Hewlett Packard
Enterprise

# HPE Security ArcSight Connectors

## Installing FIPS-Compliant SmartConnectors

February 15, 2013

**Installing FIPS-Compliant SmartConnectors**

February 15, 2013

**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 Package Enterprise Development LP shall not be liable for technical or editorial 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. Hewlett Package Enterprise Development LP 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 Development LP 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.

Follow this link to see a complete statement of Hewlett Package Enterprise Development LP copyrights, trademarks and acknowledgements:
http://www.hpenterprisesecurity.com/copyright.

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

This document is confidential.

# Revision History

| Date | Description |
|---|---|
| 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. |
| 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

## 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.

When FIPS-compliant connectors connector to a non-FIPS-compliant ESM Manager, the solution is not considered FIPS compliant. Also, when the ESM Manager is installed in FIPS Suite B compliant mode, the SmartConnectors also must be installed in FIPS Suite B compliant mode.

## Which Connectors are Supported?

### FIPS Compliant Connectors

- All syslog connectors
- All file reader connectors
- All SNMP connectors
- All database connectors (except Oracle Audit DB and when using SQL Server drivers with encryption)
- Cisco Secure IDS RDEP (Legacy) and Cisco Secure IPS SDEE connectors
- Sourcefire Defense Center eStreamer connector
- Check Point OPSEC NG connector

### FIPS Non-Compliant Connectors

- Microsoft Windows Event Log – Unified
- Database connectors using SQL Server drivers with encryption
- Connectors using Oracle drivers
- Connectors running on AIX or HP UX platforms only

### Connectors Not Certified as FIPS Compliant

- Microsoft Windows Event Log – Domain connectors
- Various API connectors with proprietary internal mechanisms

# Connector Caveats

Certain limitations apply for some connector types, as described in the sections that follow.

## CEF Syslog as the Destination

If you choose **CEF Syslog** (with TLS protocol) as the destination for the connector, the wizard attempts to retrieve the security certificate from the destination and import it based upon your input. Although the CEF Syslog destination works as expected in FIPS-compliant mode, when you edit `agent.properties` to enable FIPS-compliant mode (as described in "Enable FIPS Mode " on page 6), the certificate retrieved from the destination may not be imported properly into the truststore.

If the SmartConnector wizard is unable to fetch and import the destination certificate, you can import the certificate manually:

1. Copy the certificate from the destination to a temporary location.
2. From the **`$ARCSIGHT_HOME/current/bin`** directory, execute the following command to import the certificate:

   ```
   arcsight keytoolgui
   ```
3. Open the keystore in **`$ARCSIGHT_HOME/jre/lib/security/cacerts`** (the password will be `changeit`).
4. From the **Menu** bar, select **Tools** and **Import Certificate**. Upload the certificate file.
5. Trust the certificate.
6. Start the connector and the device.

## Running on Windows 64-bit

The NSS DB is not supported for Windows 64-bit, so FIPS support should not be enabled on 64-bit platforms.

## Running on Windows XP

If you are running connector build 4.8.1.xxxx on a Windows XP platform and unable to bring up the connector in FIPS mode, make sure that .NET Framework 2.0 is installed on your system and try again.

## Running as a Service

If you are upgrading a connector running as a service from a build earlier than 4.7.4.5335 with an intention of enabling FIPS mode on the connector, the connector service must be uninstalled and reinstalled. If you do not intend to enable FIPS mode and continue to run the connector in default mode, this step is not required.

## Microsoft SQL 2005 JDBC Driver

If you are running a database connector that uses the SQL 2005 JDBC driver *with encryption enabled*, the connector cannot be installed in FIPS-compliant mode. With encryption turned off, the MS SQL Server 2005 JDBC driver version 1.1 rather than 1.2 of the SQL Server 2005 JDBC driver should be used.

See the configuration guide for the database connector you are installing for instructions for downloading and installing a Microsoft SQL Server 2005 JDBC driver.

## Remote Upgrade

The remote connector upgrade feature does not work on Windows platforms when the connector is installed in FIPS compliant mode. The workaround is to perform a local upgrade on the connectors. A solution to this problem is under investigation.

# Enable FIPS Support

When installing a software connector, the instructions for enabling FIPS Support and FIPS Suite B support are provided as part of the installation procedure. When installing a SmartConnector on an appliance, such as Connector Appliance or ArcSight Express, you can enable FIPS support through the user interface by enabling support on the container or containers containing the connector for which you want to enable support.

## Manual Procedure: FIPS SmartConnector to FIPS Manager Installation

### Enable FIPS Mode

1. Create an **agent.properties** file at the following location:

   ```
   $ARCSIGHT_HOME/current/user/agent
   ```

   You can skip this step if the file already exists (this is the case when the mode is changed from default mode to FIPS mode).

2. Enter the following property:

   ```
   fips.enabled=true
   ```

3. Save and exit **agent.properties.**

If you selected CEF Syslog as the connector's destination, see " CEF Syslog as the Destination" on page 5 for important information.

### Import the ESM Manager Certificate

1. Step 1 turns off FIPS mode and is required only for SmartConnector releases prior to 4.8.1. If you are installing 4.8.1 or later version, continue with step 2.

   From the **$ARCSIGHT_HOME/current/bin** directory, run the following command to set FIPS mode off.

   ```
   arcsight runmodutil -fips false -dbdir $ARCSIGHT_HOME/current/user/agent/nssdb.client
   ```

2. Copy your key file (in this example, **mykey.cert**) into the **$ARCSIGHT_HOME/current/bin** directory.

3. From $**ARCSIGHT_HOME/current/bin**, enter the following:

   ```
   arcsight runcertutil -A -n mykey -t "CT,C,C" -d
   $ARCSIGHT_HOME/current/user/agent/nssdb.client -i
   $ARCSIGHT_HOME/current/bin/mykey.cert
   ```

4. Step 4 turns FIPS mode on and is required only for SmartConnector releases prior to 4.8.1. If you are installing 4.8.1 or later version, skip this step.

   From the **$ARCSIGHT_HOME/current/bin** directory, run the following command to set FIPS mode on:

   ```
   arcsight runmodutil -fips true -dbdir
   $ARCSIGHT_HOME/current/user/agent/nssdb.client
   ```

Restart the connector for your changes to take effect.

### Enable FIPS Suite B Support

Additional configuration is required to run the connector in FIPS Suite B compliant mode.

If you have installed a SmartConnector in FIPS-compliant mode, you can enable FIPS Suite B support by modifying the ESM destination parameters as follows:

> The ESM Manager must also be installed in FIPS Suite B mode.

**1** From $ARCSIGHT_HOME\current\user\agent, open `agent.properties` to edit.

**2** Locate the following property for ESM destination parameters (approximately, line 10 in the file):

```
agents[0].destination[0].params=<?xml version\="1.0" encoding\="UTF-
8"?>\n<ParameterValues>\n <Parameter Name\="port" Value\="8443"/>\n <Parameter
Name\="filterevents" Value\="false"/>\n <Parameter Name\="host"
Value\="samplehost.sv.arcsight.com"/>\n <Parameter Name\="aupmaster"
Value\="false"/>\n <Parameter Name\="fipsciphers"
Value\="fipsDefault"/>\n</ParameterValues>\n
```

**3** The destination parameters are specified here as an XML string where each element is one parameter. Based upon the Suite B mode of the ESM Manager, change `fipsDefault` to `suiteb128` (for 128-bit security) or `suiteb192` (for 192-bit security).

**4** Save and exit `agent.properties`.

Restart the connector for your changes to take effect.

# Additional Installation Instructions

## Non-FIPS Connector to FIPS Manager Installation

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 is to enable phased rollouts of FIPS mode upgrades.

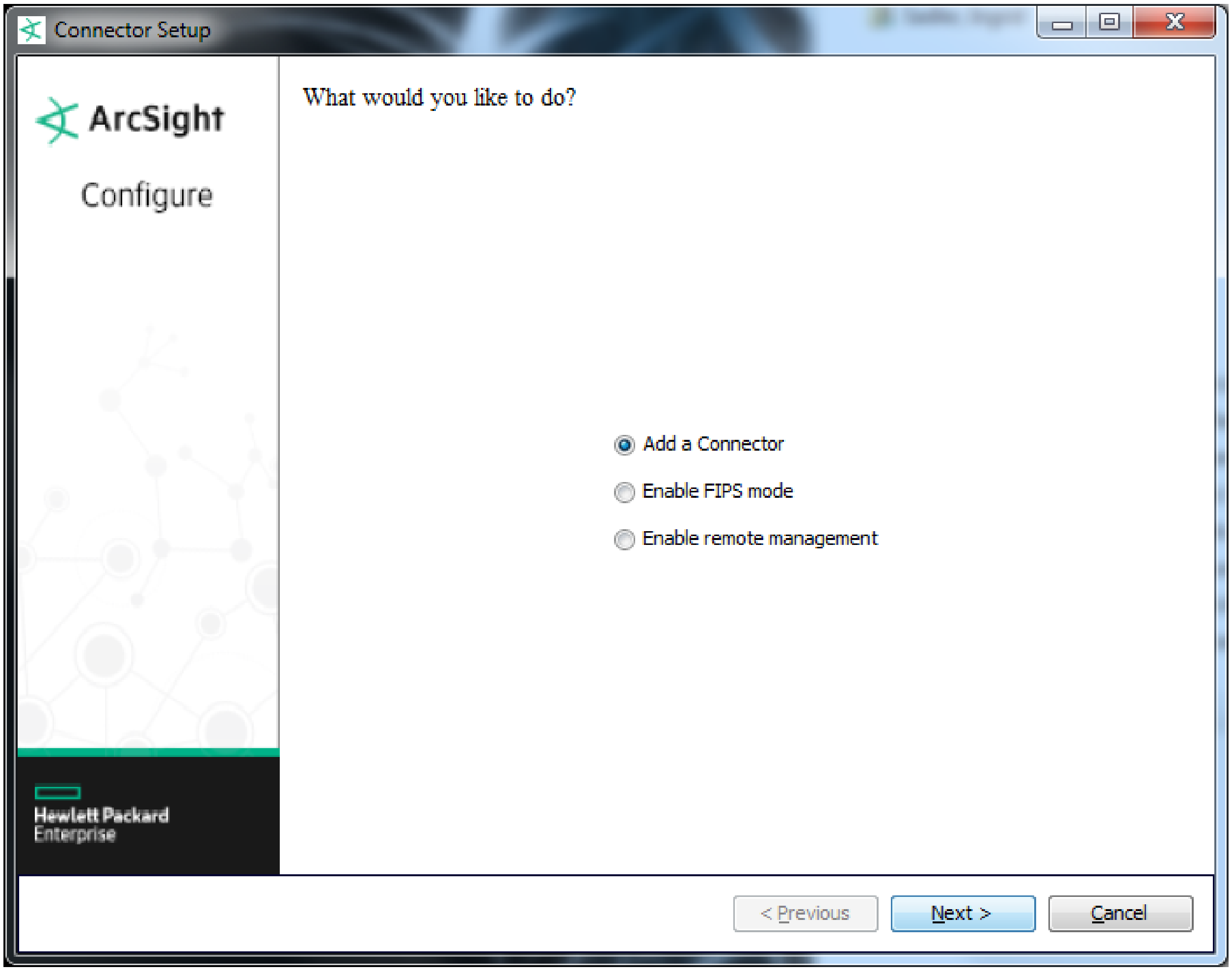
An ArcSight ESM instance that is running both FIPS mode and non-FIPS mode components simultaneously is considered **not** to be FIPS compliant.

If, during your FIPS mode rollout, you want to maintain SmartConnectors in non-FIPS mode, 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.

Follow device configuration steps provided in the configuration guide, then follow the installation procedure through installation of the core connector software (SmartConnector Installation step 2). At step 3, shown below, click **Cancel** to exit connector setup in order to perform configuration of the NSS DB, necessary for installing the connector in FIPS-compliant mode.

When the installation of ArcSight SmartConnector core component software is finished, the following window is displayed:



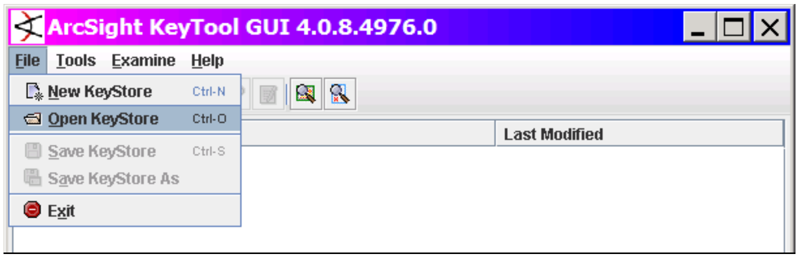
Click **Cancel** at this point to exit the configuration wizard.  You will return to the wizard, and to the SmartConnector Configuration Guide for your device, after importing your ESM Manager certificate.

## Import Your ESM Manager Certificate

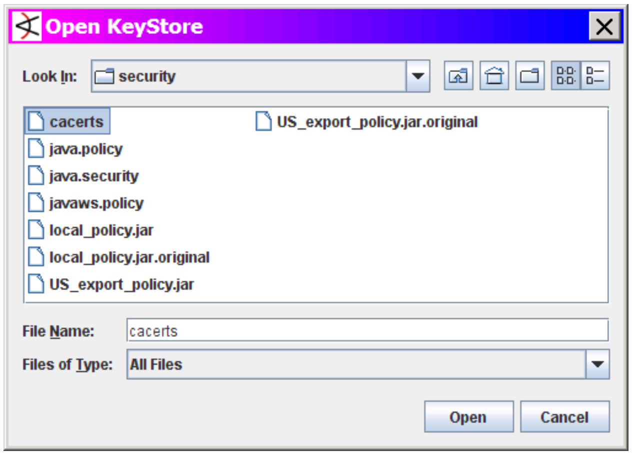
1 From **`$ARCSIGHT_HOME/current/bin`**, start the **`ArcSight KeyTool`** utility to import your ESM Manager certificate to the connector machine.

```
arcsight agent keytoolgui
```

2 A window such as the following is displayed; select **`Open KeyStore`** from the **File** menu.



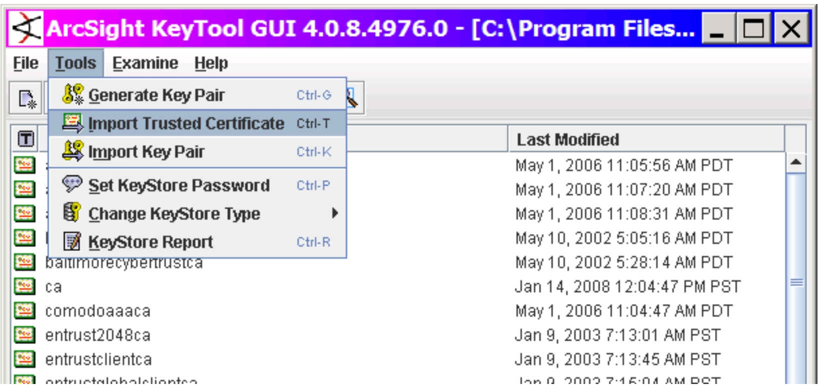
3 Open **`/current/jre/lib/security/cacerts`**:



File Name: cacerts

4 Enter the password when requested (**`changeit`**).

5 When the **`KeyStore`** opens, select **`Import Trusted Certificate`** from the **`Tools`** menu.


ArcSight KeyTool GUI 4.0.8.4976.0 - [C:\Program Files...
File
Tools
Examine
Help
Generate Key Pair Ctrl-G
Import Trusted Certificate Ctrl-T
Import Key Pair Ctrl-K
Set KeyStore Password Ctrl-P
Change KeyStore Type
KeyStore Report Ctrl-R

| | Last Modified |
|---|---|
| | May 1, 2006 11:05:56 AM PDT |
| | May 1, 2006 11:07:20 AM PDT |
| | May 1, 2006 11:08:31 AM PDT |
| | May 10, 2002 5:05:16 AM PDT |
| baltimorecybertrustca | May 10, 2002 5:28:14 AM PDT |
| ca | Jan 14, 2008 12:04:47 PM PST |
| comodoaaaca | May 1, 2006 11:04:47 AM PDT |
| entrust2048ca | Jan 9, 2003 7:13:01 AM PST |
| entrustclientca | Jan 9, 2003 7:13:45 AM PST |
| entrustglobalclientca | Jan 9, 2003 7:15:04 AM PST |

6 Locate and select your ESM Manager certificate file, then click **`Import`**.

7 Exit the **`KeyTool GUI`**.

For release 4.7.4 and later, step 8 is not required; continue with step 9.

8 From the command line, enter the following:

```
set ARCSIGHT_JVM_OPTIONS=-Dhttps.protocols=TLSv1
```

9 To return to the SmartConnector configuration wizard, enter the following from **`$ARCSIGHT_HOME/current/bin`**:

```
arcsight connectorsetup
```

10 The connector selection window is again displayed; return to your SmartConnector Configuration Guide, SmartConnector Installation step 4 to continue the connector configuration.

For the remainder of the configuration process, see the Configuration Guide for the SmartConnector you selected to install. The specific configuration guide provides information about how to configure the device for event collection, specific installation parameters required during the configuration process, and a table of vendor-specific field mappings to ArcSight events.

## Running an Non-FIPS Connector with a FIPS Manager

***The steps in this section are required only for releases prior to SmartConnector release 4.7.4.5335.***

> The information in this section is provided to assist you during your transition of your existing deployment to a FIPS 140-2 compliant mode.

For a working connector-to-Manager connection with existing connectors you now want to connect to a FIPS 140-2 Mode ESM Manager, follow the instructions in the following sections as appropriate, depending upon whether the connector is running as a process or a service.

### Connectors Running as Processes

If you have installed the connector to run **as a process**, edit **`connectors.bat`** (from **`$ARCSIGHT_HOME/current/bin/scripts`**) to add the following:

```
set ARCSIGHT_JVM_OPTIONS=-Dhttps.protocols=TLSv1
```

You can add this line following the existing ARCSIGHT_JVM_OPTIONS line in the **`connectors.bat`** file; for example, in Windows:

```
set ARCSIGHT_JVM_OPTIONS=-server-XX:MaxNewSize=128m –verbose:gc –
Djava.security.policy="%ARCSIGHT_HOME%\config\agent\agent.policy" %
ARCSIGHT_MEM_OPTIONS% -Dhttps.protocols=TLSv1
```

For Linux:

```
export ARCSIGHT_JVM_OPTIONS=-Dhttps.protocols=TLSv1
```

Save and exit the file.

### Connectors Running as Services

> If you are upgrading a connector running as a service from a build earlier than 4.7.4.5335 with an intention of enabling FIPS mode on the connector, the connector service must be uninstalled and reinstalled. If you do not intend to enable FIPS mode and continue to run the connector in default mode, this step is not required.

If you have installed the connector to run as a **service**, from **`$ARCSIGHT_HOME\current\user\agent`**, open the **`agent.wrapper.conf`** file for edit.

In the section "Java Additional Parameters," uncomment the following line and update as shown; then save and exit the file:

After:

```
wrapper.java.additional.1=-server
wrapper.java.additional.2=-XX:MaxNewSize=128m
wrapper.java.additional.3=-verbose:gc
wrapper.java.additional.4=-DARCSIGHT_HOME=../../../
wrapper.java.additional.5=-Djava.security.policy=../../../config/
                                                agent/agent.policy
```

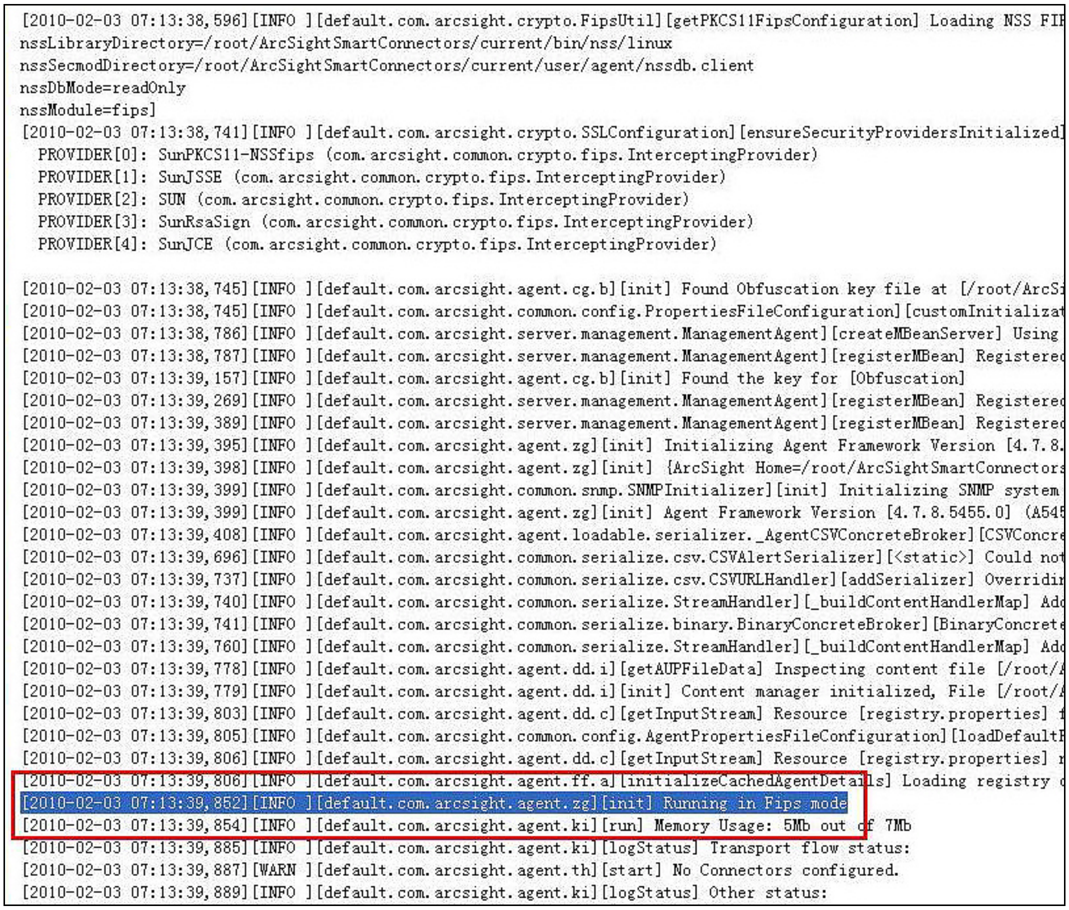
Add:

```
wrapper.java.additional.6=-Dhttps.protocols=TLSv1
```

## Checking Whether Connector is in FIPS Mode

To determine whether the connector is connecting through FIPS, and when connecting, whether it is FIPS compliant:

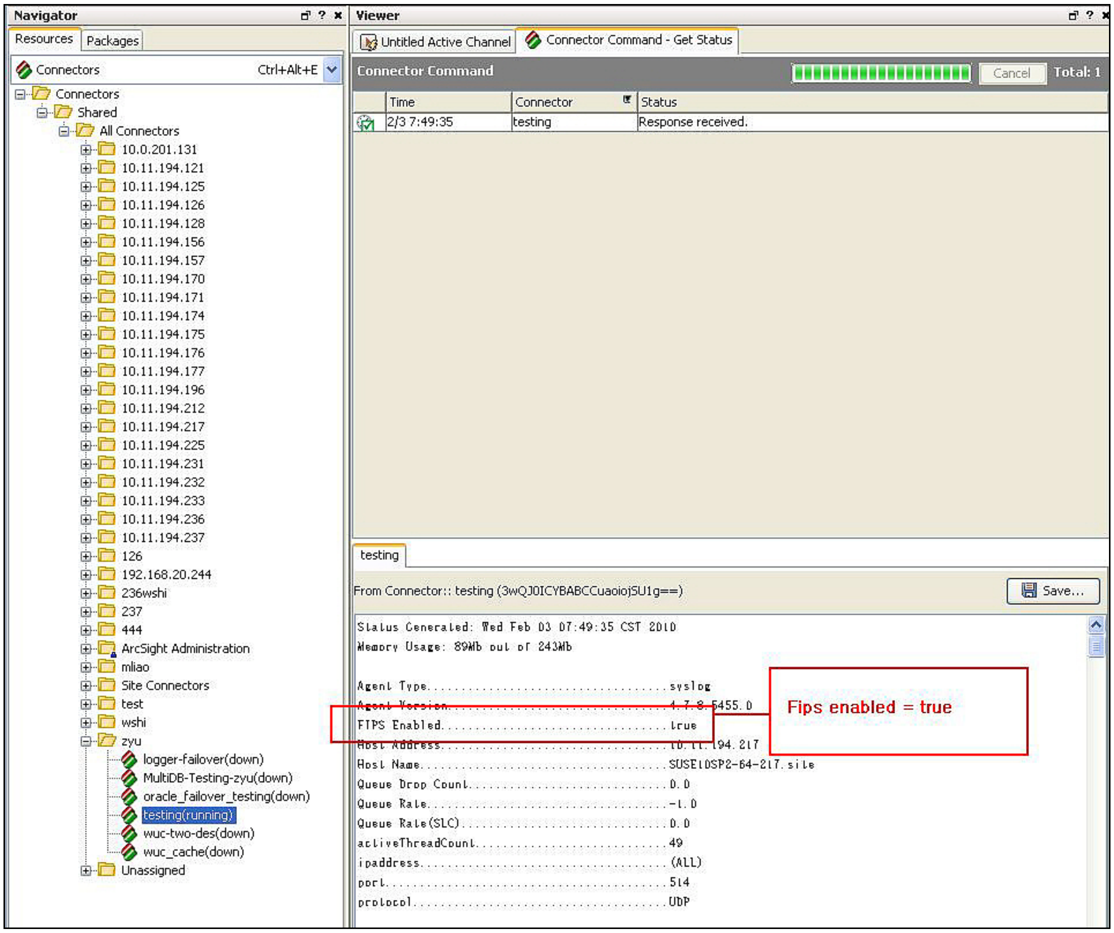
- Check the FIPS connector log. When the connector starts up, the agent.log has a log line indicating that the connector is "Running in FIPS mode."



```
[2010-02-03 07:13:38,596][INFO ][default.com.arcsight.crypto.FipsUtil][getPKCS11FipsConfiguration] Loading NSS FIP
nssLibraryDirectory=/root/ArcSightSmartConnectors/current/bin/nss/linux
nssSecmodDirectory=/root/ArcSightSmartConnectors/current/user/agent/nssdb.client
nssDbMode=readOnly
nssModule=fips]
[2010-02-03 07:13:38,741][INFO ][default.com.arcsight.crypto.SSLConfiguration][ensureSecurityProvidersInitialized]
  PROVIDER[0]: SunPKCS11-NSSfips (com.arcsight.common.crypto.fips.InterceptingProvider)
  PROVIDER[1]: SunJSSE (com.arcsight.common.crypto.fips.InterceptingProvider)
  PROVIDER[2]: SUN (com.arcsight.common.crypto.fips.InterceptingProvider)
  PROVIDER[3]: SunRsaSign (com.arcsight.common.crypto.fips.InterceptingProvider)
  PROVIDER[4]: SunJCE (com.arcsight.common.crypto.fips.InterceptingProvider)

[2010-02-03 07:13:38,745][INFO ][default.com.arcsight.agent.cg.b][init] Found Obfuscation key file at [/root/ArcSi
[2010-02-03 07:13:38,745][INFO ][default.com.arcsight.common.config.PropertiesFileConfiguration][customInitializat
[2010-02-03 07:13:38,786][INFO ][default.com.arcsight.server.management.ManagementAgent][createMBeanServer] Using
[2010-02-03 07:13:38,787][INFO ][default.com.arcsight.server.management.ManagementAgent][registerMBean] Registere
[2010-02-03 07:13:39,157][INFO ][default.com.arcsight.agent.cg.b][init] Found the key for [Obfuscation]
[2010-02-03 07:13:39,269][INFO ][default.com.arcsight.server.management.ManagementAgent][registerMBean] Registere
[2010-02-03 07:13:39,389][INFO ][default.com.arcsight.server.management.ManagementAgent][registerMBean] Registere
[2010-02-03 07:13:39,395][INFO ][default.com.arcsight.agent.zg][init] Initializing Agent Framework Version [4.7.8.
[2010-02-03 07:13:39,398][INFO ][default.com.arcsight.agent.zg][init] {ArcSight Home=/root/ArcSightSmartConnectors
[2010-02-03 07:13:39,399][INFO ][default.com.arcsight.common.snmp.SNMPInitializer][init] Initializing SNMP system
[2010-02-03 07:13:39,399][INFO ][default.com.arcsight.agent.zg][init] Agent Framework Version [4.7.8.5455.0] (A545
[2010-02-03 07:13:39,408][INFO ][default.com.arcsight.agent.loadable.serializer._AgentCSVConcreteBroker][CSVConcre
[2010-02-03 07:13:39,696][INFO ][default.com.arcsight.common.serialize.csv.CSVAlertSerializer][<static>] Could not
[2010-02-03 07:13:39,737][INFO ][default.com.arcsight.common.serialize.csv.CSVURLHandler][addSerializer] Overridin
[2010-02-03 07:13:39,740][INFO ][default.com.arcsight.common.serialize.StreamHandler][_buildContentHandlerMap] Add
[2010-02-03 07:13:39,741][INFO ][default.com.arcsight.common.serialize.binary.BinaryConcreteBroker][BinaryConcrete
[2010-02-03 07:13:39,760][INFO ][default.com.arcsight.common.serialize.StreamHandler][_buildContentHandlerMap] Add
[2010-02-03 07:13:39,778][INFO ][default.com.arcsight.agent.dd.i][getAUPFileData] Inspecting content file [/root/A
[2010-02-03 07:13:39,779][INFO ][default.com.arcsight.agent.dd.i][init] Content manager initialized, File [/root/A
[2010-02-03 07:13:39,803][INFO ][default.com.arcsight.agent.dd.c][getInputStream] Resource [registry.properties] f
[2010-02-03 07:13:39,805][INFO ][default.com.arcsight.common.config.AgentPropertiesFileConfiguration][loadDefaultF
[2010-02-03 07:13:39,806][INFO ][default.com.arcsight.agent.dd.c][getInputStream] Resource [registry.properties] r
[2010-02-03 07:13:39,806][INFO ][default.com.arcsight.agent.ff.a][initializeCachedAgentDetails] Loading registry c
[2010-02-03 07:13:39,852][INFO ][default.com.arcsight.agent.zg][init] Running in Fips mode
[2010-02-03 07:13:39,854][INFO ][default.com.arcsight.agent.ki][run] Memory Usage: 5Mb out of 7Mb
[2010-02-03 07:13:39,885][INFO ][default.com.arcsight.agent.ki][logStatus] Transport flow status:
[2010-02-03 07:13:39,887][WARN ][default.com.arcsight.agent.th][start] No Connectors configured.
[2010-02-03 07:13:39,889][INFO ][default.com.arcsight.agent.ki][logStatus] Other status:
```

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



| Time | Connector | Status |
|---|---|---|
| 2/3 7:49:35 | testing | Response received. |

From Connector:: testing (3wQJ0ICYBABCCuaoiojSU1g==)

```
Status Generated: Wed Feb 03 07:49:35 CST 2010
Memory Usage: 89Mb out of 243Mb

Agent Type.................................syslog
Agent Version..............................4.7.8.5455.0
FIPS Enabled...............................true
Host Address...............................10.11.194.217
Host Name..................................SUSE10SP2-64-217.site
Queue Drop Count...........................0.0
Queue Rate.................................-1.0
Queue Rate(SLC)............................0.0
activeThreadCount..........................49
ipaddress..................................(ALL)
port.......................................514
protocol...................................UDP
```