

Configuration Guide

Logger SmartConnector™ for HP Operations Manager Incident Web Service

October 12, 2012



Configuration Guide

Logger SmartConnector™ for HP Operations Manager Incident Web Service

October 12, 2012

Copyright © 2003-2012 Hewlett-Packard Development Company, L.P. Confidential computer software. Valid license from HP 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.

The information contained herein is subject to change without notice. The only warranties for HP 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. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks and acknowledgements:

<http://www.arcsight.com/copyrightnotice>.

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
10/12/2012	First release of Logger SmartConnector documentation supporting Logger Downloadable Version.

Logger SmartConnector for HP Operations Manager Incident Web Service

This guide provides information for installing the SmartConnector for HP Operations Manager Incident Web Service and configuring the device for event collection. This connector supports HP Operations Manager for Windows v9.0 and 8.16 (patch level 90), Operations Manager for Unix v9.10, and Operations Manager for Linux v9.10.

ArcSight Logger is a log management solution optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. This SmartConnector supports Logger 5.3 Downloadable Version.

Product Overview

HP Operations Manager (HP OM) provides comprehensive event management, proactive performance monitoring, and automated alerting, reporting, and graphing for operating systems, middleware, and applications. HP Operations Manager software acts as the consolidated enterprise operations console for your IT infrastructure. It monitors both physical and virtual servers to identify the cause of event storms, allowing faster time to resolution.

The messages generated by HP OM are retrieved through HP OM's Incident Web Service and forwarded into the ArcSight System.

Configure Operations Manager for Event Collection

The SmartConnector can validate Operation Manager's authentication certificate. To operate in this configuration, first get the certificate from Operations Manager, then import it into the SmartConnector Java Runtime Environment (JRE) during the connector installation process, prior to running the SmartConnector.



The following steps presume you have configured Operations Manager to let the SmartConnector communicate with it. If you have not done so, see your HP documentation for information about the configuration of access lists or allowed hosts.

Obtain the Authentication Certificate

HP recommends that you connect to the HP OM Web Services using HTTPS connections, which require a suitable certificate on the server. Although the Incident Web Service can listen to both HTTP and HTTPS at the same time, the SmartConnector always attempts to connect through HTTPS. Both the Incident Web Service and its certificate are components generally installed on the HP OM server by default. The port that the service uses for HTTPS communication depends upon the configuration of the HP OM server. The default HTTPS port number on HP OM on UNIX or Linux is 8444. For Windows, the default port is 443.

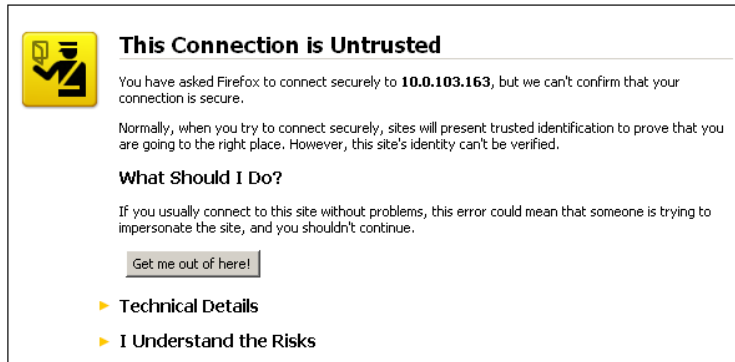
For further security, HP recommends you verify the hostname and certificate for each HTTPS connection. To verify the certificate for an HTTPS connection, the client system must trust the server's certificate. You will export the server's certificate and import it to the SmartConnector system.

On Windows

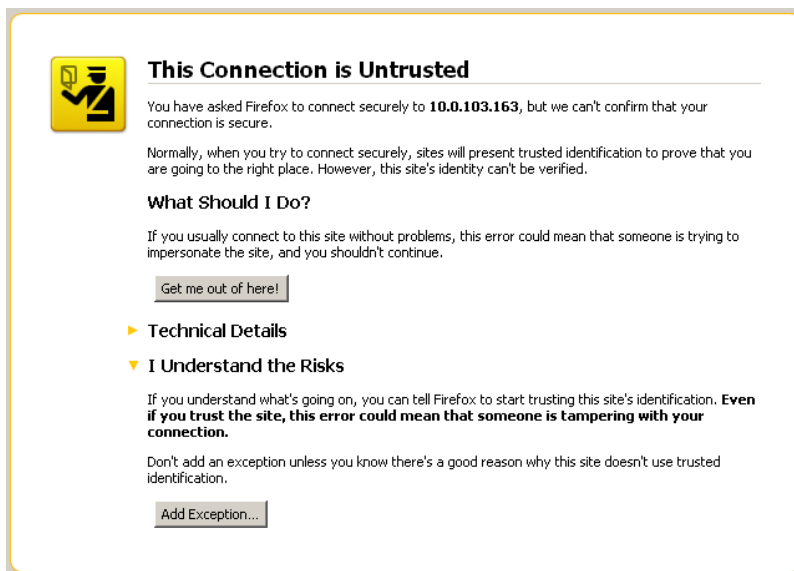
The examples in the following procedure use Mozilla Firefox.

To export the Incident Web Service certificate using Windows:

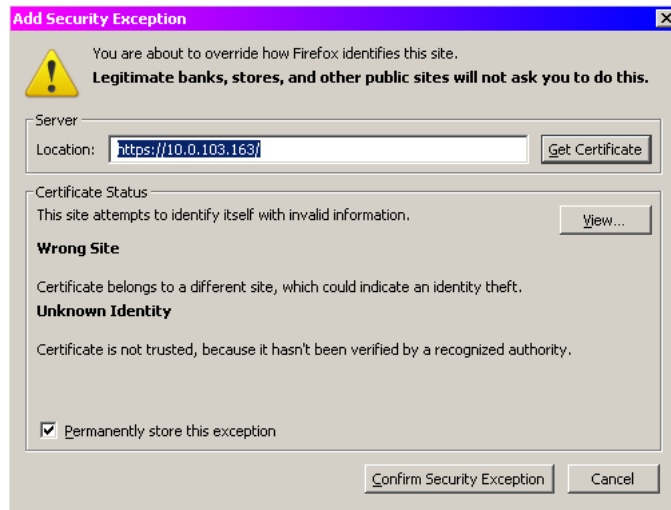
- 1 Enter the HP OM server IP address in your browser.



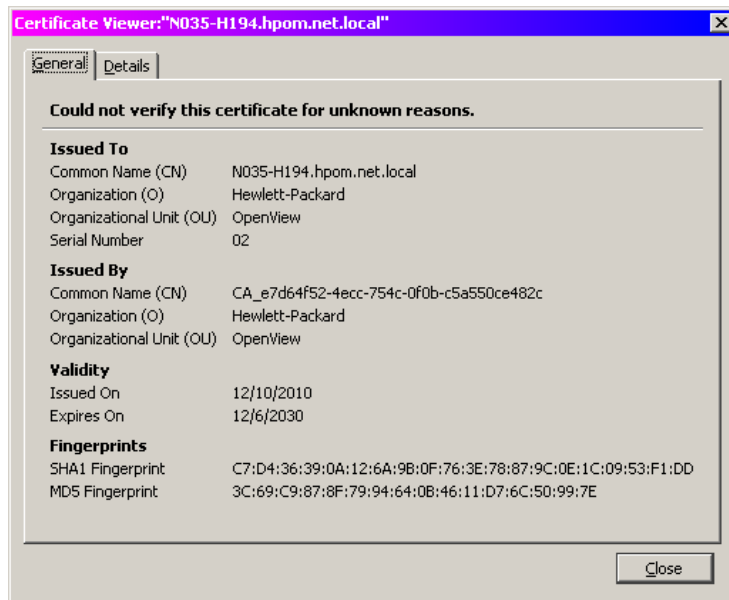
- 2 Click **I Understand the Risks**.



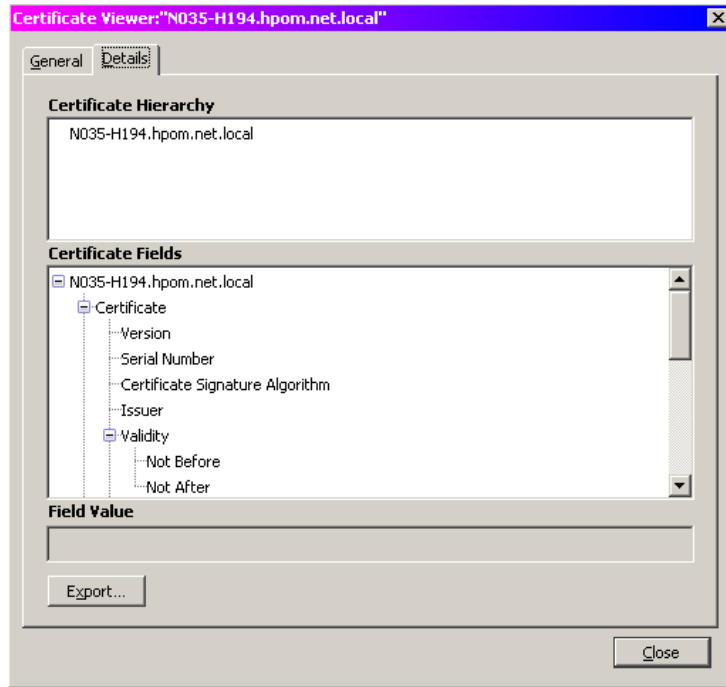
- 3 Click **Add Exception...**



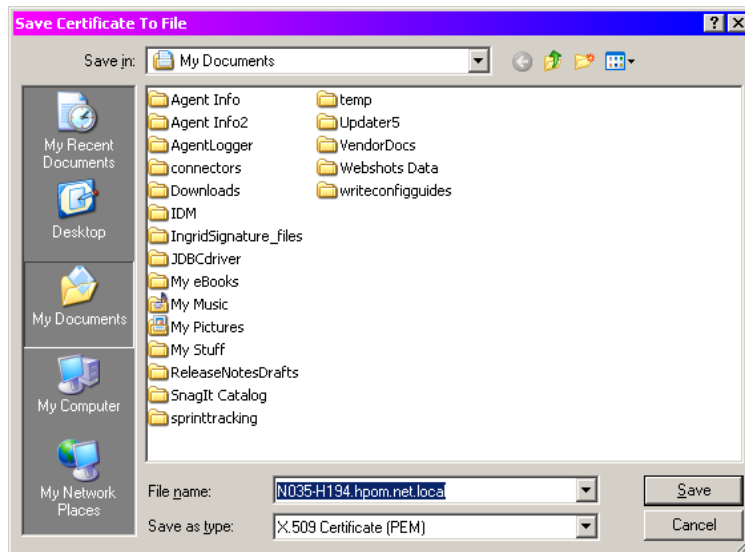
4 Click **View....**



5 Click the **Details** tab.



6 Click **Export...**



7 Navigate to the folder into which you want to save the certificate; click **Save**.

On Linux

To export the server's certificate from your management server:

1 Open a shell and navigate to the directory containing the keystore file:

```
/var/opt/OV/certificates/tomcat/b
```

2 Issue the following command to determine the keystore list containing the certificate:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -list
```

- 3 When prompted, enter the default password `changeit`. Keystore information such as shown in the following example is displayed.

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
ovtomcatb, Dec 15, 2010, PrivateKeyEntry,
Certificate fingerprint (MD5):
36:FC:82:FB:46:E0:54:3B:FB:D8:18:F6:53:C8:9F:4A
```

- 4 Export the certificate using the following command:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -export -alias
<keystorename> -file /tmp/<server.cer>
```

where `<keystorename>` is the keystore name and `<server.cer>` is the name of the certificate file. For example:

```
/opt/OV/nonOV/jre/b/bin/keytool -keystore tomcat.keystore -export -alias
ovtomcatb -file /tmp/hpoml910.cer
```

- 5 Enter the default password `changeit` and the certificate will be saved into the certificate file you specified under `/tmp`. You will receive a message such as the following:

```
Certificate stored in file </tmp/hpoml910.cer>
```

You will import the certificate during the SmartConnector installation process.

Install the SmartConnector

Before you install any SmartConnectors, make sure that the ArcSight Logger product with which the connectors will communicate has already been installed correctly.

For complete product information, read the *ArcSight Logger Administrator's Guide* before installing a new SmartConnector. If you are adding a connector to the Connector Appliance, see the *ArcSight Connector Appliance Administrator's Guide* for instructions, and start the installation procedure at step 3.

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the HP SSO and Protect 724 sites.

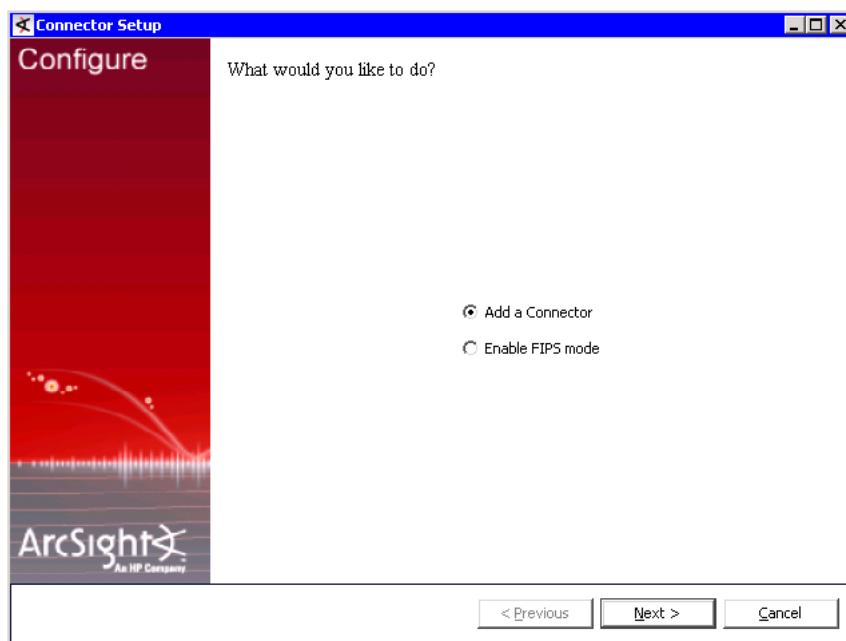
- 1 Download the SmartConnector executable for your operating system from the HP SSO site.

- 2 Start the SmartConnector Installer by running the executable.

Follow the installation wizard through the following folder selection tasks and installation of the core connector software:

Introduction
 Choose Install Folder
 Choose Install Set
 Choose Shortcut Folder
 Pre-Installation Summary
 Installing...

- 3 When the installation of SmartConnector core component software is finished, the following window is displayed.



The following steps are for importing the server certificate to the connector's Local Java Run Environment; this example is for Windows systems. If you are making use of Linux or Unix, change the command to reflect your \$ARCSIGHT_HOME and change \ to /.

- A Click **Cancel** to exit the configuration wizard.
- B From `$ARCSIGHT_HOME\current\user\agent`, create an `hpom` subdirectory; copy the certificate file you obtained during HPOM configuration (for example, `server.cer`) and save it into this subdirectory.
- C From `$ARCSIGHT_HOME\current\bin`, execute the **keytool** application to import the `server.cer` certificate. Enter this **keytool** command on a single line.

```
arcsight agent keytool -import -alias server_1_1_1_1 -file
<\user\agent\hpom\server.cer> -store clientcerts
```


where `<\user\agent\hpom\server.cer>` is the path and name of the HPOM Incident Web Service's certificate file.

- D** Following the prompts, answer **yes** for the prompt **Trust this certificate?**.

```
Trust this certificate? [no]: yes
```

The certificate is added to keystore.

- E** Verify the imported certificate by entering the following command from `$ARCSIGHT_HOME\current\bin`:

```
arcsight agent keytool -list -store clientcerts
```

The new certificate (for example, alias=server_1_1_1_1) is displayed in the list.

- F** From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

- 4** Select **Add a Connector** and click **Next**.

- 5** Select **HP Operations Manager Incident Web Service** and click **Next**.

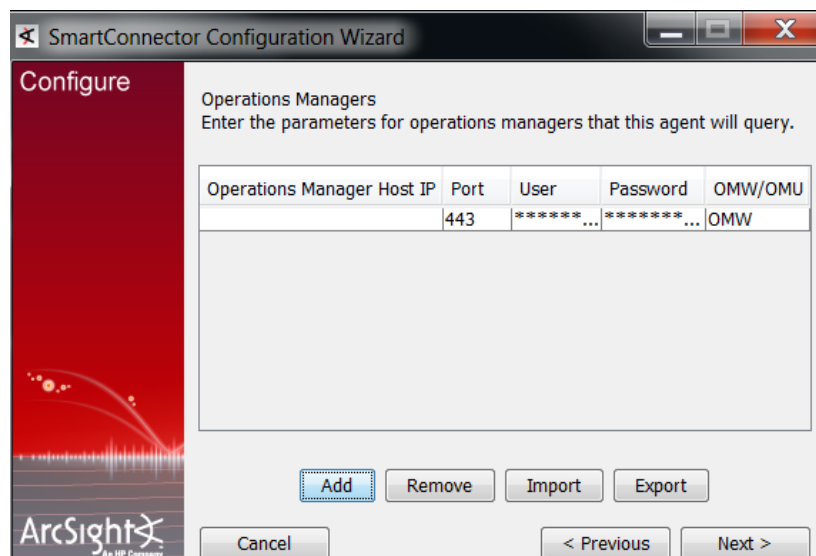
Depending upon your platform, choose between the required connector types.

For **Windows** platforms, **Syslog Daemon** is the only available option.

For **Linux** platforms, select **Syslog Daemon**, **Syslog File**, or **Syslog Pipe**.

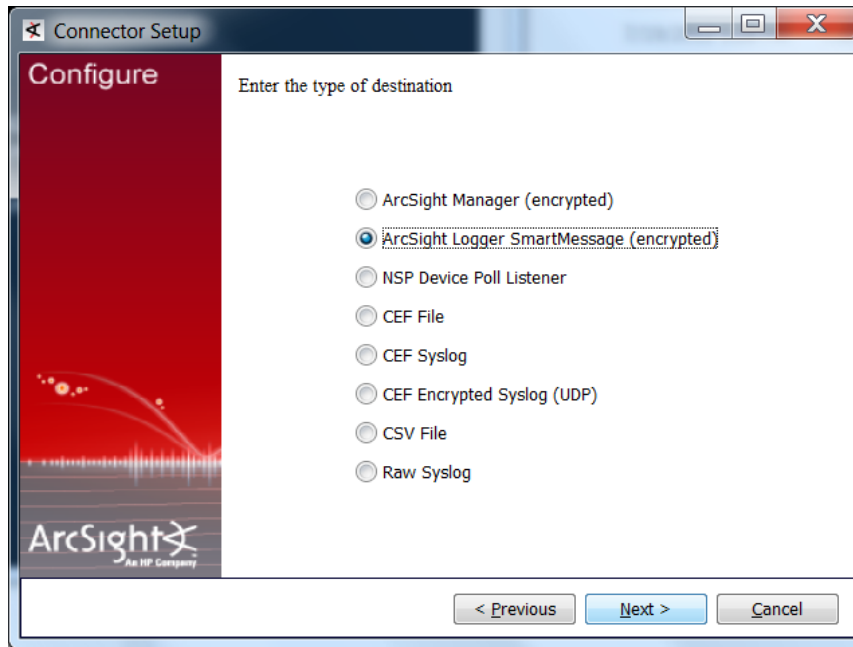
- 6** Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



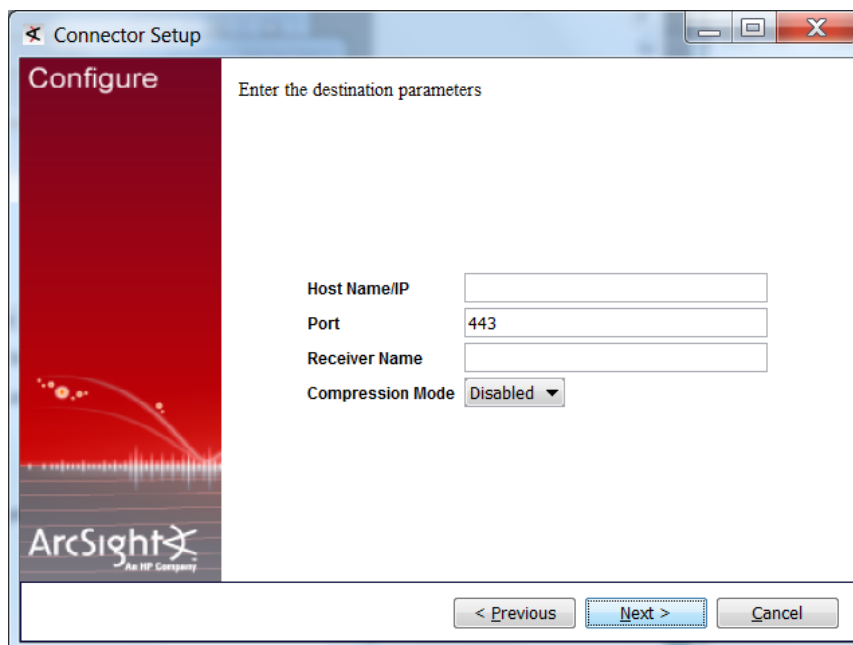


Parameter	Description
Enable Certificate Validation	Specify whether the SmartConnector is to enable the validation of HP Operations Manager certificate for the client. Certificate validation is enabled (true) by default.
Enable Hostname Validation	Specify whether the SmartConnector is to enable the validation of HP Operations Manager hostname. Hostname validation is enabled (true) by default.
Operations Manager Host IP	Enter the host name or IP address of the HP OM server.
Port	Specify the port to which the Incident Web Service is listening. To detect whether the Incident Web Service is listening, enter the following URL in your browser. You should receive a response from the service. https://<HPOM server IP>:<HPOM Incident Web Service Listening Port, by default 443>/opr-webservice/incident.svc.
User	Enter the user name for the Incident Web Service user.
Password	Enter the password for the Incident Web Service user.
OMW/OMU	Select OMW for Operations Manager for Windows; select OMU for Operations Manager for Unix. Operations Manager for Linux is the currently supported Unix platform.

- When the destination window is displayed, make sure **ArcSight Logger SmartMessage (encrypted)** is selected and click **Next**. For information about the other destinations listed, see the *ArcSight SmartConnector User's Guide* as well as the *Administrator's Guide* for your ArcSight product.

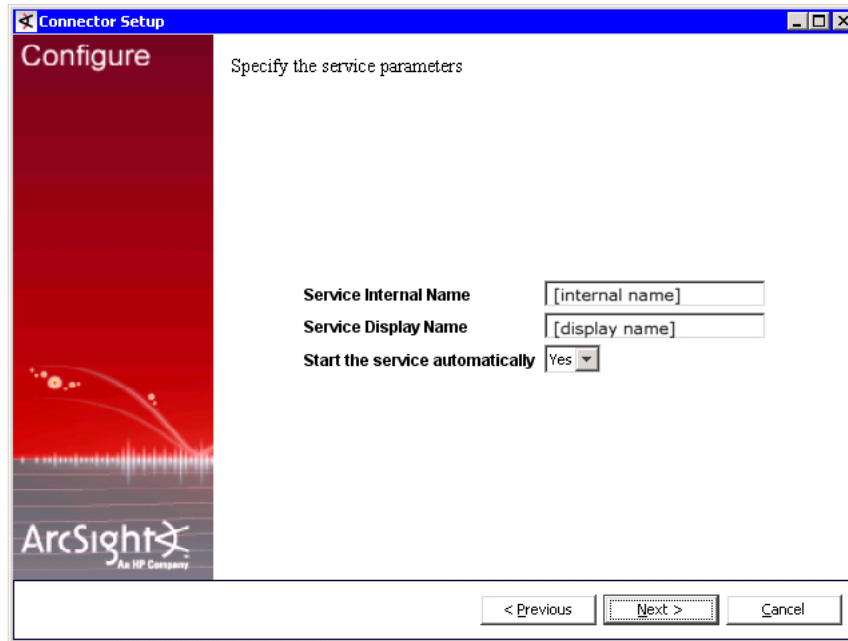


- 8 Before proceeding with step 9, set up the **SmartMessage Receiver** from Logger (see the *ArcSight Logger Administrator's Guide* for detailed instructions).
- 9 From the Configuration Wizard, enter the Logger **Host Name/IP** and **Port**. Make sure the port number is the same that you used to set up your Logger. For the **Receiver Name**, enter the Receiver name you created in the previous step so that Logger can listen to events from this SmartConnector. Click **Next**.



- 10 Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**; the connector starts the registration process.

- 11 The **Add connector Summary** is displayed; review and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 12 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, skip step 12. If you choose to run the connector as a service, the wizard prompts you to define service parameters.



- 13 Enter the service parameters and click **Next**. The **Install Service Summary** window is displayed.
- 14 Click **Next**.

To complete the installation, choose **Exit** and click **Next**.

For some SmartConnectors, a system restart is required before the configuration settings you made take effect. If a **System Restart** window is displayed, read the information and initiate the system restart operation.



Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *HP ArcSight SmartConnector User's Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Limit Message Type (optional)

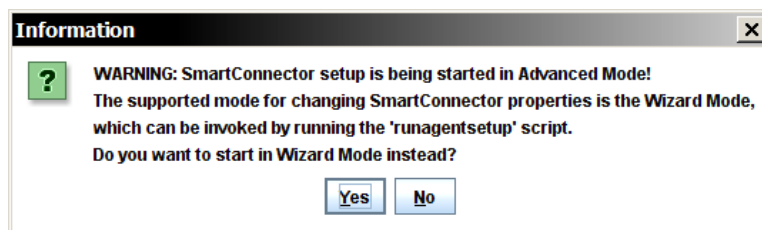
By default, the connector deals with all open, closed, and work in progress message types. To limit the message types collected, you can change this setting to **open**, **closed**, or **work in progress** to limit the connector to deal with only one type of message.

To make changes to these parameters:

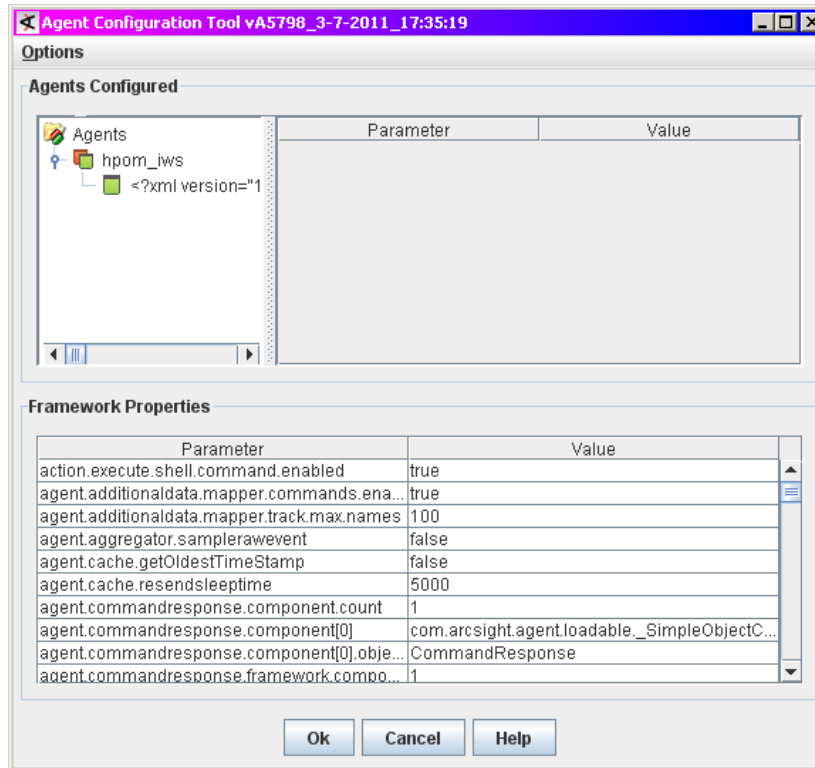
- 1 From the `$ARCSIGHT_HOME\current\bin` directory in a DOS command window enter:

```
arcsight connectorsetup
```

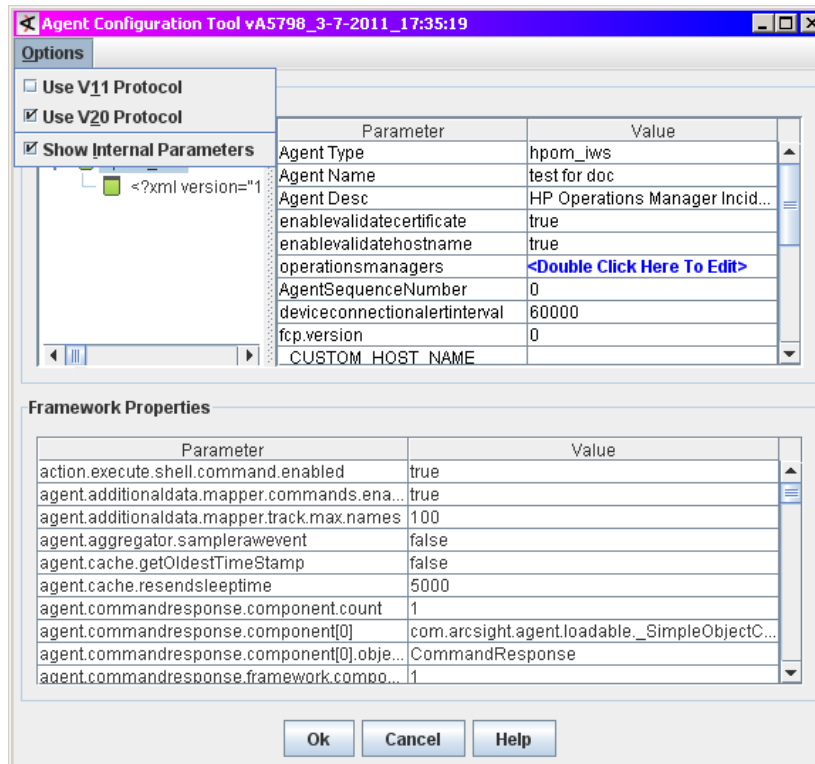
- 2 When the following message is displayed, click **No**.



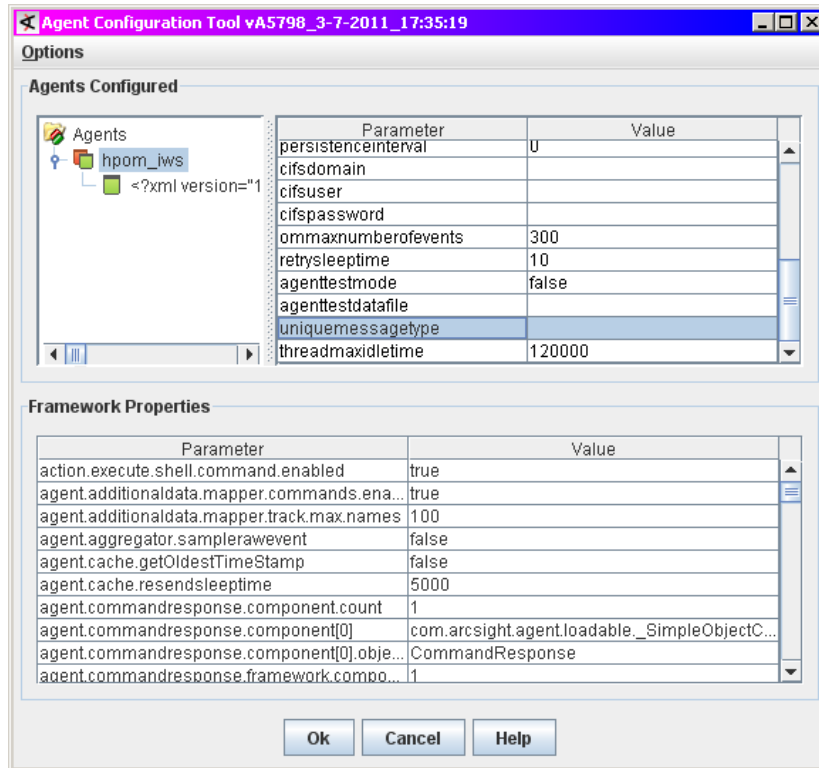
- 3 The Agent Configuration Tool window is displayed. Select the HPOM connector:



- From the **Options** menu, select **Show Internal Parameters**.



The advanced configuration parameters for the connector are displayed as shown in the following figure.



- 5 Make changes to the new parameters as desired; click OK to exit the Agent Configuration window.