HPE Security ArcSight Forwarding Connector

Software Version: 7.5.0.7986.0

Release Notes

April 6, 2017

Legal Notices

Warranty

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

This document is confidential.

Restricted Rights Legend

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

ArcSight Forwarding Connector Release Notes

These release notes provide information for the current release of the ArcSight Forwarding Connector.

ArcSight ESM Forwarding Connector

The ArcSight ESM Forwarding Connector can receive events from a source ESM Manager and then send them to a secondary destination such as ESM Manager, or to an ArcSight Logger.

In general, Forwarding Connectors support the last two ESM versions. Refer to the ESM Support Matrix for details.

What's New in the ArcSight Forwarding Connector

- New build number.
- Supported OS: RHEL 7.3, RHEL 6.8 and CentOS 7.3, CentOS 6.8.

ESM and Logger Connectivity

ESM in dual stack **preferred** IPV4/IPV6 will connect with Logger 6.4 or earlier releases. ESM in **pure** IPV6 mode will not connect with Logger 6.4 or earlier releases.

Supported Versions of HPE OM and HPE OMi

The supported versions of HPE OM and HPE OMi include:

- HPE OM for Windows v9.0 and 8.16 (patch level 90)
- HPE OM for UNIX v9.10
- HPE OM for Linux v9.10
- HPE OMi v9.0.1

  Note: OMi users are strongly encouraged to apply the latest patch, OMI_00005 (build 09.01.210), to obtain critical fixes before running this integration.

- HPE OMi v9.10 and v10

  Note: Only IPv4 addresses are supported for the HPE OM and HPE OMi destinations.

To Apply This Release

The installation executables are:

- ArcSight-7.5.0.7986.0-SuperConnector-Linux64.bin

Download and install the executable for your platform from the HPE Software Support site at https://softwaresupport.hpe.com. Use the executable included with your ESM or HPE integration release. The Linux executable serves all the Linux and Unix platforms.

Refer to the ESM Release Notes for details about what Forwarding Connector executables and features apply to your version of ESM.

> **Note:** The Forwarding Connector version number is specific to the Forwarding Connector component, and is not the same as the version number of the product with which it is released.
>
> Check the ESM release notes for Forwarding Connector features and upgrade paths supported for your version of ESM.

Forwarding Connector is not limited to use the same supported OS versions as the ESM due to not always being installed on the same machine as an ESM. In case the Forwarding Connector that is being upgraded is installed on the same machine as an ESM that will be upgraded, follow this order:

1. Upgrade the OS.
2. Upgrade the ESM source and destination.
3. Upgrade the Forwarding Connector.

Resolved Issues

There are no resolved issues at this time.

Known Issues

Number	Description
NGS-8926	If there is a Forwarding Connector running between a source Manager and any destination and a correlation event occurs on the source Manager then the Forwarding Connector will forward the correlation event and its associated correlated events to the destination. However, the EventAnnotationFlags=correlated field will not be populated for the correlated events in the source Manager's database. As a result, if there is any correlation content on the source Manager looking for the value EventAnnotationFlags=correlated, the content will not be matched or triggered.
NGS-12407	Annotation flag indicating 'forwarded' may not get set when forwarding events from ESM 6.11. 0
NGS-12742	Event ID may appear as negative when using three or more forwarding connectors to a single destination. ESM forwarding information and Event ID are stored together as one value, and the negative number can be considered expected.
NGS-13253	GUI agent setup must be used to add or modify fifth destination.
CON-14754	When Forwarding Connector is re-registered with the same destination, a new hierarchy is created with the original connector’s name as a folder. The connector name in the folder hierarchy displays in numerics.
CON-14748	When Forwarding Connector is installed by a specific user, it cannot be accessed by other users. This causes a user mismatch and an error displays saying: “The uninstallation could not complete due to an error.” **Workaround**: The same user who installs should be performing other operations.

Number	Description
CON-12107	The certificate auto-import feature does not work for FIPS Suite B. **Workaround:** The certificate must be manually imported for FIPS Suite B installations.
NGS-21805	Forwarding Connector destinations OM & OMi do not support IPv6. **Workaround:** Only IPv4 addresses are supported for the OM and OMi destinations.

NGS-23503	Unable to replace source Manager certificate in Forwarding Connector.
	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 Installation Guide*. But there are problems that may occur while attempting to replace a source Manager certificate on a Forwarding Connector. A deleted source Manager certificate may reappear in the Forwarding Connector truststore unless it is deleted from two separate truststores.
	Workaround:
	Use the following procedure when the certificate of a source ESM Manager of a Forwarding Connector has changed:
	1. Export the new Manager certificate from the source Manager.
	2. Delete the old Manager certificate in the Forwarding Connector from both FIPS and non-FIPS truststores using the following sample commands. (Command samples are derived from the *SmartConnector 7.5 User's Guide*. The certificate alias and keystore password will vary based on your installation.)
	`jre/bin/keytool -keystore jre/lib/security/cacerts -delete -storepass changeit -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388"`
	`jre/bin/keytool -keystore user/agent/fips/bcfips_ks -storetype BCFKS -storepass change -delete -providername BCFIPS -providerclassorg.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -J-Djava.security.egd=file:/dev/urandom -alias "hostname.yourdomain.net_8443-cn=hostname.yourdomain.net, ou=yourorg, o=acme, l=95014, st=ca, c=us-1490656465388"`
	3. Import the source Manager certificate into Forwarding Connector truststore.
	4. Run agent setup on Forwarding Connector to re-register the destination Managers to the connector.
	The full alias of the Manager certificate may be found by running the keytool command with the `-list` option using the following sample:
	`jre/bin/keytool -keystore jre/lib/security/cacerts -list -storepass changeit`

Send Documentation Feedback

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

Feedback on Release Notes (Forwarding Connector 7.5.0.7986.0)

Just add your feedback to the email and click send.

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

We appreciate your feedback!