Micro Focus Security ArcSight ESM

Software Version: 7.3

ESM 7.3 Release Notes

Document Release Date: July 2020
Software Release Date: July 2020

Legal Notices

Copyright Notice

Trademark Notices

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 7.3 6
What's New in This Release 6
ArcSight Command Center in Fusion 6
Read from Avro Topics 7
Upgrade Enhancements 7
OSP Client Only Authentication Enhancements 7
ArcSight Console Enhancements 8
ArcSight Command Center Enhancements 8
Improved Response Codes for new APIs 8
Use SAN Field from PKCS#11 Token as User's External ID 9
Threat Detector Automatically Enabled 9
Verifying the Downloaded Installation Software 9
Upgrade Support 10
Upgrade Paths for Earlier Versions 10
Geographical Information Update 10
Vulnerability Updates 10
Supported Versions for Distributed Searches 11
Supported Platforms 11
Supported Languages 11
Support for ActivClient Issues 11
Section 508 Compliance 13
Usage Notes 13
Required Workarounds for G10 Appliance 13
Uninstall the Chrony RPM 13
Remove Health-related RPMs 14
Configuring Connectors to Write to Transformation Hub 14
ArcSight Command Center 14
Scroll Bar Issues with Google Chrome and Apple Safari 14
Viewing Secure Operations Center Dashboard Using Edge Browser on Windows 10 15
ArcSight Console 16
Events from Transformation Hub 16
Using Windows 10 16
Oversized Pie Charts on Dashboards 16

Limit on Dashboards Being Viewed 16
Distributed Correlation Mode 17
Configuration Changes Require Restart of All Services 17
Active List Updates in Distributed Correlation 17
Stop and Start All Services if a Major Service is Stopped 17
Stopping Message Bus Services 18
Hierarchy Map Data Monitor in Distributed Correlation - Not Recommended 18
Converting IPv4 to IPv6 in Distributed Correlation Mode - Consult Professional Services 18
Distributed Cache Inconsistency 19
Large Lists Can Take Time to Load on Cluster Startup 20
Using the Edge Browser 20
Oversized Event Graphs 20
Full Text Search 20
ESM Peer Certification for Content Synchronization 21
ESM and Logger Connectivity 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
New Default Setting for Session List Entry Expiration Time 24
Deprecated - Optimize Data Feature for Active Lists 24
Unsupported Features in This Release 25

Resolved Issues 27
Analytics 27
ArcSight Console 28
ArcSight Manager 28
Command Center 29
Installation and Upgrade 29

Open Issues 30
General 30

Analytics 30
ArcSight Console 31
ArcSight Manager 34
CORR-Engine 37
Command Center 38
ArcSight Fusion 40
Connector Management 43
Connectors 43
Installation and Upgrade 43
Localization 45
Reports 45

Security Fixes 46

Send Documentation Feedback 47

Welcome to ESM 7.3

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 Micro Focus online portal for submitting feature requests.

What's New in This Release

This topic describes the new features and enhancements in ESM 7.3.

Updated guides for ESM 7.3 are available on the ESM documentation page.

ArcSight Command Center in Fusion

Command Center is now available in Fusion.

Deploying ArcSight Command Center for ESM (ESM for Fusion) in this platform incorporates the dashboards and some functions of the ArcSight Command Center console. Users will be able to run and review searches, reports, and case management, as well as perform administrative functions for managing active channels, content, connectors, storage, archives, search filters, saved searches, peer configuration, and system logs. For the Dashboard, ESM for Fusion adds several widgets that display data from your ESM sources. If you also deploy the Layered Analytics capability, widgets such as the Active Lists widget can incorporate data from both ESM and Interset for greater insights. If you want to create widgets specific for your organization, you can build them in the Widget SDK.

Note: The Command Center console deployed in this platform (ESM for Fusion) and the Command Center console installed separately with ESM can run concurrently.

ESM for Fusion scales to match the footprint of your environment. You can install ESM for Fusion on the same server as ESM, if there are enough spare resources on the server, or install on multiple servers.

All Command Center functionality is available from Fusion, with the following limitations:

- On the Logger configuration pages, the search, search filters, and peers functions do not work in Google Chrome. Instead, use Mozilla Firefox. Upon first use, you must clear the browser cache.
- The **Tools** menu does not work.
- If you enter the Command Center URL directly from Fusion and the ESM host is not configured, the Command Center login will display.
- To switch to Command Center from Fusion the first time, you must click the back button three times. After the first time, you must click the back button twice when you want to switch to Command Center from Fusion.

To use this feature, you must install ESM in Fusion and then configure the ESM host in Fusion. For more information, see the documentation for ArcSight Fusion.

Read from Avro Topics

You can now specify Avro topics when you configure a connection to Transformation Hub version 3.3.0. ESM will read Avro-format events from any topic where the name contains "avro" in lower case. For example, `th-arcsight-avro`. For more information, see the *ESM Installation Guide* on the ESM documentation page.

Upgrade Enhancements

In both GUI mode and console mode, the upgrade process displays ongoing status updates with details about what it is doing. For example, `Upgrading database`, `Updating startup scripts`, or `Completing installation`.

OSP Client Only Authentication Enhancements

In this version, the OSP Client Only Authentication method supports all FIPS modes.

Additional security enhancements require the server and console keystores trust the OSP certificate.

For more information, see the “One SSO Provider (OSP) Authentication” topic in the *ESM Administrator’s Guide* on the ESM documentation page.

ArcSight Console Enhancements

New features in the ArcSight Console include:

- The **Optimize Data** option has been deprecated and is no longer available.
- Users can now debug a rule by creating an active channel with the filter condition defined in the rule.
- You can use rules to create a ticket in ServiceNow® ITSM.
- Security Operation Center (SOC) Analysts can now:
  - Use short cut keys to run searches in Recon.
  - Use an Active List to create an event graph.
  - Create a ServiceNow ticket from a rule.

For more information about these features, see the *ArcSight Console User's Guide* on the ESM documentation page.

ArcSight Command Center Enhancements

New features and enhancements in ArcSight Command Center include:

- Users in the Analyzer Administrators group can access the Security Operation Center (SOC) Dashboard by default. All other users in non-administrator groups need read access to the following resource groups:
  - /All Data Monitors/ArcSight Foundation/ArcSight SocView
  - /All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview
  - /All Query Viewers/ArcSight Foundation/ArcSight SocView
  - /All Filters/ArcSight Foundation/ArcSight SocView
  - /All Filters/ArcSight System/Event Types
- Users can access the ESM API documentation by clicking **Help > API**.

For more information about these features, see the *Command Center User's Guide* on the ESM documentation page.

Improved Response Codes for new APIs

New APIs that contain `/esm-api` in the URL have improved http response codes over older APIs. Following are the response codes for new APIs:

- 400

  This response code applies to validation errors.

- 401

  This response code applies to authentication exceptions.
- 403

  This response code applies to authorization exceptions.
- 404

  This response code applies to invalid paths.

Old APIs continue to give a response code of 400 for invalid paths and 500 for errors and exceptions, but include improved error messages.

Use SAN Field from PKCS#11 Token as User's External ID

You can now use the SAN field from a PKCS#11 token as the ESM user's external ID.

To enable this feature, you must add the property `auth.userlookup.ssl.sanfield=upn` to the `server.properties` file under `manager/conf`. By default, the field does not exist in `server.properties`. With this field set to `upn`, the user lookup module will use the Subject Alternative Name: Principal Name(UPN) field instead of defaulting to the subject's common name.

To disable this feature, you must remove the property from the `server.properties` file.

Threat Detector Automatically Enabled

Threat Detector (formerly known as Pattern Discovery) enables you to discover and analyze previously unknown patterns that might pose a threat. This feature is automatically enabled upon installation or upgrade to ESM 7.3. For more information, see the *ArcSight Console User's Guide* on the ESM documentation page.

Verifying the Downloaded Installation Software

After you download the software, contact support to verify that the signed software you received is indeed from Micro Focus and has not been manipulated by a third party.

Upgrade Support

If you are running ESM version 7.2 or 7.2 Service Pack 1, you can upgrade directly to ESM 7.3.

Upgrade Paths for Earlier Versions

Following are the upgrade paths for ESM versions earlier than 7.2 (in both compact mode and distributed correlation mode) and ESM on an appliance:

- If you plan to upgrade from ESM 6.11:
  a. Upgrade to ESM 7.0 Patch 1.
  b. Upgrade to ESM 7.2.
- If you plan to upgrade from ESM 7.0:
  a. Apply ESM 7.0 Patch 2.
  b. Upgrade to ESM 7.2.
- If you plan to upgrade from ESM 7.0 Patch 1 or Patch 2, upgrade to ESM 7.2.

For information about supported platforms, see the ESM Support Matrix 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_2020601.

Vulnerability Updates

This release includes recent vulnerability mappings from the March 2020 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2983	Bugtraq,CVE
Cisco Secure IDS S1040	CVE
Juniper IDP update 3286	Bugtraq, CVE, MSSB
McAfee HIPS 7.0/8.0 content version 10141	CVE

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 IPv6 data search are ESM 6.11.0 and above.

For more information about distributed searches, see the *Command Center User's Guide* on the ESM documentation page.

Supported Platforms

For information about ESM 7.3 platform and browser support, see the ESM Support Matrix on the ESM documentation page.

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 Micro Focus.

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

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.

Section 508 Compliance

ArcSight recognizes the importance of accessibility as a product initiative. To that end, ArcSight continues to make advances in the area of accessibility in its product lines.

Usage Notes

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

To remove the chrony RPM, you can use one of the following methods:

- Pre-setup
- Post-setup

Pre-setup

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.

Post-setup

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 hp-health package, run the following:
   `yum remove hp-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 SmartConnector to write binary events to a Transformation Hub topic for consumption by ESM 7.3, 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 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.
- *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

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 7.3 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.
- 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 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` with the following property:

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

For more information, see the *ESM Administrator's Guide* on the ESM documentation page.

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.

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 Command 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.

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 inconsistency . . . "**.
3. Hover your mouse pointer over the **"Hazelcast cluster inconsistency . . . "** 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 service. For example:

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

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

5. Run this command to remove information repository records from non-responsive distributed cache instances; for example, for the instance *dcache2*:

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

   Run this command if a standalone distributed cache instance did not properly shutdown or was abruptly disconnected (for example, due to a network problem) and as a result is still reported as available according to information repository runtime records, but is not accessible from the persistor.

In the above example, the command cleans internal runtime record for `dcache2` in the information repository. The record is 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.

Using the Edge Browser

- The ArcSight Console Help does not support Edge as the preferred browser. See also "Using Windows 10" on page 16 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. 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* on the ESM documentation page.

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 *Command Center User's Guide* on the ESM documentation page.

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. 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* on the ESM documentation page. The Actor Model Import Connector for Microsoft Active Directory to install for ESM 7.3 is version 8.0.0.8315.0.

See the ESM Support Matrix on the ESM documentation page for information about ESM 7.3 supported platforms.

Caution: Install and use the Actor Model Import Connector for Microsoft Active Directory that is provided with the ESM 7.3 release. That is the version of the connector that is tested and certified to work with ESM 7.3. Do not use previously-supplied versions of the Actor Model Import Connector for Microsoft Active Directory with ESM 7.3.

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* on the ESM documentation page. The Asset Model Import FlexConnector to install for ESM 7.3 is version 8.0.0.8316.0.

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 ESM Support Matrix on the ESM documentation page for information about 7.3 supported platforms.

Caution: Install and use the Asset Model Import FlexConnector that is provided with the ESM 7.3 release. That is the version of the connector that is tested and certified to work with ESM 7.3. Do not use previously-supplied versions of the Asset Model Import FlexConnector with ESM 7.3.

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 7.3.

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 on the ESM documentation page for the version that is supported with ESM 7.3.

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* on the ESM documentation page.

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* on the ESM documentation page.

New Default Setting for Session List Entry Expiration Time

The default value for the session list Entry Expiration Time was **0 second(s)**. In this case, *0 seconds* actually means *unlimited*. Now the default value for the session list Entry Expiration Time has been changed to read as **Unlimited**. For more information, see the *ArcSight Console User's Guide* on the ESM documentation page.

Deprecated - Optimize Data Feature for Active Lists

The **Optimize Data** feature for active lists is deprecated and may be removed in a future release.

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:
  - 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.
- 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 7.3:

- 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.

- Analytics 27
- ArcSight Console 28
- ArcSight Manager 28
- Command Center 29
- Installation and Upgrade 29

Analytics

Issue	Description
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.

ArcSight Console

Issue	Description
NGS-31939	On a Linux workstation, if you install the Console with OSP Client Only authentication, when you run the Console it attempts to pop up a browser. If the browser does not pop up, ensure the following: 1. The link to open the browser must point to the binary and not to a script that runs the binary. 2. When launching the browser link from the command line, there must not be any output generated there. This includes any type of output, not just errors and warnings, but informational messages as well.
NGS-31774	When using OSP authentication, a browser window/tab opens when redirecting to the OSP/IdP. After the redirect is complete, the window/tab remains open. Users must close it manually.
NGS-32452	This release resolves an issue where, if a case has a large number of correlated events attached, editing the case takes a long time.

ArcSight Manager

Issue	Description
NGS-32076	OSP client authentication relies on timestamps to determine the validity of authentication tokens, so the servers exchanging these tokens, such as the OSP server and the ESM server, must be synchronized to the same time sources.
NGS-32077	SAML2 client authentication relies on timestamps to determine the validity of authentication tokens, so the servers exchanging these tokens, such as the SAML2 server and the ESM server, must be synchronized to the same time sources.
NGS-32082	If you have mbus instances configured and you run mbussetup to add, delete, or change those instances, the following error message occurs: `Restarting Message Bus Services failed.`
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.

Command Center

Issue	Description
NGS-32031	Peer search does not work in the following environments: 1. Pure IPv6 network 2. Dual stack network with IPv6 preferred
NGS-32007	If the Command Center is configured to use OSP Client Only Authentication authentication, the following bookmarks do not redirect correctly: • https://<managerDNS>:8443/www/ui-phoenix/com.arcsight.phoenix.PhoenixLauncher/#channels • https://<managerDNS>:8443/www/ui-phoenix/com.arcsight.phoenix.PhoenixLauncher/#storage • https://<managerDNS>:8443/www/ui-phoenix/com.arcsight.phoenix.PhoenixLauncher/#license • https://<managerDNS>:8443/www/ui-phoenix/com.arcsight.phoenix.PhoenixLauncher/#eventStatistics • https://<managerDNS>:8443/www/ui-phoenix/com.arcsight.phoenix.PhoenixLauncher/#administration
NGS-20280	The WHERE operator is now supported in user-defined fields.
NGS-31903	When clicking a technique node in the MITRE Activity Dashboard, the dashboard now correctly displays the details panel close to the node.

Installation and Upgrade

Issue	Description
NGS-31397	When you are preparing your system to install ESM, if you are running RHEL or CentOS 8.x and using the GNOME desktop environment, the `ulimit` values might be too low and ESM installation might fail. **Workaround:** The issue does not occur if you log in through SSH. Using an xterm window might also resolve the issue.
NGS-31943	When you are installing ESM in console mode, ensure that the OS environmental setting for the `DISPLAY` variable is either unset or correctly set. An incorrect setting for the `DISPLAY` variable might cause the installation process to fail.

Open Issues

This release contains the following open issues.

- General 30
- Analytics 30
- ArcSight Console 31
- ArcSight Manager 34
- CORR-Engine 37
- Command Center 38
- ArcSight Fusion 40
- Connector Management 43
- Connectors 43
- Installation and Upgrade 43
- Localization 45
- Reports 45

General

Issue	Description
NGS-30460	The `disasterrecovery` command does not work with the following operating systems: • RHEL 8.x • CentOS 8.1

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.

Issue	Description
NGS-24957	The GetSessionData function that uses sessionlist with multiple keys may show an incorrect result.
NGS-29732	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
NGS-32055	The following Console command fails on Macintosh operating systems (Mac OS): `./arcsight check-console-libraries`
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.
NGS-29702	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. **Workaround**: When you perform an event search, specify the time zone for the ESM server.
NGS-27091	Drill down from stacked bar charts doesn't work as expected.
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-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.

Issue	Description
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 one of the following: • String value: `'',NONE` • Integer value: `0,NONE`
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.
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, remove the entry that is not encrypted. If you do not do this, then the ArcSight Console might not run properly.
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.

Issue	Description
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-17387	There was an issue in the reports editor where after selecting another query, or modifying the current one for the given report, the OK/Apply buttons were not being enabled correctly when doing further modifications to the Fields Table cells on the Data tab of the Report Editor.
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 contained in the Device Custom Date1 of an Active List is not being displayed accurately in the ArcSight Console. It shows the creation date of December 31, 1969.
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-32038	If you are running macOS Catalina, using dashboards might cause the console to stop unexpectedly. **Workaround:** 1. Delete the user's `.ast` file. 2. Start the console. 3. Select **Edit** > **Preferences** and select the option to use classic charts. **Note:** Integration with ServiceNow® will not work.

ArcSight Manager

Issue	Description

NGS-32039	If you set up your environment as follows:
	• ESM configured for FIPS 140-2 mode
	• Transformation Hub certificates configured in ESM for TLS Client Authentication to Transformation Hub
	When you configure the Transformation Hub connection using `managersetup`, an input topic name might not be verified to exist in Kafka. Typically, you receive a warning if a topic you entered is not currently available. Without the warning, you might not notice a mistake in a topic name, such as a copy-paste error or a typo.
	If this problem occurs, you will see no warning that the topic is invalid. If Manager is started, it will connect to Transformation Hub but will not find the configured incorrect topic. As a result, Manager will not read events from Transformation Hub.
	Workaround:
	1. Manually verify that the topic name exists in Transformation Hub. For example, the pre-configured topic `th-binary_esm` is visible in the Transformation Hub documentation.
	2. View `/opt/arcsight/var/logs/manager/default/serverwizard.log` after configuring Transformation Hub in `managersetup`.
	• If the problem occurs, `managersetup` logs this error message:
	`GET_TOPICS_FAILED: ... <reason>`
	• If the problem does not occur, `managersetup` logs this message:
	`THub has this configured topic: ... <input topic name>`
	3. (Conditional) If you receive the error message in Step 2, view `server.log` after Manager starts and verify Manager connects to Kafka within a few minutes of the log time of the "Ready" line. If Kafka readers do not read from the configured topic, identify the incorrect topic name and change the Transformation Hub topic using `managersetup`.
	• If the problem occurs, Manager logs the following two messages:
	◦ `TLS connection is successful to at least one of the configured brokers`
	◦ `Tested the Kafka configuration, and it will not work right now. Trying again in ...`
	• If the problem does not occur, Manager logs the following two messages:
	◦ `Tested Kafka configuration. Connecting to Kafka works.`
	◦ `Starting Kafka readers.`

NGS-30718	If you uninstall the Security Monitoring - Base package, some resources will be unavailable, such as the variables related to MITRE ATT&CK. **Workaround**: Uninstall the Security Monitoring - Base - Active List package, and then reinstall both packages.

Issue	Description
NGS-29788	Using five-digit Unicode characters in the **Destination user name** field causes the following: • An Active Channel might not display existing events. • When running a report, the **THETEXT** column might contain the following incorrect string value at row 354359: `\xF0\x9F\x92\x98\xF0\x9F...` **Workaround**: Do not use five-digit Unicode characters in the **Destination user name** field.
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 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.
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	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* on the ESM documentation page. 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=file:/dev/urandom -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 the `runagentsetup` command 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 Transformation Hub 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 Transformation Hub connected to ESM. Ensure that the Transformation Hub is running properly.
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 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-9734	In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.
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.

CORR-Engine

Issue	Description
NGS-28849	If a rule creates a large number of cases (500,000 or more), the persistor and embedded dcache might run out of memory. **Workaround:** Use the Manager Configuration Wizard to increase the Java heap memory size.
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.

Command Center

Issue	Description
NGS-32851	When scanning the `cdf-2020.05.00100-2.3.0.7.zip` file or an installer `*.tar` file that contains this file, certain malware detection programs might report a false positive in a subroutine called updateRoleId. This subroutine is within `/cdf/images/cdf-master-images.tgz` file. **Workaround:** None needed. We validated that the code is not malware. We have verified that the package was built and compiled in a secure and trusted fashion. In an coming release, we will modify the packaging to avoid this false positive.
NGS-32858	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). **Workaround:** Delete the row with empty values or manually update the row with the correct data.
NGS-29702	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. **Workaround**: When you perform an event search, specify the time zone for the ESM server.
NGS-29743	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. **Workaround**: Ensure there is only one operator at the parent level. You can then add other operators under the parent operator.
NGS-30647	If license usage data is corrupted, the 45-median report will state, "No results were returned from the server."
NGS-26382	When a case is expanded in the SOC Manager Dashboard metrics grid view, full history may not be displayed. **Workaround:** In this situation, 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-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.

Issue	Description
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.
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* on the ESM documentation page 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-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 JavaScript 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.

Issue	Description
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-19267	You cannot restrict access to cases by user in the ArcSight Command Center.
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.

ArcSight Fusion

Issue	Description
ANGUX-1059	When you change the title of the Active Lists widget, the filter settings for the widget disappear. No action you take can make the settings reappear. This issue occurs only if you attempt to change the title before configuring the filter settings. **Workaround:** Do not change the title of the widget or deselect Display Widget Title until after you have modified the widget settings.
ANGUX-971	When running the install-single-node.sh script on a server that uses a non-English operating system, the installation process fails. **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.

Issue	Description
ANGUX-1041	After you upgrade Fusion, the Dashboard flickers or fails to display appropriately. This issue occurs because you had set an out-of-the-box dashboard as a default dashboard with the previous release, but the upgrade process moved the built-in dashboards to a new location. **Workaround:** Perform one of the following actions: • Log in using the URL for the Dashboards list page: `https://<host>/dashboard/list`. From this page, you can reset the default dashboard. • Log in to the URL for the specific dashboard: `https://<host>/dashboard/<the_dashboard's_UUID>`. From this page, you can reset the dashboard as a default dashboard.
ANGUX-990	It is possible that the option for ESM Command Center or Dashboard fails to appear in the UI even though you have deployed Fusion and ESM Command Center for Fusion. And for ESM Command Center you have also configured the ESM Host settings in the CDF Management Portal. **Workaround:** If this issue occurs, restart the dashboard-web-app pod. Use the following command: `kubectl delete pod -n <namespace> <dashboard-web-app pod name>` For example: `kubectl delete pod -n arcsight-install-test dashboard-web-app` When you delete a pod, the pod restarts automatically.
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-838	If Fusion and Interset are in the same cluster in your environment, and the CDF Management portal is open in another browser tab, when you click any entity in the Entity Count Overview widget, you receive the following error:
	
	`Bad Message 413`
	
	`reason: Request Entity Too Large`
	
	Workaround: Clear the browser cookies store and cache, and then close the CDF Management portal.

<table>
<tr><th>Issue</th><th>Description</th></tr>
<tr><td>ANGUX-776</td><td>The Case Breakdown widget fails to display data for the specified assigned owners or owner groups when you choose to group the data by Assigned Owner Group or Assigned Owner.

Workaround: If you select Assigned Owner or Assigned Owner Group for the Group by filter, do not specify owners or groups in the filter. Rather, leave the default value of Any.</td></tr>
<tr><td>ANGUX-634</td><td>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.</td></tr>
<tr><td>Bug 1145490

Bug 1144088</td><td>Known issues associated with RedHat can affect Fusion by causing sluggish performance and errors in the server log, particularly in a single-node deployment.
• 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: <code>StatusCodeError: 401</code>
(Bug 1144088)
• After logging into Fusion, you may be redirected to ADMIN > Account Groups page wherever you click on the user interface. (Bug 1144088)
Workaround:
1. Follow the instructions in RedHat Solution 3915571.
2. Restart the User Management pod by performing the following:
a. Get the User Management pod details:
<code>kubectl get pods --all-namespaces | grep hercules-management</code>
Example output:
<table><tr><th>NAMESPACE</th><th>NAME</th><th>READY</th><th>STATUS</th><th>RESTARTS</th><th>AGE</th></tr><tr><td>arcsight-installer-p2dlt</td><td>hercules-management-7f876b4978-9xkl6</td><td>2/2</td><td>Running</td><td>6</td><td>10d</td></tr></table>b. Delete the User Management pod:
<code>kubectl delete pod -n <namespace> <management pod name></code>
Example:
<code>kubectl delete pod -n arcsight-installer-p2dlt hercules-management-7f876b4978-9xkl6</code>
When you delete any pod, the pod will start automatically.</td></tr>
</table>

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
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.

Installation and Upgrade

Issue	Description
NGS-32790	If you are using ESM 7.2.1 with either of the following: • OSP Client Only Authentication • External SAML2 Client Only Authentication When you upgrade to ESM 7.3, the OSP configuration will be incomplete. You must run `managersetup`, accept all the default settings, and then restart manager.
NGS-32698	In some cases, an upgrade might fail with a message stating that the `arcsight` user does not own some files. **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.

Issue	Description
NGS-30503	If you are upgrading in distributed mode, an automated step recreates the configurations of all mbus_data and mbus_control 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 mbus instances. As a result, the mbus instance cannot start. **Workaround**: Ensure repo is running, then complete the following steps: 1. Log in to the affected node as `arcsight` user. 2. Go to `/opt/arcsight/manager`, and run the following command: `bin/arcsight mbus-configure-instances` The command automatically locates the mbus instances on the current node and correctly configures them. 3. Repeat these steps for all affected nodes. 4. From the persistor, run the following: • `/etc/init.d/arcsight_services stop` • `/etc/init.d/arcsight_services start`
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.
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 to determine 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-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.

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.

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.

Security Fixes

This release contains a fix for ESM 7.2 Distributed Vulnerability port 10003 (CVE-2015-0225).

Authentication is required for all JMX communication. If desired, JMX communication can be disabled by adding the property `jmx.rmi.enabled=false` to the `esm.properties` file of each cluster node.

Note: JMX communication supports status information presented in Cluster View. Turning JMX off renders Cluster View unusable.

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 7.3 Release Notes (ESM 7.3)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!