Hewlett Packard
Enterprise

HPE Security ArcSight ESM and Connectors

Configuring FIPS and Non-FIPS Compliant Modes for ESM and SmartConnectors

February 15, 2017

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

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

This document is confidential.

Restricted Rights Legend

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

Copyright Notice

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

Revision History

Date	Description
02/15/2017	Initial release.

Contents

What is FIPS? 4

Installation Instructions for ESM Destination 4

Install a Non-FIPS Connector 4

Import the ESM Manager Certificate Into a Non-FIPS Connector 5

Client Authorization 6

Enable FIPS and non-FIPS Modes for ESM 6.9.1 and SmartConnector 7.5 and Later 6

FIPS Mode 6

Non-FIPS Mode 9

Check Whether the Connector is in FIPS Mode 11

Remote Upgrade 12

Send Documentation Feedback 13

What is FIPS?

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

FIPS Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange. The entire suite of cryptographic algorithms is intended to protect both classified and unclassified national security systems and information.

Note: When FIPS-compliant connectors connect to a non-FIPS-compliant destination, the solution is not considered FIPS compliant. When the destination is installed in FIPS Suite B compliant mode, the SmartConnectors must also be installed in FIPS Suite B compliant mode.

Installation Instructions for ESM Destination

FIPS compliance in ArcSight connectors has been enhanced by moving to a new provider, Bouncy Castle, replacing provider NSS. This certified, pure Java provider brings new benefits, such as support for Windows 64-bit operating systems. With this move comes changes to the commands for working with certificates, trust stores, key stores, etc. For example, the NSS-specific commands, such as `runcertutil`, no longer apply. Regarding upgrades, certificates in the NSS store are automatically migrated to the new Bouncy Castle store. See the following sections for details.

Install a Non-FIPS Connector

A system is considered FIPS-compliant only if all members of the system operate using FIPS-compliant cryptographic modules. However, it is possible for an ArcSight ESM environment to simultaneously support both FIPS mode and non-FIPS mode components. This functionality enables phased rollouts of FIPS mode upgrades.

An ArcSight ESM instance that is running both FIPS mode and non-FIPS mode components simultaneously is considered **not** to be FIPS compliant.

To maintain SmartConnectors in non-FIPS mode during FIPS rollout, this section provides the installation and configuration steps that let the connector still authenticate with a FIPS-mode Manager.

This section supplements the information in the SmartConnector Configuration Guide for your connector.

Import the ESM Manager Certificate Into a Non-FIPS Connector

If ESM is in FIPS Default mode (FIPS 140-2), skip this section. The manager certificate will be downloaded during connector setup. Once you have installed and configured the connector with an ArcSight Manager (encrypted) destination, use the Java `keytool` command in a command shell to import your ESM Manager certificate.

The following example assumes that you installed the connector at `/opt/connector/syslog` and saved the certificate to import as `/opt/connector/syslog/current/user/agent/certs/esm.cer`.

The example below uses the default password. See the appendix for FIPS Compliant SmartConnectors in the *SmartConnector User Guide* on Protect 724 to set a non-default password.

Note: These steps import the certificate to the non-FIPS keystore. When the agent starts, it will copy all certificates, which are not already present, from this trust store to the FIPS trust store.

1. Navigate to the `/opt/connector/syslog/current` folder, for example:

   ```
   cd /opt/connector/syslog/current
   ```
2. Run the Java `keytool` command to import the certificate. See the following table for a description of `keytool` parameters.

   ```
   jre/bin/keytool -importcert -file user/agent/certs/esm.cer -keystore
   jre/lib/security/cacerts -storepass changeit
   ```
3. Enter `yes` when you are prompted to trust the certificate.

keytool Parameter Name	Parameter Value
file	Path to the certificate to import into the keystore.
keystore	Path to the Java keystore: <*Installation directory*>`/current/jre/lib/security/cacerts`.
storepass	Password for the Java keystore. Default is `changeit`. For a non-default value, the value must be the same as set in `agent.properties`: `ssl.truststore.password`.
alias	A unique name for this certificate in this trust store.

Client Authorization

Follow these instructions to enable Client Authorization for ESM and Connectors with ESM destinations. For any additional ESM configuration, see the *ESM Administrator's Guide* on Protect 724.

Enable FIPS and non-FIPS Modes for ESM 6.9.1 and SmartConnector 7.5 and Later

The instructions in the following sections list the steps to configure FIPS and non-FIPS modes for client authorization.

FIPS Mode

Note: The examples assume that you are on the Linux platform. For Windows platforms, use backslashes when entering commands.

The examples below use the default password. See the appendix for FIPS Compliant SmartConnectors in the *SmartConnector User Guide* on Protect 724 to set a non-default password.

On Connector

1. When installing a connector, after core software is installed, you are given the choice of adding a connector or setting global parameters. Select **Set global parameters** and select **Enabled** for **Set FIPS Mode**. Exit setup.
   If you had already added the connector, the **Modify Connector** window is displayed. Click **Next**, then select **Set Global Parameters**; click **Next**. Select **Enabled** for **Set FIPS Mode**. Exit setup.
2. Open a command window.
3. Enter `cd <installation directory>/current`
4. Generate the key pair in FIPS client key store:

   For Linux: jre/bin/keytool -genkeypair -alias agent -keystore config/keystore.client.bcfks -storepass changeit -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar -dname "cn=admin, ou=ArcSight, o=HP, c=US" -validity 365 -J-Djava.security.egd=file:/dev/urandom

For Windows: -J-Djava.security.egd=file:/dev/urandom is not needed.

5. Enter key password for <agent>.
6. Click **Enter** if the key password is the same as keystore password.
7. List the certification key. This is optional to validate the entry.

```
jre/bin/keytool -list -alias agent -keystore config/keystore.client.bcfks -storepass changeit -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar
```

8. Export the certificate from key pair:

```
jre/bin/keytool -exportcert -file ../agent.cer -alias agent -keystore config/keystore.client.bcfks -storepass changeit -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath lib/agent/fips/bc-fips-1.0.0.jar
```

Certificate stored in file <../agent.cer>

9. Copy certificate to ESM server.
10. Edit `user/agent/agent.properties`, add these lines:

```
auth.null=true
ssl.client.auth=true
ssl.keystore.password=changeit
ssl.fips.keystore.path=config/keystore.client.bcfks
```

11. If a non-default password was used to create the FIPS key store, add the following property:

```
ssl.fips.keystore.password=<new password>
```

On ESM Manager

1. Run the following commands to import the connector certificate:

```
cd /opt/arcsight/manager/bin
./arcsight runcertutil -A -n "agent" -t "CT,C,C" -d /opt/arcsight/manager/config/jetty/nssdb -i /tmp/agent.cer
```

2. Run the following commands to validate:

```
./arcsight runcertutil -L -d /opt/arcsight/manager/config/jetty/nssdb
```

3. Export the ESM manager certificate:
```
./arcsight runcertutil -L -r -d /opt/arcsight/manager/config/jetty/nssdb/
-n mykey -o /tmp/manager.cer
```
4. Copy `manager.cer` to connector installation directory**.**
5. Stop, then restart ESM Manager:
```
/etc/init.d/arcsight_services stop manager
/etc/init.d/arcsight_services start manager
/etc/init.d/arcsight_services status all
```

Back to Connector

1. Import the ESM manager cert to Connector FIPS trust store:
   a. `cd <install dir>/current`

   jre/bin/keytool -importcert -file ../manager.cer -keystore "user/agent/fips/bcfips_ks" -storepass changeit -storetype BCFKS -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath "lib/agent/fips/bc-fips-1.0.0.jar" -J-Djava.security.egd=file:/dev/urandom -alias esm

   For Windows: -J-Djava.security.egd=file:/dev/urandom is not needed.

   b. Enter **yes** to trust the certificate.
2. Run agent setup:
```
cd <installation dir>/current/bin
./runagentsetup.sh
```

   For Windows: Use runagentsetup.bat.

3. Select the connector to add. Enter connector configuration parameter values as required. Click **Next** to proceed to destination selection.
4. Add the ESM destination. For FIPS Ciphers, select the option that matches how the target ESM is configured (Default (140-2), FIPS-128, etc.) This should match how ESM is configured.

   If ESM is in SSL-Only mode, do not enter anything for username and password. See the table for details.

ESM Configuration	Username	Password
SSL-Only	Leave blank	Leave blank
Password and SSL	Enter name	Enter password
Password or SSL	Leave blank	Leave blank

5. Wait until connector registration completes. The next window displays:

```
Following are the added connector details: Connector Name [the name you
provided], Connector Type [syslog]
```

6. When you are given the choice to **Continue** or **Exit** the wizard, click Exit.

Non-FIPS Mode

Note: The examples assume that you are on the Linux platform. For Windows platforms, use backslashes when entering commands.

The examples below use the default password. See the appendix for FIPS Compliant SmartConnectors in the *SmartConnector User Guide* on Protect 724 to set a non-default password.

On Connector

1. After the connector core software is installed, you are given the choice of adding a connector or setting global parameters. Select **Set global parameters** and select **Enabled** for **Set FIPS Mode**. Exit setup.
   If you had already added the connector, the **Modify Connector** window is displayed. Click **Next**, then select **Set Global Parameters**; click **Next**. Select **Disabled** for **Set FIPS Mode**. Exit setup.
2. Open a command window.
3. Enter `cd <installation directory>/current`
4. Generate the key pair in FIPS client key store:

   ```
   jre/bin/keytool -genkeypair -keystore config/keystore.client -storetype JKS -storepass changeit
   -dname "cn=admin, ou=ArcSight, o=HP, c=US" -alias admin -validity 365
   ```

5. Enter key password for <agent>.
6. Click **Enter** if the key password is the same as keystore password.
7. List the certification key. This is optional to validate the entry.

   ```
   jre/bin/keytool -list -keystore config/keystore.client -storetype JKS -storepass changeit
   ```

8. Export the certificate from key pair:

   ```
   jre/bin/keytool -exportcert -keystore config/keystore.client -alias agent -storepass changeit -file
   ../agent.cer
   ```

   Certificate is stored in file `<../agent.cer>`
9. Copy certificate to ESM server.

10. Edit `user/agent/agent.properties`, add these lines:

```
auth.null=true
ssl.client.auth=true
ssl.keystore.password=changeit
```

On ESM Manager

1. Run the following commands to import the connector certificate:

```
cd /opt/arcsight/manager/bin
./arcsight keytool -store managercerts -importcert -alias agent -file
/opt/agent.cer
```

2. Enter `yes` to trust.
   If there is an error that the alias already exists, just change alias.
3. Run the following commnand to export the ESM manager certificate:

```
./arcsight keytool -exportcert -store managerkeys -alias mykey -file
/opt/arcsight/manager.cer
```

4. Copy `manager.cer` to the connector installation directory.
5. Stop, then restart ESM Manager:

```
/etc/init.d/arcsight_services stop manager
/etc/init.d/arcsight_services start manager
/etc/init.d/arcsight_services status all
```

Back to Connector

1. Run the following commands to import the ESM manager certificate to the Connector FIPS trust store:
   a. `cd <install dir>/current`

   jre/bin/keytool -keystore jre/lib/security/cacerts -storepass changeit -importcert –file ../manager.cer

   b. Enter **yes** to trust the certificate.
2. Run agent setup:

```
cd <installation dir>/current/bin
./runagentsetup.sh
```

   For Windows: Use runagentsetup.bat.

3. Select the connector to add. Enter connector configuration parameter values as required. Click **Next** to proceed to destination selection.
4. Add the ESM destination.

   If ESM is in SSL-Only mode, do not enter anything for username and password. See the table for details.

ESM Configuration	Username	Password
SSL-Only	Leave blank	Leave blank
Password and SSL	Enter name	Enter password
Password or SSL	Leave blank	Leave blank

5. Wait until connector registration completes. The next window displays:

   ```
   Following are the added connector details: Connector Name [the name you provided], Connector Type [syslog]
   ```

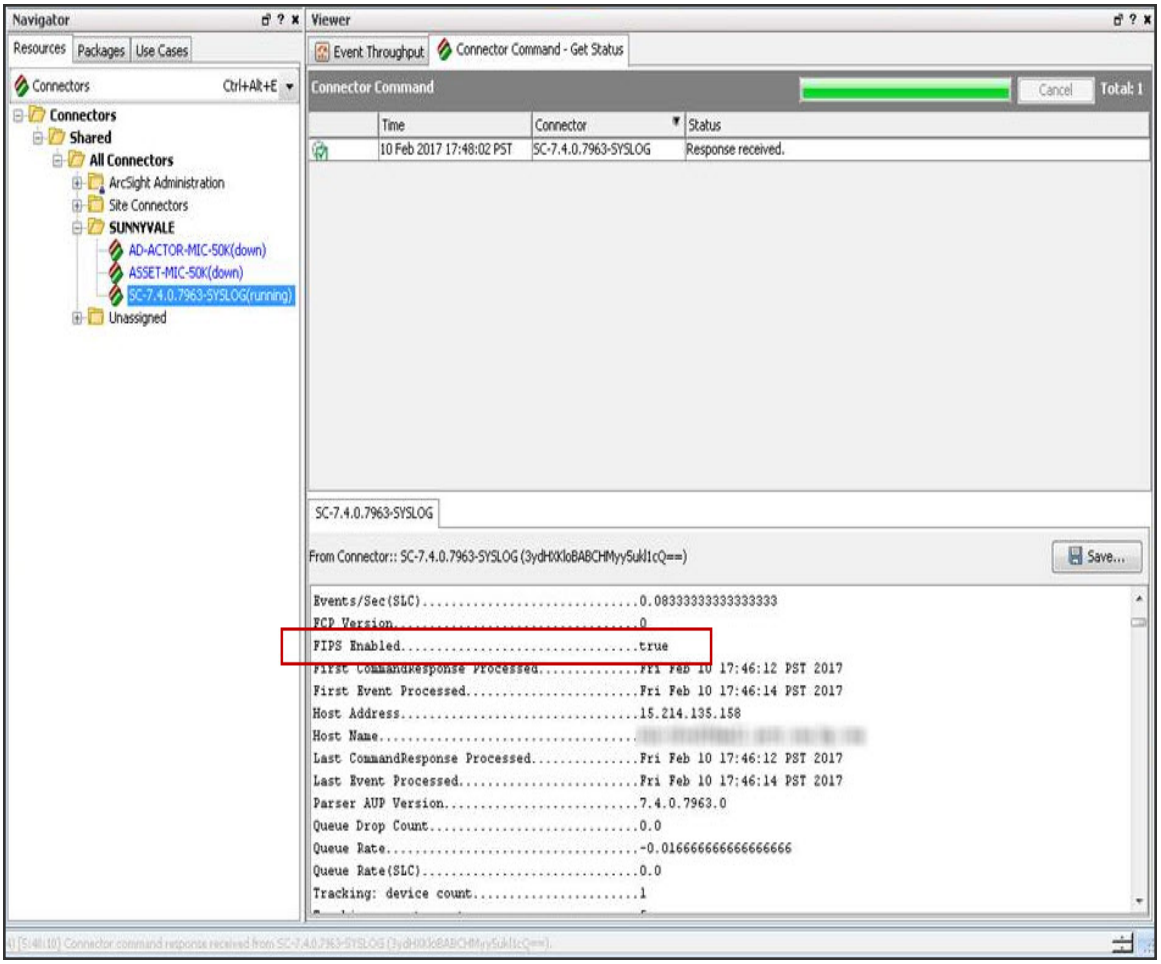
6. Exit the setup wizard.

Check Whether the Connector is in FIPS Mode

You can determine whether the connector is connecting through FIPS and is FIPS compliant by checking either the FIPS connector log or the ArcSight Console.

- Check the FIPS connector log. When the connector starts, the `agent.log` contains a log line indicating that the connector is `Running in FIPS mode`.

- Issue the **Send Command > Status > Get Status** command from the ESM Console. A property `FIPS Enabled` is set to `true` in the output returned to the ESM Console.



Remote Upgrade

The remote connector (AUP) upgrade feature does not work on Windows platforms when the connector is installed in FIPS compliant mode. See *Installing FIPS-Compliant SmartConnectors* on Protect 724 for details.

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 Configuring FIPS and Non-FIPS Compliant Modes for ESM and SmartConnectors (ESM and Connectors)

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!