

Micro Focus Security ArcSight ESM

Software Version: 7.2

ESM 7.2 Release Notes

Document Release Date: November 2019

Software Release Date: November 2019



Legal Notices

Copyright Notice

© Copyright 2001-2019 Micro Focus or one of its affiliates

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

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

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

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

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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 7.2	6
What's New in This Release	6
ArcSight Command Center Enhancements	6
ArcSight Console Enhancements	7
Administration Enhancements	7
Integration Enhancements	8
Improved Concurrency of Deferred Rule Action	8
Script Timeouts are Configurable	8
Global Event IDs	9
Standard Content	9
Verifying the Downloaded Installation Software	10
Upgrade Support	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
Section 508 Compliance	13
Usage Notes	14
Post-Upgrade Steps	14
Keep These TCP Ports Open	14
Configuring a New Transformation Hub Destination	14
ArcSight Command Center	15
Scroll Bar Issues with Google Chrome and Apple Safari	15
Viewing Secure Operations Center Dashboard Using Edge Browser on Windows 10	15
ArcSight Console	16
ArcSight Console Dark Theme	16
Events from Transformation Hub	16
Using Windows 10	16
Oversized Pie Charts on Dashboards	17
Limit on Dashboards Being Viewed	17
Distributed Correlation Mode	17

Configuration Changes Require Restart of All Services	17
Active List Updates in Distributed Correlation	17
Services are not Started During an ESM Distributed Correlation Installation	18
Stop and Start All Services if a Major Service is Stopped	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
Using the Edge Browser	20
Oversized Event Graphs	21
Full Text Search	21
Resource Validation	21
ESM Peer Certification for Content Synchronization	22
ESM and Logger Connectivity	22
Actor Model Import Connector	22
Asset Model Import FlexConnector	23
Forwarding Connector	23
Running ArcSight Investigate Searches	23
Post Upgrade - Install ArcSight SocView and ClusterView Packages	29
Rule Recovery Timeout Possible During High EPS	29
Audit Events Now Generated by Creation or Deletion of Mark Similar Configurations	30
Reference to SmartConnectors Not Updated (Customer URI)	30
Silent Install Not Supported in Dark Theme	30
New Default Setting for Session List Entry Expiration Time	31
Deprecated - Optimize Data Feature for Active Lists	31
Unsupported Features in This Release	32
Resolved Issues	34
General	34
API Web Services	34
ArcSight Console	35
ArcSight Manager	36
CORR-Engine	37
Command Center	38

Connectors	38
Localization	38
Open Issues	39
Analytics	39
ArcSight Console	41
ArcSight Manager	45
CORR-Engine	49
Command Center	50
Connector Management	54
Connectors	54
Installation and Upgrade	54
Localization	56
Pattern Discovery	57
Reports	57
Send Documentation Feedback	58

Welcome to ESM 7.2

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 7.2.

Updated guides for ESM 7.2 are available from the [Micro Focus Community website](#).

ArcSight Command Center Enhancements

New features and enhancements in ArcSight Command Center include:

- You can view active lists that you created in the ArcSight Console from ArcSight Command Center.
- The MITRE Activity dashboard allows you to view tactic and technique information about any activity that matches the MITRE ATT&CK™ matrix in order to identify security gaps.
- ESM generates a 45-day moving median EPS (MMEPS) report that tracks the history of average EPS, average EPS per day, MMEPS, and the entitled EPS limit so that you can identify whether you are in danger of being out of compliance with the license agreement.

You are considered to be in compliance with the license agreement as long as the MMEPS values remain at or below the purchased license capacity. You are considered to be in violation of the license agreement if three or more consecutive MMEPS values exceed the purchased license capacity.

- When viewing event information for an active channel, you can double-click an event in the **Event List** to view event details. When viewing event details, you can click the

pushpin icon to dock the Event Details dialog in the channel viewer grid.

- Non-admin users can now view the Security Operation Center (SOC) Dashboard, with the following permissions:
 - /All Data Monitors/ArcSight Administration/ESM/Event Analysis Overview/Event Overview/
 - /All Data Monitors/ArcSight Administration/ESM/System Health/Events/Event Throughput/
 - /All Data Monitors/ArcSight Foundation/ArcSight SocView/
 - /All Filters/ArcSight Foundation/ArcSight SocView/
 - /All Filters/ArcSight System/Event Types/
 - /All Queries/ArcSight Foundation/ArcSight SocView/
 - /All Query Viewers/ArcSight Foundation/ArcSight SocView/

For more information about these features, see the [ArcSight Command Center User's Guide](#).

ArcSight Console Enhancements

New features in the ArcSight Console include:

- When configuring ESM to integrate with the ServiceNow® IT Service Management (ITSM) application, you can modify the export form as follows:
 - Customize field names
 - Add or hide fields
 - Set required fields
 - Map values from ESM cases to ServiceNow® ITSM ticket fields
- A new aggregate function, GROUP_CONCAT, allows you to create a comma-separated list of aggregated items.
- A new property, rules.batch.query.timeout, allows you to set the maximum timeout (in seconds) when querying historical events for scheduled rules. The default is 600 seconds (10 minutes). If the query takes longer than the specified value, the query times out and its status is Timeout. To see the status, go to **Scheduled Jobs** > **Scheduled Runs**.

If the query times out twice, the scheduled rules are disabled and the task will not run again. To run the task again, delete the job and reconfigure the scheduled rules.

For more information about these features, see the [ArcSight Console User's Guide](#).

Administration Enhancements

The following changes apply to ESM administration:

- This release upgrades MySQL from version 5.1.54 to version 5.7.21. When upgrading, be aware that you must manually port any changes made to the 5.1.54 configuration file to the 5.7.21 configuration file.
- This release includes a new troubleshooting utility, `tdswlogs.v7.sh`. If you run into an issue, run this utility before contacting Support. The utility gathers logs and system information Support needs to help you diagnose the problem.

To run the utility, use one of the following methods:

- `sudo /opt/arcsight/manager/bin/tdswlogs.v7.sh` (recommended)
- Run as arcsight user

The utility takes about five minutes to complete. You will be asked to provide the MySQL database password during the process.

- You can now add or remove instances of information repository (repo), distributed cache (dcache), correlator, and aggregator services on existing cluster nodes without having to restart ESM.

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

- ESM is packaged with a new Java Development Kit, OpenJDK version 8u212. If you have a need to use a JDK other than the packaged OpenJDK, ESM allows you to do so. Your JDK version must be equivalent to or higher than the packaged OpenJDK version.

Note: ESM 7.2 does not support JDK 9 or later.

For more information about using your own JDK, contact [Customer Support](#).

Integration Enhancements

The following enhancements apply to ESM integration.

Improved Concurrency of Deferred Rule Action

In versions prior to 7.2, one thread processed all deferred rule actions. Version 7.2 introduces a new `rules.action.threads` property, which allows you to specify the number of threads to process rule actions. The default setting is 2.

Script Timeouts are Configurable

In versions prior to 7.2, a script timed out after 30 seconds. Version 7.2 introduces a new property that allows you to define the timeout limit. The default setting is 60 seconds.

In the `server.properties` file, the `action.command-executor.max.timeout` property is set to a default value of 60 seconds:

```
action.command-executor.max.timeout=60
```


If you think the script might take more than two minutes to finish, you can increase the value accordingly. For example:

```
action.command-executor.max.timeout=150
```

Global Event IDs

ESM 7.2 adds Global Event IDs to events. Global event IDs uniquely identify events across the ArcSight product suite and specify the origin of events that appear in multiple components.

Standard Content

New features for ESM Standard Content include:

- Security Threat Monitoring package

This package is included in the ArcSight Foundation category and includes the following use cases:

- Application Monitoring detects code injections, cross-site scripting from other devices, SQL injections, and multiple access attempts to malicious domains from the same source address.
- Entity Monitoring detects brute force attacks and unsuccessful login attempts and monitors account activity.
- Host Monitoring detects pass the hash attempts and monitors cleared log and service down events.
- Malware Monitoring detects malware infections.
- Network Monitoring gathers information from intrusion detection systems and monitors denial of service activities, exploit attempts, and privilege escalation attempts.
- Perimeter Monitoring detects clear text protocols that cross a perimeter, egress communications to suspicious countries, suspicious DNS communications, and egress communications to restricted services.
- Vulnerability Monitoring detects suspicious activity on vulnerable assets.

- Threat Intelligence Platform package

This package is included in the ArcSight Foundation category and monitors the following:

- Botnet activity
- Dangerous browsing
- Assets found in reputation lists
- Phishing attempts

- Presence of ransomware
- Suspicious DNS queries
- Suspicious emails

Note: The Threat Intelligence Platform package requires ArcSight MISP Model Import Connector version 7.14 or higher.

- Model Import Connector (MIC) for MISP CIRCL

This connector allows the Threat Intelligence Platform package to use the MISP CIRCL threat intelligence feed. For more information about the connector, see the connector Configuration Guide on the [ArcSight Connectors Documentation](#) page.

- MITRE Activity dashboard

This dashboard monitors activity that matches the MITRE ATT&CK™ matrix. The content includes rules that are tagged with the MITRE Technique ID.

- Data Monitor Status dashboard

This dashboard provides information about the top data monitors based on event count, event processing time, distributed cache synchronization count, and distributed cache synchronization time so that you can identify data monitors that place a high load on the system.

- Improvement to Content Management content

When there is a content package failure, ESM sends an alert to the Content Management group. You must configure a notification destination in the ArcSight Console.

For more information about configuring notification destinations, see the [ArcSight Console User's Guide](#).

For more information about these features, see the [ESM Standard Content Guide](#).

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

The following upgrade paths are supported for software ESM (in both compact mode and distributed correlation mode) and ESM on an appliance:

- If you plan to upgrade from ESM 6.11, first upgrade to ESM 7.0 Patch 1, then upgrade to ESM 7.2.
- For ESM 7.0, first apply ESM 7.0 Patch 2, then upgrade to ESM 7.2.
- For ESM 7.0 Patch 1 and Patch 2, you can upgrade directly to ESM 7.2.

For details on supported platforms, refer to the [ESM Support Matrix](#).

Geographical Information Update

This version of ESM includes an update to the geographical information used in graphic displays. The version is GeoIP-532_20190901.

Vulnerability Updates

This release includes recent vulnerability mappings from the September 2019 Context Update.

Device	Vulnerability Updates
Snort / Sourcefire SEU 2983	Faultline, Bugtraq, CVE, X-Force, Nessus, CERT
Enterasys Dragon IDS 20190911	CVE
Cisco Secure IDS S1032	CVE
Juniper IDP update 3202	Faultline, Bugtraq, CVE, X-Force, Nessus
TippingPoint UnityOne DV9327	MSSB
McAfee HIPS 7.0/8.0 content version 9528	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 [ArcSight Command Center User's Guide](#).

Supported Platforms

See the [ESM Support Matrix](#) document for details on ESM 7.2 platform and browser support.

Supported Languages

These languages are supported by ESM:

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

Support for ActivClient Issues

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

Post-Upgrade Steps

ESM 7.2 contains performance enhancements in distributed correlation that significantly increase the throughput of correlators. After you upgrade to ESM 7.2, you might be able to decrease the number of correlators on each cluster node, resulting in improved resource usage. For example, in previous releases, the “Large Configuration” recommended two correlators per node. It now recommends one per node. For more information, see the [ESM Installation Guide](#).

Keep These TCP Ports Open

Before you install software ESM, open the ports that are listed in this section if they are not already open. Ensure that no other processes are using these ports.

Open the following ports for external incoming connections:

- 8443/TCP - SmartConnectors and consoles
- 9000/TCP - Peering
- 5404/UDP - High Availability module
- 5405/UDP - High Availability module
- 7789/TCP - High Availability module
- 22/TCP - SSH login

Open the following TCP ports for inter-component communication:

1976, 2812, 3306, 5555, 6005, 6009, 7777, 7778, 7779, 7780, 8005, 8009, 8080, 8088, 8089, 8666, 8765, 8766, 8808, 8880, 8881, 8888, 8889, 9000, 9090, 9095, 9123, 9124, 9999, 28001, 45450

Some ports are used in a distributed correlation environment. The information repository uses ports 3179, 3180, 3181, and 3182. Also, there are port ranges reserved for use by cluster services. Other processes must not use ports in these reserved ranges. For more information about reserved port ranges, see the [ESM Administrator's Guide](#).

Configuring a New Transformation Hub Destination

When you are configuring a new Transformation Hub destination for the Forwarding Connector, there is a new parameter called **For ESM Topic, The ESM version**, where you specify the correct version of the source ESM Manager.

If 7.2.x is not available in the list, follow these steps:

1. Edit the connector `../current/user/agent/agent.properties` file.
2. Add `esm_version_7_2_for_th_dest=true` and save the file.
3. Stop and restart the Configuration wizard.
4. (Conditional) If the connector is running, you must stop it and restart it for the new property to take effect.

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

ArcSight Console Dark Theme

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

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

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

For the above, use the daylight theme instead.

Events from 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 7.2 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 may run out of Java memory if you are viewing dashboards above the limit, which is 15 dashboards. For Windows 10 in particular, limit from 7 to 10 dashboards. If you must view dashboards over the limit, try switching to classic charts in the Console's Preferences menu, under Global Options.

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

If you want to view more dashboards than the limit:

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

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

Follow instructions in the topic, "Managing and Changing Properties File Settings" in the [ESM Administrator's Guide](#).

Distributed Correlation Mode

Configuration Changes Require Restart of All Services

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

Active List Updates in Distributed Correlation

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

Similarly, if you have a pair of rules: the first rule populates a list, and the second rule depends on data being on that list, and both rules are expected to operate on the same

event, the list may not be updated by the first rule in time for the second rule to trigger as expected.

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

Services are not Started During an ESM Distributed Correlation Installation

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

Stop and Start All Services if a Major Service is Stopped

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

Major services include:

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

Otherwise you may see reduction in event processing speed.

Major services typically stop in these cases:

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

If the ESM Console or 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. Disk space is required for storing events for full text search, approximately 40 to 50% more than if full text search were disabled.

The feature is controlled by the property:

```
fulltext.search.enabled
```

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

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

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

Resource Validation

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

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

For more information on supported IP address range formats, refer to "IP Address Ranges" topic in the [ArcSight Console User's Guide](#).

ESM Peer Certification for Content Synchronization

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

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

For more information about content management, refer to the following:

- "Creating or Editing Packages" and "Supported Package Resources for Content Synchronization" in the [ArcSight Console User's Guide](#)
- "Content Management" and "Configuring Peers" in the [ArcSight Command Center User's Guide](#)

ESM and Logger Connectivity

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

Actor Model Import Connector

The Actor Model Import Connector for Microsoft Active Directory allows you to develop a model import connector to import actor model data. This connector can be configured in a dual stack or pure IPv6 environment. Refer to the *Actor Model Import Connector for Microsoft Active Directory Configuration Guide*. The Actor Model Import Connector for Microsoft Active Directory to install for ESM 7.2 is version 7.13.0.8235.1.

See the [ESM Support Matrix](#) for details on ESM 7.2 supported platforms.

Caution: Install and use the Actor Model Import Connector for Microsoft Active Directory that is provided with the ESM 7.2 release. That is the version of the connector that is tested and certified to work with ESM 7.2. Do not use previously-supplied versions of the Actor Model Import Connector for Microsoft Active Directory with ESM 7.2.

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. Refer to the *Asset Model Import FlexConnector Developer's Guide*. The Asset Model Import FlexConnector to install for ESM 7.2 is version 7.13.0.8237.1.

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

See the [ESM Support Matrix](#) document available on the Protect 724 site for details on 7.2 supported platforms.

Caution: Install and use the Asset Model Import FlexConnector that is provided with the ESM 7.2 release. That is the version of the connector that is tested and certified to work with ESM 7.2. Do not use previously-supplied versions of the Asset Model Import FlexConnector with ESM 7.2.

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 7.2.

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

See the [ESM Support Matrix](#) document for Forwarding Connector version on ESM 7.2.

Running ArcSight Investigate Searches

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

General search instructions

- If the search query is on an empty field that is an Integer or Number data type, the query should be of the format
`<FieldName> = '',Null`
For example
`sourcePort = '',Null`
- When launching ArcSight Investigate integration command, use the default port 443, unless the port is configured differently.
- If you are a non-administrator user in ArcSight Investigate, you may not be authorized to view certain field values. If you are searching such fields, you will see an Unknown column error. If you are a non-administrator user in ArcSight Investigate and you are not authorized to execute a search query, you will see an error that says you are not authorized.
- If you open multiple browser sessions for ArcSight Investigate searches, you will eventually observe slowness in browser response. The threshold is from 5 to 6 sessions. If you open more than that, you should close some browsers.
- ArcSight Investigate search results are case-insensitive. That is by design.

Searching for Attacker Address and Target Address Based on Originator

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

Assume these values for the following fields:

Attacker Address = 1.1.1.1

Target Address = 2.2.2.2

Source Address = 1.1.1.1

Destination Address = 2.2.2.2

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

Searching for empty fields

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

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

Permission for searches

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

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

Search error due to complex characters

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

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

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

and it got inserted into Investigate as:

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

then truncate it after the single quote:

```
Name= 'my_esm_value'
```

and replace = with starts with:

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

Supported ESM fields

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

List of ESM Fields Supported in ArcSight Investigate Searches

ESM Fieldname
agentAddress
agentDnsDomain
agentHostName
agentMacAddress
agentTranslatedAddress
agentType
agentVersion
applicationProtocol
bytesIn
bytesOut
categoryDeviceGroup
categoryDeviceType
categoryObject
categoryOutcome
categorySignificance
categoryTechnique
destinationAddress
destinationDnsDomain
destinationHostName
destinationMacAddress
destinationNtDomain
destinationPort
destinationProcessId
destinationProcessName
destinationServiceName
destinationTranslatedAddress
destinationTranslatedPort
destinationUserId
destinationUserName
destinationUserPrivileges
deviceAction

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
deviceAddress
deviceCustomFloatingPoint1
deviceCustomFloatingPoint2
deviceCustomFloatingPoint3
deviceCustomFloatingPoint4
deviceCustomIPv6Address1
deviceCustomIPv6Address2
deviceCustomIPv6Address3
deviceCustomIPv6Address4
deviceCustomNumber1
deviceCustomNumber2
deviceCustomNumber3
deviceCustomString1
deviceCustomString2
deviceCustomString3
deviceCustomString4
deviceCustomString5
deviceCustomString6
deviceDnsDomain
deviceDomain
deviceEventCategory
deviceEventClassId
deviceExternalId
deviceFacility
deviceHostName
deviceInboundInterface
deviceMacAddress
deviceNtDomain
deviceOutboundInterface
deviceProcessId
deviceProcessName

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
deviceProduct
deviceSeverity
deviceTranslatedAddress
deviceVendor
deviceVersion
eventOutcome
fileHash
fileId
fileName
filePath
filePermission
fileSize
fileType
flexNumber1
flexNumber2
flexString1
flexString2
name
oldFileHash
oldFileId
oldFileName
oldFilePath
oldFilePermission
oldFileSize
oldFileType
requestClientApplication
requestMethod
requestUrl
sourceAddress
sourceDnsDomain
sourceHostName

List of ESM Fields Supported in ArcSight Investigate Searches, continued

ESM Fieldname
sourceMacAddress
sourceNtDomain
sourcePort
sourceProcessId
sourceProcessName
sourceServiceName
sourceTranslatedAddress
sourceTranslatedPort
sourceUserId
sourceUserName
sourceUserPrivileges
transportProtocol

Post Upgrade - Install ArcSight SocView and ClusterView Packages

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

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

Rule Recovery Timeout Possible During High EPS

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

Note that the timeout can still occur after increase the value of the `rules.recovery.time-limit` property, due to overall system load, high EPS, or a large

number of rules. Also, the Manager will take longer to start up if the recovery time limit is increased.

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

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 Not Supported in Dark Theme

When in silent mode, the ESM Console installer does not trigger the `consolesetup` step at the end of the install. As a result, a default `console.properties` file is not generated during the installation. Dark theme requires access to this properties file.

Workaround:

1. Run the `consolesetup` wizard in first 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 ESM Console installation.

3. Now use the dark theme.

Syntax:

Note that 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)

See the [ESM Administrator's Guide](#), Appendix A: Administrative Commands for details on commands and parameters.

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**. See List Authoring, Creating or Editing a Session List, in the *ArcSight Console User Guide*, for details.

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
- Large Partially Cached Active Lists are not supported in distributed mode.

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 7.2:

- 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](#) 34
- [API Web Services](#) 34
- [ArcSight Console](#) 35
- [ArcSight Manager](#) 36
- [CORR-Engine](#) 37
- [Command Center](#) 38
- [Connectors](#) 38
- [Localization](#) 38

General

Issue	Description
NGS-27938	The <code>arcsight_services</code> status property might occasionally report that a dcache instance is unavailable even though it is running properly. You can safely ignore this warning.
NGS-28935	This release resolves an issue where the <code>stop all</code> command does not stop the <code>execprocsvc</code> service.

API Web Services

Issue	Description
NGS-30033	This release resolves an issue where using the ESM API to check aggregated event data always returns an <code>aggregatedEventCount</code> value of 0.
NGS-30316	This release resolves an issue where using the ESM API to check event data returns a <code>baseEventCount</code> value of 0, even though the event type is BASE.
NGS-29627	This release resolves an issue where the case event annotations audit history shows any call to the Rest API CaseService update method removing events and then adding them back to the case.

ArcSight Console

Issue	Description
NGS-30516	<p>By default, chart-style views (Pie and Bar charts) are limited to a maximum of 20 results. Table views can retrieve up to 10,000 rows of data, so it is possible the results in chart views and table views for the same query viewer might not match.</p> <p>Workaround: To allow for more results in a chart view, select the Use classic charts option in Global Preferences. By default, classic charts display a maximum of 99 results. To increase that number, add the following property to the <code>console.properties</code> file and specify the desired value:</p> <pre>queryviewer.max.dashboard.chart.rows</pre> <p>For more information about editing the <code>console.properties</code> file, see the ESM Administrator's Guide.</p>
NGS-29560	<p>This release resolves an issue where the color change option was incorrectly available for D3 charts.</p>
NGS-28602	<p>This release resolves an issue with maps. The global option that allows you to display a world map with country borders, a world map without country borders, or a custom map in the background is now enabled by default.</p>
NGS-28075	<p>When you change the global font size for the Console via Edit > Preferences > Global Options, some dashboard graphs do not reflect the font change. This is by design. Only classic dashboard graphs reflect global font options.</p>
NGS-29243	<p>This release resolves an issue where you could not resize the event tree in the Event Inspector panel.</p>
NGS-28547	<p>This release resolves an issue where ESM did not display all of the available integration commands when you right-clicked a row in the event grid and selected Integration Commands.</p>
NGS-25203	<p>This release resolves an issue where ESM did not save changes to the background color for some data monitors on dashboards.</p>
NGS-24703	<p>This release resolves an issue where the Save As button was not activated when you tried to create a new field set from the Event Inspector panel.</p>
NGS-18468	<p>This release resolves an issue where you could not view the list of available commands from all CounterACT connectors when you added new integration commands. You could only view the available commands for the first CounterACT connector that was started.</p>

ArcSight Manager

Issue	Description
NGS-29703	<p>The <code>certadmin</code> command does not work in interactive mode on the following operating systems:</p> <ul style="list-style-type: none">• RHEL 6.10• CentOS 6.10 <p>You can run the <code>certadmin</code> command in CLI mode:</p> <pre>/arcsight certadmin</pre>
NGS-25518	<p>This release resolves an issue where connections from ESM services to Transformation Hub and to Message Bus can fail intermittently from various causes, including networking issues, operating system resource contention, Kafka and ZooKeeper processing loads, or ESM service instance processing.</p>
NGS-27729	<p>This release resolves an issue where installing ESM in distributed mode on a High Availability system and then performing a failover causes <code>/usr/lib/arcsight/highavail/bin/arcsight firstBootWizard</code> to stop working.</p>
NGS-26898	<p>This release resolves an issue in ESM distributed mode, where network instability might cause the following issues:</p> <ul style="list-style-type: none">• The message bus does not list topics.• Correlators and aggregators do not consume any events.
NGS-27964	<p>This release resolves an issue where, after an HA failover, the command <code>/usr/lib/arcsight/highavail/bin/arcsight_cluster status</code> indicates a failure on ESM.</p>
NGS-26393	<p>This release resolves an issue where <code>zoneUpdate.log</code> is written to the wrong location.</p>
NGS-28789	<p>This release resolves an issue where a timeout issue in the SNMP library for SNMP version 3 might cause events per second to drop.</p>

CORR-Engine

Issue	Description
NGS-28860	<p>In rare cases, if the network is down when you activate or deactivate a rule in a correlator or an aggregator, ESM might set the resource status to <code>Invalid</code>.</p> <p>Workaround: Restart the cluster services and then run the <code>resvalidate</code> command to resolve the issue.</p> <p>For more information about the <code>resvalidate</code> command, see the ESM Administrator's Guide.</p>
NGS-29020	<p>When you create a rule for correlated event count, the number of returned base events is always 100.</p> <p>Workaround: To change the number of base events in correlated events, modify the following properties:</p> <ul style="list-style-type: none">• <code>rules.max.rulechain.size</code> (default is 100)• <code>rules.max.unique.valuechain.size</code> (default is 100) <p>If you are using compact mode, make these changes in the <code>server.properties</code> file.</p> <p>If you are using distributed mode, make these changes in the <code>aggregator.properties</code> file.</p>
NGS-26989	<p>This release resolves an issue in distributed mode, where removing an entry from an Active List generates a Success audit event, even if the specified entry does not exist.</p>
NGS-29395	<p>This release resolves an issue where using the Console to modify a core attribute on an actor does not delete the original value from the Base Attributes table.</p>
NGS-29821	<p>If a rule creates a large number of cases (500,000 or more), the persistor and embedded dcache might run out of memory.</p> <p>Workaround: Use the Manager Configuration Wizard to increase the Java heap memory size.</p> <p>For more information about using the wizard, see the ESM Administrator's Guide.</p>
NGS-28734	<p>This releases resolves an issue where expensive rules cause ESM to run slowly in production. New parameters in the <code>server.properties</code> file allow ESM to automatically deactivate rules with high partial matches and then reactivate them later.</p> <p>The default values are as follows:</p> <pre># join rules partial match/minute rules.max.partial.matches=20000 # filter rules partial match/minute rules.filter.max.matches=50000</pre>

Command Center

Issue	Description
NGS-29490	<p>When using the Edge browser to access Command Center, if you create a new channel and attempt to configure a field set, the Edge browser does not display the field names. To avoid this issue, use one of the following browsers:</p> <ul style="list-style-type: none">• Internet Explorer• FireFox• Chrome• Safari
NGS-27960	<p>This release resolves an issue where non-admin users cannot access Saved Searches/Search/Event Search pages in Command Center.</p>
NGS-28788	<p>This release resolves an issue where you might see an unknown error when you attempt to log in to the Command Center.</p>
NGS-28461	<p>This release resolves an issue where reducing the retention period for a storage group by more than 10 days resulted in severe performance issues. With this release, ESM does not allow you to reduce the retention period by more than five days per day.</p>

Connectors

Issue	Description
NGS-29953	<p>If you configure ESM to directly consume events from Event Broker (in ESM version 7.1 or older) or Transformation Hub (in ESM version 7.2), connector versions prior to 7.11.0.8139.0 do not populate the Global Event ID on binary events. To ensure the Global Event ID is correctly populated, use a connector version 7.11.0.8139.0 or later with ESM version 7.2.</p>
NGS-30528	<p>If you install the Forwarding Connector on RHEL 7.7, the installation process displays an unsupported platform message. You can safely ignore this message and continue with the installation process.</p>
NGS-26739	<p>This release removes the HPE Operations Manager and Operations Manager options from the Forwarding Connector setup wizard.</p>

Localization

Issue	Description
NGS-26414	<p>This release resolves an issue in localized environments, where some counts in the Security Operation Center view are not updated properly.</p>

Open Issues

This release contains the following open issues.

• Analytics	39
• ArcSight Console	41
• ArcSight Manager	45
• CORR-Engine	49
• Command Center	50
• Connector Management	54
• Connectors	54
• Installation and Upgrade	54
• Localization	56
• Pattern Discovery	57
• Reports	57

Analytics

Issue	Description
ESM-49283	<p>When defining filters, for a hostname to be properly interpreted from the Request URL, the host name needs to be enclosed either within // (double slash) and / (single slash); or within // (double slash) and : (colon). For example:</p> <pre>"https://hostname.example.com:8443" class="external-link" rel="nofollow">https://hostname.example.com:8443</pre> <p>Such an event is retrieved correctly with the Request Url Host Is Not Null filter. Do not use a filter with a condition that says Request Url Host != Null because != makes the filter invalid.</p>
ESM-39405	<p>If you create a report whose name contains Chinese characters, and then send the report as a PDF attachment, the received email does not display the attachment's name correctly. The content of the report is correct; only the email attachment field that displays the name of the attachment is affected.</p>
NGS-28062	<p>When a standard rule is replayed, active list related actions are triggered. Other types of rule actions are not triggered.</p>
NGS-28027	<p>In a distributed cluster, after starting up the cluster, while loading large active lists, an error (ConcurrentModificationException) can occur in the logs. Add the following property in server.properties: activelist.parallel.load.threshold=false and restart the cluster.</p>

Issue	Description
NGS-27914	<p>Reports which output the URL filename will no longer suppress the leading slash (/). This will match the ArcSight Console output.</p> <p>For example, the filename portion of the URL "http://www.example.com/index.html" class="external-link" rel="nofollow">http://www.example.com/index.html is /index.html. The filename portion of the URL "http://www.example.com/" class="external-link" rel="nofollow">http://www.example.com/ is / and for the URL "http://www.example.com" class="external-link" rel="nofollow">http://www.example.com the filename is NULL.</p>
NGS-27096	An error is reported during time based eviction for an Active List that has optimize data selected and contains no defined keys. In this case, uncheck optimize data. Optimize data feature is deprecated and may be removed in a future release.
NGS-27045	HTML reports embedded in email were not displaying Unicode Standard characters appropriately.
NGS-26720	If you move a rule group from the Real-time Rules folder to another folder (and delete from Real-time Rules), and then you schedule that new rule group, when rules in this new group are triggered, you will notice that the generated correlation events show the wrong information: the URI is still remembered as the old Real-time Rules folder instead of the new URI.
NGS-26663	On distributed ESM, when the cluster is installed or started up, the Event Throughput dashboard takes some time to display the graph on the top.
NGS-26380	In the Last State data monitor, the Override Status and Remove Entry options are not working correctly.
NGS-25756	<p>An ESM system that uses Partially Cached Active Lists (PCALs) runs out of memory in distributed mode.</p> <p>Workaround:</p> <p>If you have PCALs in your content and need to use them in distributed mode, you can:</p> <ol style="list-style-type: none"> 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.
NGS-24957	The GetSessionData function that uses sessionlist with multiple keys may show an incorrect result.
NGS-7181	Queries are very slow when they have a combination of aggregation, groupby, orderby, and a condition on a large active list or session list.

ArcSight Console

Issue	Description
NGS-29487	<p>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.</p> <p>Workaround: Change the ESM Console font to one that does not demonstrate this behavior, such as Arial.</p> <p>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.</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>
NGS-30606	<p>To categorize an event, you must add the following columns to the event:</p> <ul style="list-style-type: none">• Device Event Class ID• Device Vendor• Device Product
NGS-30648	<p>When using the provided ServiceNow® Security Incident Response schema, a URL mismatch prevents the correct result from displaying when you click over the ServiceNow ITSM ID field in the case editor.</p> <p>Workaround:</p> <pre>{instance_url}/nav_to.do?uri=%2Fsn_si_incident.do%3Fsys_id%3D{sys_id}</pre> <p>Replace {instance_url} with the ServiceNow instance URL.</p> <p>Replace {sys_id} with the ServiceNow ITSM ID field value.</p> <p>Launch it in a browser.</p>
NGS-30832	<p>If you use the Windows operating system, ensure the scaling percentage is 100% (the default). If you increase the percentage, the ServiceNow login window might experience display issues.</p>
NGS-30656	<p>If you add more fields to the ServiceNow configuration template, the information icon in the upper right part of the ServiceNow ITSM window incorrectly overlaps the scroll bar. This occurs in both Linux and Windows operating systems. This is a visual issue only and does not affect functionality.</p>
NGS-27091	<p>Drill down from stacked bar charts doesn't work as expected.</p>

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

Issue	Description
NGS-23214	<p>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.</p> <p>ssl.keystore.password</p> <p>ssl.keystore.password.encrypted</p> <p>and likewise for ssl.truststore.password. 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-23207	The ArcSight Console will not work in FIPS mode with SSL and ca-signed if installed on Windows 7 Professional.
NGS-23198	The ArcSight Console does not check Certificate Revocation Lists to determine if a CA-signed manager certificate has been revoked by the Certificate Authority.
NGS-22659	<p>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.</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 InSubnet condition strictly enforces the use of the wildcard asterisk "*". For example, a filter like 10.10. is invalid, and 10.10.*.* is valid.</p> <p>Old content that uses inSubnet 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>
NGS-17864	<p>On some systems, the Show Event Details option on an eventID in a Query viewer does not show event details like EventID, Start time, ManagerReceipt Time.</p> <p>Workaround:</p> <p>Open the event in an Active channel first and then view the event using Query viewer using Show Event Details. In some cases, restarting of the ArcSight Console also solves the issue.</p>
NGS-17863	<p>In an MSSP environment, under certain circumstances a tenant may notice event(s) which should match the user group's Access Control List settings for Events, but these events will be stuck in Loading Event... state in the Active Channel.</p> <p>Workaround:</p> <p>Add the Customer Name column to the Active Channel and the events will load successfully.</p>

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

ArcSight Manager

Issue	Description
NGS-30346	<p>Dynamic Active channels might stop showing the recent events, if a user edits the channel while it is active or open.</p> <p>Workaround: You can refresh the Active Channel by stopping it and then restarting it.</p>
NGS-29788	<p>Using five-digit Unicode characters in the Destination user name field causes the following:</p> <ul style="list-style-type: none">• 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 . . . <p>Workaround: Do not use five-digit Unicode characters in the Destination user name field.</p>
NGS-30718	<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-30888	<p>A limitation with the .lic file extension requires the file name to be arcsight.lic.</p> <p>Workaround: If you plan to add licenses with the .lic extension to the ESM product, ensure the file name is arcsight.lic prior to importing it into ESM. Note that there is no such naming restriction for other license file extensions.</p>
ESM-51070	<p>Connector statistics file to be processed correctly on Managers other than the primary destination Manager. Related content such as the rule Connector Discovered or Updated will be impacted.</p>
ESM-48068	<p>After asset auto-creation, if the Manager does not restart and the server.std.log shows a message about a "conflicting device with the same hostname/ipaddress <resource id>", then two assets have the same resourceid. This conflict has to be resolved before starting the Manager.</p>
ESM-47625	<p>When exporting a case or other resource, the Creation Time is changed to the time of the export.</p>
ESM-46699	<p>Updating a Trend by refreshing it works only once. Subsequently, the trend does not refresh with updated information.</p>
NGS-27487	<p>Sometimes, installation of Activate package bundles could fail on FIPS-mode ESM installations. If that happens, repeat the same command to install Activate bundle.</p>
NGS-27111	<p>Similar to the previous versions, ESM 7.0 Patch 1 expects ET in a local time zone when receiving event data from Connectors and TH. However, CTH pods use UTC time for ET when submitting events to TH. When consuming such events, ESM may not show them in the sliding Active Channels based on ET as the ET time of those events is out of the Active Channels time intervals. Switching Active Channels to MRT instead of ET helps.</p>

Issue	Description
NGS-26917	When a system is first setup or installed, the audit events are generated as soon as Manager is started. In distributed mode, due to the time it takes for all the components to come up, the audit events not displayed by the dashboard displaying the status. When Manager is restarted, or a failover is done, audit events are processed by the distributed cluster and the correct status is displayed in the dashboard.
NGS-26846	In ESM distributed mode, when lags on topics start growing, look at Partial Match data monitor to find high Partial Match rules and tune them or disable them.
NGS-26237	In ESM distributed mode, System Monitor and System Monitor Attribute data monitors display information from the persistor node. They do not have access to information from nodes running correlators or aggregators.
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. 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-1.0.0.jar -J-Djava.security.egd="file:/dev/urandom" class="external-link" rel="nofollow">file:/dev/urandom -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388"</pre> <ol style="list-style-type: none"> 3. Import the source Manager certificate into Forwarding Connector truststore (SmartConnector User Guide) 4. Runagent setup 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>
NGS-23341	<p>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.</p>
NGS-14860	<p>Multiple failure messages are generated in logger_web.out.log when stopping arcsight services. These messages can be ignored.</p>
NGS-14437	<p>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.</p>

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>
NGS-12105	<p>The annotation stage name default value (Queued) is displayed in the Active Channel, but this value name does not display in the query viewer or in a report. Other non-default values (for example, Initial or Follow-Up) are displayed correctly in the query viewer or report.</p>
NGS-9734	<p>In Russian, when a notification is sent with an email attachment, the filename and email subject lines contain garbled characters.</p>
NGS-9109	<p>An incorrect OID is provided for ArcSight SNMP Trap. A third party package causes the OID for the trap to be translated incorrectly.</p>
NGS-8926	<p>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.</p> <p>However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database.</p> <p>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.</p>
NGS-3825	<p>If the field size of an event exceeds 32 KB, that event does not persist.</p>
NGS-1937	<p>The archive tool occasionally fails to import entries into an active list due to transient errors. In such situations, you might not see errors, but the list is not populated.</p> <p>Workaround: Re-import the same package.</p>
NGS-172	<p>Base events are not automatically annotated after rules trigger.</p> <p>Workaround: Set logger.base-event-annotation.enabled=true in server.properties.</p>

CORR-Engine

Issue	Description
NGS-29732	In distributed mode, when a user deletes a list that a rule references, the rule is disabled but continues to fire.
NGS-14477	Space-based retention cleans up same day data, but even after increasing the space, the system does not recognize that the space has been increased until midnight.
NGS-14041	Database queries using the UPPER or LOWER built-in string functions in the Russian locale return incorrect results when filtering events. This applies especially to queries using the Ignore Case option, which rely on the UPPER function.
NGS-4837	<p>With certain long running queries, a deadlock might occur in the JDBC driver. You might notice decreased throughput. If you suspect this deadlock, request a thread dump through <code>manage.jsp</code> and determine if the end of the dump specifically indicates deadlock.</p> <p>Workaround: If a deadlock does occur and is an issue for you, restart the Manager to resume normal operations.</p>
NGS-4790	<p>To resolve a "database full" condition, free up space in the ArcSight System Storage Space.</p> <p>Workaround:</p> <ol style="list-style-type: none">1. Delete any unused trends. Deleting the trend frees up any data in the table associated with this trend.2. Reduce the retention period of specific trends. By default, trends retain 180 days of data. You can set this retention time on a per-trend basis. Any data falling outside this range will be removed the next time the trend runs.3. Examine the contents of your session lists. Data is not usually removed from session lists. Running "<code>bin/arc sight dropSLPartitions -h</code>" will explain how to remove data older than a specified time. Note that this will apply to ALL session lists on your system.

Command Center

Issue	Description
NGS-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-29743	<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>
NGS-30647	<p>If license usage data is corrupted, the 45-median report will state, "No results were returned from the server."</p>
NGS-27190	<p>The range for finished cases is defined by <code>socmetrics.finished.cases.lower.end</code> and <code>socmetrics.finished.cases.higher.end</code> in <code>server.properties</code>. Note that, when the value for finished cases is in the defined range, this value displays in gray, indicating it is in range. When the value is less than the defined range, it is displayed in red; when the value is greater than the range, it is displayed in blue.</p>
NGS-27159	<p>You cannot drill down from Geo Map Datamonitor in the Microsoft Internet Explorer and Microsoft Edge browsers. Use Firefox, Chrome, or Safari.</p>
NGS-26382	<p>When a case is expanded in the SOC View Dashboard metrics grid view, full history may not be displayed.</p> <p>Workaround:</p> <p>In this situations, view the history in the Cases editor by clicking the case.</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:</p> <p>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 User's Guide states that FIPS Suite B Mode is not supported for peering or content management. The Administration->Content Management and Administration->Peers menu items are disabled if the server is running in FIPS Suite B mode.</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 Java Script unresponsive error.</p> <p>Workaround:</p> <p>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:</p> <p>Refresh the page (press F5).</p>
NGS-20280	The WHERE operator is not supported in user-defined fields.
NGS-19267	You cannot restrict access to cases by user in the ArcSight Command Center.
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:</p> <p>Stop the Manager, delete unused notifications such as undeliverable or old pending notifications, and start the Manager.</p>
NGS-14900	There is a rare case that may cause confusion in channel event data visualization screen, if the event interval is less than 1 minute apart. The depending charting library, d3.js, is not able to handle this minute rounding case.
NGS-13926	<p>The stages available in the ArcSight Console Stage drop-down list do not always display in the ArcSight Command Center Active Channel.</p> <p>The stage Follow-Up" is available in the ArcSight Console Annotation Stage drop-down list, but does not display in the Annotation Stage drop-down list in ArcSight Command Center - Active Channels.</p>
NGS-8530	<p>In the ArcSight Command Center event search feature, some expected fields are missing from exported search results.</p> <p>For example, if you search for events, click Export Results, and check All Fields in the Export Options page, then click Export and download the exported results, then only some basic fields are listed, such as endTime, Name, sourceAddress.</p> <p>Workaround:</p> <p>In the ArcSight Command Center search page, after a search is completed click Export. Instead of selecting the checkbox to include All Fields, enter a comma-separated list of fields in the text area provided.</p>

Issue	Description
NGS-7912	In peer search, the search result is not refreshed responsively if one peer node has high hits, or the system is busy due to high ingestion rate or multiple searches running.
NGS-7891	<p>In an ArcSight Command Center Search, queries using some operators, such as eval, rename, replace, rex, and regex, may not return the correct results when searching the following types of fields:</p> <p>IPv4 fields such as sourceAddress</p> <p>MAC address fields such as destinationMacAddress</p> <p>IPv6 fields such as dvc_custom_ipv6_address1</p> <p>Geo Location fields such as dest_geo_latitude</p> <p>agentSeverity and locality fields</p> <p>For example the following queries may not return the correct results:</p> <p>... replace Low with notToWorry in agentSeverity</p> <p>... replace Local with localevents in locality</p>
NGS-7594	<p>In the ArcSight Command Center, after search results are exported and the session times out, you will see a logout message in the export window.</p> <p>Workaround:</p> <p>When this occurs:</p> <ol style="list-style-type: none"> 1. Close the export window. 2. Log in to ArcSight Command Center again. 3. Continue with the search.
NGS-7584	Fixed issue where a condition in a case query group with owner = <username> will return an error while viewing cases of a case query group in any user interface. Now search group will display cases for set username.
NGS-6886	<p>When a system has several peers and a peer stops responding, some pages in the ArcSight Command Center user interface might become slow to display. The delay happens regardless of the reason the peer system stopped responding.</p> <p>Workaround: Identify the peer that is not responding and remove its peer relationship on the Administration > Peers page, Peer Configuration tab. You can re-add the peer later, when it is back in service.</p>
NGS-6812	<p>The ESM server log and the Logger server log may contain messages that say "...NotSerializableException: ...PeerLoggerRequestDestination".</p> <p>These messages do not indicate an active problem, and can be ignored.</p>

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-23179	The command <code>./arcsight agent tempca -i</code> in connector version 7.5.0.7983.0 in FIPS SuiteB mode will throw an exception. Update the connector to a version later than version 7.5 where this might be addressed.
NGS-13049	When upgrading the Forwarding Connector, two fatal exception messages will appear, regarding <code>[agents[0].arcsightuser]</code> and <code>[agents[0].arcsightpassword]</code> . Workaround: Ignore these messages.
NGS-12407	Annotation flag indicating forwarded' may not get set when forwarding events from ESM.
NGS-1423	Upgrading a connector running on Windows from the ArcSight Console will fail if any process is using the connector's current folder. Workaround: <ol style="list-style-type: none">1. Make sure there are no files in the connector's "current" folder open.2. Start the connector by using Start > Programs > Connector Programs. Do not start the connectors using the "arcsight agents" command.

Installation and Upgrade

Issue	Description
NGS-30852	If your hostname includes periods and has a number after the last period, such as <code>this.is.2bad</code> , the installation fails when attempting to start up the manager. Hostnames with periods must be Fully Qualified Domain Names (FQDNs), which means that the last label is defined by IANA. Workaround: Change the hostname so that the last label is defined by IANA.
NGS-30686	Apple recently issued a warning relating to 32-bit app compatibility with macOS High Sierra 10.13.4 and later. This compatibility warning will show up during the Console installation process. You can safely ignore the warning and proceed with the installation.

Issue	Description
NGS-30503	<p>During the upgrade procedure, 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.</p> <p>Workaround: Ensure repo is running, then complete the following steps:</p> <ol style="list-style-type: none"> 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 mbus instances. 4. Restart the ESM cluster.
NGS-26661	<p>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.</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 /opt/arcsight/logger/current/arcsight/logger/logs/logger_init_driver.log if it contains this message: "Starting Apache...httpd: Could not open configuration file /opt/arcsight/logger/current/local/apache/conf/httpd.conf: No such file or directory Failed to start. Stopping APS...APS was not running." To prevent this failure, make sure the fully qualified domain name is configured properly on the ESM host before starting the upgrade.</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 consolesetup script from the ArcSight Console ..\current\bin directory.</p>

Issue	Description
NGS-7497	<p>Console installation on localized path works in some Windows 7 machines, but not in others. .</p> <p>Workaround:</p> <p>Due to the inconsistent behavior in Windows 7 machines, use English filenames only in installation paths. Local language names in paths may cause installation to fail in certain Windows 7 environments.</p>
NGS-3839	<p>Occasionally, the First Boot Wizard may fail to proceed due to some errors.</p> <p>Workaround:</p> <p>If this happens, terminate the process. After checking the logs and correcting the errors, follow the clean up instruction in the ESM Installation Guide and re-launch the installer.</p>
NGS-2783	<p>When a Forwarding Connector is installed, Superconnectors group is created under Custom Users Groups group. In addition, No Events enforcing filter is replaced by a specific event filter. After the upgrade, No Events enforcing filter will be reinstated meaning that no events will be forwarded from the Manager to the destination.</p> <p>Workaround: Remove the No Events enforcing filter.</p>

Localization

Issue	Description
NGS-23004	<p>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.</p>
NGS-22991	<p>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.</p>
NGS-22600	<p>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.</p>
NGS-22568	<p>In Traditional Chinese the function LengthOf may display incorrect values and/or produce the wrong filter results.</p>
NGS-21872	<p>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.</p> <p>Workaround: Go to the log retrieval page; you will find your newly generated logs.</p>

Pattern Discovery

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

Reports

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

Send Documentation Feedback

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

Feedback on ESM 7.2 Release Notes (ESM 7.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arcsight_doc@microfocus.com.

We appreciate your feedback!