HPE Security ArcSight ESM and Connectors

Configuring FIPS for ESM and SmartConnectors

April 14, 2017

Legal Notices

Warranty

Restricted Rights Legend

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
04/14/2017	Renamed *Configuring FIPS and Non-FIPS Compliant Modes for ESM and SmartConnectors* to *Configuring FIPS for ESM and SmartConnectors*.
02/15/2017	Updated FIPS installation procedures to support Bouncy Castle.
02/15/2013	Restored material regarding manual steps for enabling FIPS mode.
11/15/2012	Added connectors using Oracle drivers to the non FIPS-compliant connectors list.
02/15/2012	Added information for installing connectors in FIPS Suite B Compliant mode.

Date	Description
08/12/2011	Updated commands for importing nssdb.client. Clarified that connectors operating in FIPS-complient mode sending events to an ESM Manager that is not FIPS-compliant does not constitute a FIPS-compliant solution.
05/15/2011	Added additional configuration required when installing connectors to CEF Syslog (TLS) destination in FIPS-compliant mode.
03/30/2011	Fixed issues with some commands and procedures. Added FIPS-compliant and non-compliant connectors lists.
06/25/2010	Added known limitations for installation platforms.
02/11/2010	Added FIPS Suite B support, as well as how to check whether connector is running in FIPS-compliant mode.
06/30/2009	First version of this guide.

Contents

Chapter 1: 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.

Chapter 2: 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. 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 ArcSight Manager.

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

Import the ArcSight Manager Certificate Into a Non-FIPS Connector

If ESM was not setup with FIPS Suite B certificates, skip this section and continue with "Client Authorization".

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 ArcSight Manager certificate.

> **Note:** The following example:
>
> - 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.
> - 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`.
> - assumes that you are on the Linux platform. For Windows platforms, use backslashes when entering commands.

Follow these steps to import the certificate to a non-FIPS keystore:

1. Navigate to the `/opt/connector/syslog/current` folder and run the Java `keytool` command to import the certificate. See the following table for a description of `keytool` parameters.

   ```
   cd /opt/connector/syslog/current

   jre/bin/keytool -importcert -file user/agent/certs/esm.cer -keystore
   jre/lib/security/cacerts -storepass changeit
   ```

2. 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.

Chapter 3: 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 following sections describe the steps to configure FIPS and non-FIPS modes for client authorization.

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

FIPS Mode (ESM 6.9.1 and SmartConnector 7.5 and Later)

Step 1: On the 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 and navigate to the `current` directory, for example:

   `cd <installation directory>/current`

3. Generate the key pair in the FIPS client key store:

   For Linux platforms:

   ```
   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
```

> **On Windows platforms: Omit** the -J-Djava.security.egd=file:/dev/urandom
> option.

4. Enter the key password for `<agent>`.

5. Click **Enter** if the key password is the same as keystore password.

6. 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
```

7. Export the certificate from the 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
```

The certificate is stored in the `<../agent.cer>` file.

8. Copy the certificate to the ESM server.

9. Edit the `user/agent/agent.properties` file to add these lines:

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

> **Note:** The auth.null=true and ssl.client.auth=true settings imply that the
> authentication mode is SSL **or** password authentication. If the mode is SSL **and** password
> authentication, then they should be: auth.null=false and ssl.client.auth=true.

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

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

Step 2: On the ArcSight Manager

1. Navigate to the `bin` directory and run the following command to import the connector certificate,
   for example:

```
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
```

> **Note:** This example assumes that there is an account on ArcSight Manager whose external
> ID matches the `cn=admin` value in the connector's certificate. This value will be different for
> each customer. For information on the external ID string see the *ArcSight Manager
> Administrator's Guide*.

3. Export the ArcSight Manager certificate:

```
./arcsight runcertutil -L -r -d /opt/arcsight/manager/config/jetty/nssdb/
-n mykey -o /tmp/manager.cer
```

4. Copy the `manager.cer` file to the connector installation directory.

5. Stop, then restart ArcSight Manager:

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

Step 3: On the Connector

1. Navigate to the `current` directory and import the ArcSight Manager certificate to the Connector
   FIPS trust store, for example:

```
cd <installation directory>/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
```

> **On Windows platforms: Omit** the `-J-Djava.security.egd=file:/dev/urandom`
> option.

2. Enter **yes** to trust the certificate.

> **For Connector version 7.5 only:** If you plan to upgrade from ESM, follow these steps:
>
> a. Navigate to the `current` directory and import the ArcSight Manager certificate to the
>   connector FIPS key store, for example:
>
>    ```
>    cd <install dir>/current/
>    ```
>
>    ```
>    jre/bin/keytool -importcert -file ../manager.cer -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"
-J-Djava.security.egd=file:/dev/urandom -alias esm
```

On Windows platforms: Omit the `-J-Djava.security.egd=file:/dev/urandom`
option.

   b. Enter **yes** to trust the certificate.

3. Navigate to the `bin` directory and run agent setup:

   `cd <installation directory>/current/bin`

   `./runagentsetup.sh`

> **On Windows platforms:** Run the `runagentsetup.bat` executable.

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

5. Add the ESM destination. For FIPS Ciphers, select the option that matches how the target ESM is
   configured (Default (140-2), FIPS-128, and so on). This should match how ESM is configured.

   If ESM is in SSL-Only mode, do not enter anything for username and password. See the following
   table for details. For more information on these configuration modes, see the *ESM Administrator's
   Guide* on Protect 724.

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

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

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

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

Non-FIPS Mode (ESM 6.9.1 and SmartConnector 7.5 and Later)

Step 1: On the 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 **Disabled** for **Set FIPS Mode**.
   Exit setup.

If you have 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 and navigate to the current directory, for example:

   ```
   cd <installation directory>/current
   ```

3. Generate the key pair in FIPS client key store, for example:

   ```
   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
   ```

4. Enter key password for <agent>.

5. Click **Enter** if the key password is the same as keystore password.

6. List the certification key. This is optional to validate the entry.

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

7. Export the certificate from key pair:

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

   The certificate is stored in the <../agent.cer> file.

8. Copy the certificate to the ESM server.

9. Edit the user/agent/agent.properties file to add these lines:

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

   > **Note:** The auth.null=true and ssl.client.auth=true settings imply that the authentication mode is SSL **or** password authentication. If the mode is SSL **and** password authentication, then they should be: auth.null=false and ssl.client.auth=true.

Step 2: On the ArcSight Manager

1. Navigate to the bin directory and run the following command to import the connector certificate, for example:

   ```
   cd /opt/arcsight/manager/bin
   ```

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

2. Enter yes to trust the certificate.

   If you receive an error that the alias already exists, change the value of alias.

3. Run the following command 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 ArcSight Manager:

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

Step 3: On the Connector

1. Navigate to the `current` directory and run the following commands to import the ArcSight Manager certificate to the Connector FIPS trust store, for example:

   `cd <installation directory>/current`

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

   Enter **yes** to trust the certificate.

2. Navigate to the `bin` directory and run agent setup:

   `cd <installation directory>/current/bin`

   `./runagentsetup.sh`

   > **On Windows platforms:** Run the `runagentsetup.bat` executable.

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 or password. See the following table for details. For more information on these configuration modes, see the *ESM Administrator's Guide* on Protect 724.

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.

Enable FIPS and non-FIPS Mode for ESM 6.11 and SmartConnector 7.4 and Earlier

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

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

FIPS Mode (ESM 6.11 and SmartConnector 7.4 and Earlier)

Step 1: On the 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 and navigate to the `current` directory, for example:

   `cd <installation directory>/current`

3. Generate the key pair in the FIPS client key store:

   - **For FIPS Default (140-2)**:

     `bin/arcsight runcertutil -S -s "CN=admin" -v 1 -n agent -k rsa -x -t "C,C,C" -m 1234 -d user/agent/nssdb.client`

   - **For FIPS Suite B**:

     Refer to "Types of Key Pairs Used in FIPS Mode" in the *ESM Administrator's Guide* on Protect 724.

4. Enter the NSS DB password.

5. List the certification key. This is optional to validate the entry.

   `bin/arcsight runcertutil -L -d user/agent/nssdb.client -n agent`

6. Export the certificate from the key pair:

```
bin/arcsight runcertutil -L -n agent -r -d user/agent/nssdb.client -o
../agent.cer
```

The certificate is stored in the `<../agent.cer>` file.

7. Copy the certificate to the ESM server.

8. Edit the `user/agent/agent.properties` file to add these lines:

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

> **Note:** The `auth.null=true` and `ssl.client.auth=true` settings imply that the authentication mode is SSL **or** password authentication. If the mode is SSL **and** password authentication, then they should be: `auth.null=false` and `ssl.client.auth=true`.

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

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

Step 2: On the ArcSight Manager

1. Navigate to the `bin` directory and run the following command to import the connector certificate, for example:

```
cd /opt/arcsight/manager/bin
```

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

2. Run the following commands to validate:

```
./arcsight keytool -store managercerts -list -alias agent
```

3. Export the ArcSight Manager certificate:

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

4. Copy the `manager.cer` file to the connector installation directory.

5. Stop, then restart ArcSight Manager:

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

Step 3: On the Connector

1. Navigate to the `bin` directory and import the ArcSight Manager certificate to the Connector FIPS trust store, for example:

```
cd <installation directory>/current/bin
```

```
./arcsight agent keytool -store clientcerts -importcert -alias esm -file
/opt/manager.cer
```

> **On Solaris platforms:** Run the following command instead:
>
> ```
> ./bin/arcsight runcertutil –A –n esm -t "CT,C,C"
> –d /user/agent/nssdb.client –I /opt/manager.cers
> ```

2. Enter **yes** to trust the certificate.

3. Navigate to the `bin` directory and run agent setup:

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

   > **On Windows platforms:** Run the `runagentsetup.bat` executable instead.

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

5. Add the ESM destination. For FIPS Ciphers, select the option that matches how the target ESM is configured (Default (140-2), FIPS-128, and so on). This should match how ESM is configured.

   If ESM is in SSL-Only mode, do not enter anything for username and password. See the following table for details. For more information on these configuration modes, see the *ESM Administrator's Guide* on Protect 724.

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

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

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

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

Non-FIPS Mode (ESM 6.11 and SmartConnector 7.4 and Earlier)

Step 1: On the 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 **Disabled** for **Set FIPS Mode**. Exit setup.

If you have 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 and navigate to the `current` directory, for example:

   `cd <installation directory>/current`

3. Generate the key pair in FIPS client key store, for example:

   ```
   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
   ```

4. Enter key password for `<agent>`.

5. Click **Enter** if the key password is the same as keystore password.

6. List the certification key. This is optional to validate the entry.

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

7. Export the certificate from key pair:

   ```
   jre/bin/keytool -exportcert -keystore config/keystore.client -alias admin
   -storepass changeit -file ../agent.cer
   ```
   The certificate is stored in the `<../agent.cer>` file.

8. Copy the certificate to the ESM server.

9. Edit the `user/agent/agent.properties` file to add these lines:

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

   > **Note:** The `auth.null=true` and `ssl.client.auth=true` settings imply that the authentication mode is SSL **or** password authentication. If the mode is SSL **and** password authentication, then they should be: `auth.null=false` and `ssl.client.auth=true`.

Step 2: On the ArcSight Manager

1. Navigate to the `bin` directory and run the following command to import the connector certificate, for example:

   `cd /opt/arcsight/manager/bin`

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

2. Enter `yes` to trust the certificate.

   If you receive an error that the alias already exists, change the value of `alias`.

3. Run the following command 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 ArcSight Manager:

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

Step 3: On the Connector

1. Navigate to the `current` directory and run the following commands to import the ArcSight Manager certificate to the Connector non-FIPS trust store, for example:

   ```
   cd <installation directory>/current
   ```

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

   Enter **yes** to trust the certificate.

2. Navigate to the `bin` directory and run agent setup:

   ```
   cd <installation directory>/current/bin
   ```

   ```
   ./runagentsetup.sh
   ```

   > **On Windows platforms:** Run the `runagentsetup.bat` executable.

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 or password. See the following table for details. For more information on these configuration modes, see the *ESM Administrator's Guide* on Protect 724.

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.

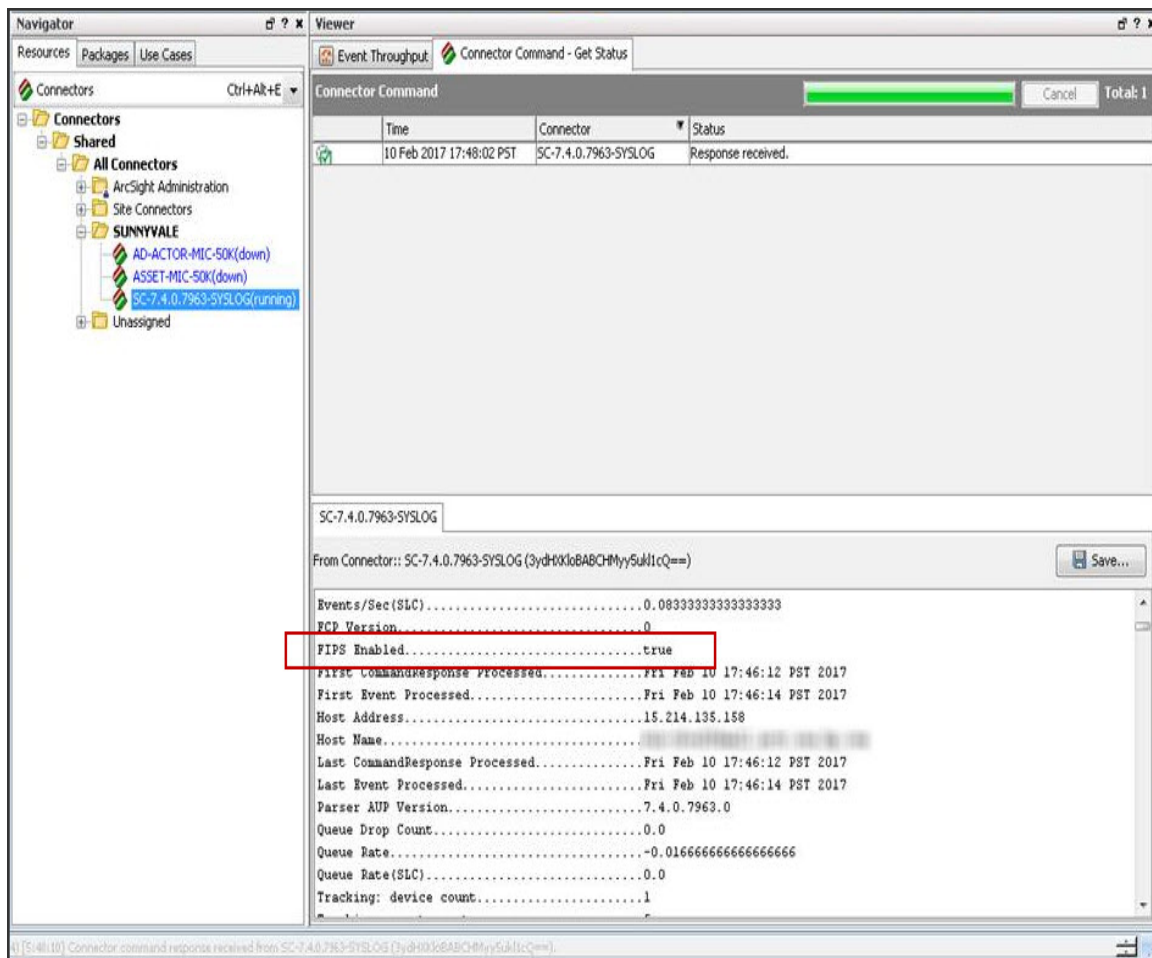# Chapter 4: Check Whether the Connector is in FIPS Mode

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` file contains a log line indicating that the connector is `Running in FIPS mode`.

- Issue the **Send Command > Status > Get Status** command from the ArcSight Console. The FIPS

`Enabled` property is set to `true` in the output returned to the ArcSight 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 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!