1t	hercules-management-7f876b4978-9xk16	2/2	Running	6	10d
NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE								
arcsight-installer-p2d1t	hercules-management-7f876b4978-9xk16	2/2	Running	6	10d								

Connector Management

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

Connectors

Issue	Description
OCTCR33I235042	The connector upgrade process fails the first time you try to run it from the Console. Workaround: Please restart the Console, connect to ESM, and start the connector upgrade process again. The upgrade will proceed without further error.
NGS-13049	When upgrading the Forwarding Connector, two fatal exception messages will appear, regarding [agents[0].arcsightuser] and [agents[0].arcsightpassword]. You can safely ignore these messages.
NGS-12407	Annotation flag indicating 'forwarded' may not get set when forwarding events from ESM.

Active Passive High Availability Module

Issue	Description
OCTCR33I233541	On a RHEL or CentOS 7.x APHA system running in IPv6 only mode, APHA software might not start automatically after reboot. Workaround: As user root, run <code>crm cluster start</code> on the node where the software does not start.

Localization

Issue	Description
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.

Publication Status

Released: August 2024

Updated: Wednesday, January 8, 2025

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ESM 7.8 Release Notes (ESM 7.8)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!