Hewlett Packard
Enterprise

# HPE Security ArcSight Connectors

## SmartConnector for Sun ONE Web Access Server File (Legacy)

## Configuration Guide

May 15, 2017

**Configuration Guide**

**SmartConnector for Sun ONE Web Access Server File (Legacy)**

May 15, 2017



**Warranty**



**Restricted Rights Legend**



## Revision History

| Date | Description |
|---|---|
| 05/15/2017 | Marked connector as Legacy; use the SmartConnector for Sun ONE Web Access Server Multiple File. |
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 05/15/2012 | Added new installation procedure. |
| 02/11/2010 | Added support for FIPS Suite B and CEF File transport. |
| 06/30/2009 | Updated log mappings information and global update to installation procedure. |
| 03/01/2008 | Updated installation procedure. |
| 09/20/2007 | General content update. |
| 03/31/2006 | Updated installation and configuration information. |
| 01/19/2005 | Added the specific log format the SmartConnector can accept as well as Troubleshooting. |
| 12/06/2004 | First release of SmartConnector documentation. |

# SmartConnector for Sun ONE Web Access Server File (Legacy)

This guide provides information for installing the SmartConnector for Sun ONE Web Access Server File and configuring it for event collection. Sun ONE Web Access Server Version 6.0 SP8 is supported.

## Product Overview

Sun ONE Web Server (formerly iPlanet) provides organizations with a single deployment platform for Web services, JavaServer Pages (JSP) and Java Servlet technologies, Microsoft Active Server Pages, PHP, and CGI.

## Configuring Sun ONE Directory Server to Send Events

This section provides instructions for configuring the Sun ONE Web Server log files for ArcSight SmartConnector collection.

To configure Sun ONE Web Server to send events to the SmartConnector:

1. From the main menu, select the **Preferences** tab, then select **Logging Options**.
2. Under **Format**, make sure the option **Use Common Logfile Format** is selected.
3. Click the **OK** button at the bottom of the page.

The SmartConnector currently supports only the Common Log Format with the following fields logged in the following order. Future SmartConnector releases will support logging of other fields and a flexible logging format.

- Host Name or IP Address of the Client
- RFC 931 Identify
- User Name
- Date and Time of Request
- Request (Request Method followed by the URL)
- Protocol (Request Protocol and Version)
- Status Code
- Bytes Transferred
- User Agent (Optional. This field may be configured to be logged.)

## Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

## Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

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

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

## Install Core Software

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 HPE SSO and Protect 724 sites.

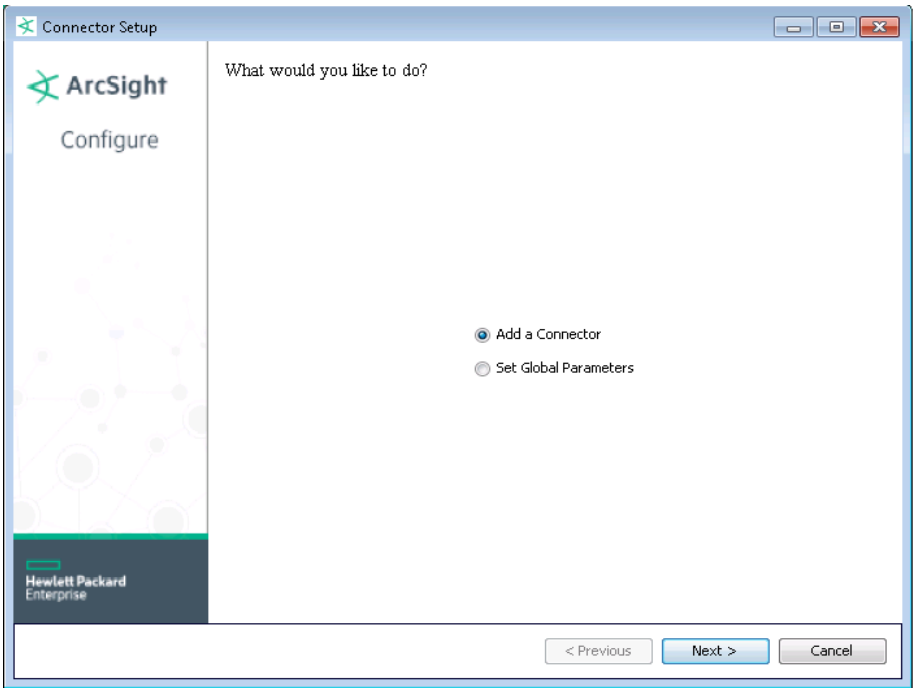
**1** Download the SmartConnector executable for your operating system from the HPE SSO site.

**2** Start the SmartConnector installation and configuration wizard by running the executable.

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

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

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




## Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

| Global Parameter | Setting |
|---|---|
| Set FIPS mode | Set to 'Enable' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disable'. |
| Set Remote Management | Set to 'Enable' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disable'. |
| Remote management listener port | The remote management device will listen to the port specified in this field. The default port number is 9001. |
| Preferred IP Version | If both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. When both values are present, the initial setting is IPv4. |

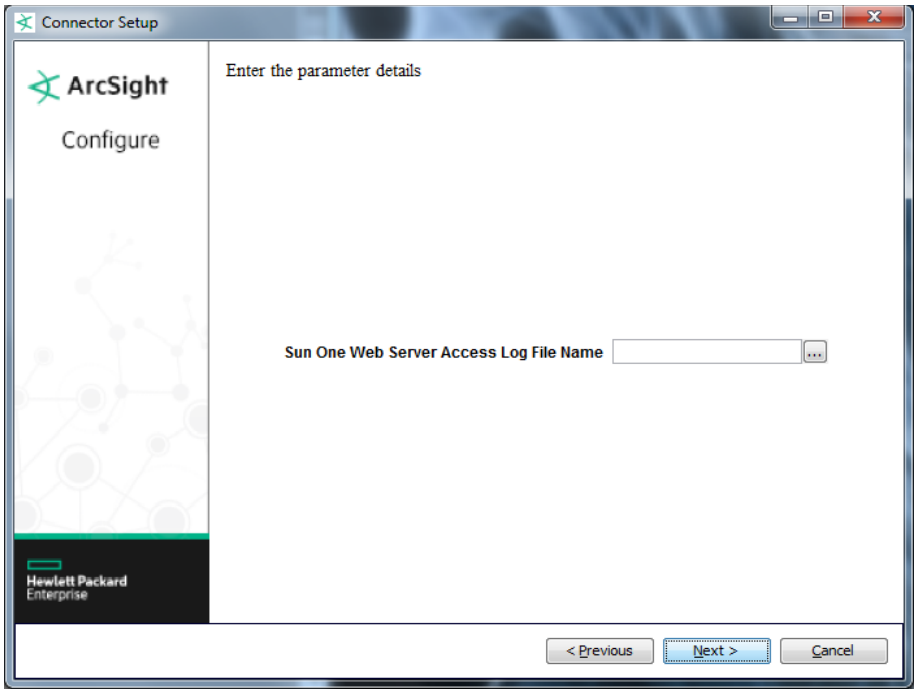
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to the "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

## Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.

2. Select **Sun ONE Web Server Access File** and click **Next**.

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




| Parameter | Description |
|---|---|
| Access Log File Name | Complete path and name of the directory containing the Access log files. |

## Select a Destination

1 The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.

2 Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.

3 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.

4 If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

## Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2. 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, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4. Click **Next** on the summary window.

5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

## 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 *ArcSight SmartConnector User 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.

## Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

### Sun ONE Web Server Access Log Mappings to ArcSight ESM Fields

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Application Protocol | The request protocol and version |
| Bytes Out | Bytes Transferred |
| Device Event Class Id | HTTP status code |
| Device Receipt Time | Time the URL was accessed |
| Name | HTTP Request |

| ArcSight ESM Field | Device-Specific Field |
|---|---|
| Request Client Application | HTTP User Agent |
| Request Method | The HTTP method that was requested |
| Request URL | URL that was requested |
| Source Address | IP Address of the accessing machine |
| Source Host Name | Host name of the accessing machine |

## Connector Verification and Troubleshooting

**SmartConnector unable to parse the access log.**

Doublecheck the logging format configured for your Sun ONE Web Server under **Log Preferences**. Make sure that only Common Log Format is selected with or without the optional user agent.

**SmartConnector not picking up events from all Sun ONE Web Server instances.**

The SmartConnector can only work with the access log of one instance of the Sun ONE Web Server. A separate SmartConnector is to be installed for each separate instance of the Web Server you may be running under your chosen Sun ONE Web Server deployment.