**Hewlett Packard Enterprise**

# HPE Security ArcSight Connectors

SmartConnector for Squid Web Proxy Server
File

Configuration Guide

November 30, 2016

**Configuration Guide**

**SmartConnector for Squid Web Proxy Server File**

November 30, 2016

## Revision History

| Date | Description |
|---|---|
| 11/30/2016 | Updated installation procedure for setting preferred IP address mode. |
| 09/30/2015 | Added support for versions 2.7 and 3.5. |
| 05/15/2012 | Added new installation procedure. |
| 02/11/2010 | Added support for FIPS Suite B and CEF File transport. |
| 06/30/2009 | Global update to installation procedure for FIPS support. |
| 03/01/2008 | Updated installation procedure. |
| 09/20/2007 | First edition of this Configuration Guide. |

# SmartConnector for Squid Web Proxy Server File

This guide provides information for installing the SmartConnector for Squid Web Proxy Server File and configuring the device for event collection. Squid 2.6.STABLE9, 2.7, and 3.5 are supported.

## Product Overview

The Squid Web Proxy Server acts as an agent, accepting requests from clients (such as browsers) and passing them to the appropriate Internet server. It stores a copy of the returned data in an on-disk cache. Squid's real benefit is displayed when the same data is requested multiple times, since a copy of the on-disk data is returned to the client, speeding up Internet access and saving bandwidth.

## Configuration

All Squid configuration files are kept in the directory `/usr/local/squid/etc`. The configuration file is the `squid.conf` file.

Squid access log files log client request activities. These activities are logged to the specified file using the specified format.  The `squid` logformat is required for the ArcSight SmartConnector to read the log files.  (This is defined using the `logformat` parameter in `squid.conf`).  The location of the access log file is determined by the `access_log` parameter in the Squid configuration file.

The suggested configuration is as follows:

`access_log /usr/local/squid/var/logs/access.log squid`

where:

`access_log` is the LOGFILE parameter

`/usr/local/squid/var/logs/access.log` is the location and name of the log file (required during SmartConnector installation)

`squid` is the name of the logformat, which should be the default format defined as follows:

`logformat squid  %ts.%03tu %6tr %>a %Ss/%03Hs %<st %rm %ru %un %Sh/%<A %mt`

The SmartConnector will not be able to read the log file if the `logformat` is not this value. See the latest changes to the Squid log format at:  http://www.squid-cache.org/Doc/config/logformat/

| Format Code | Meaning |
| --- | --- |
| >a | Client source IP address |
| <A | Server IP address or peer name |
| ts | Seconds since epoch |
| tu | Subsecond time (milliseconds) |
| tr | Response time (milliseconds) |
| un | User name |
| Hs | HTTP status code |

| Format Code | Meaning |
| --- | --- |
| Sh | Squid hierarchy status (DEFAULT_PARENT, etc.) |
| mt | MIME content type |
| rm | Request method (GET/POST, etc.) |
| ru | Request URL |
| <st | Reply size including HTTP headers |
| <sS | Upstream object size |
| % | A literal % character |

See the Squid Configuration Manual for LOGFILE Options at http://ww.squid-cache.org/Versions/v2/2.6/cfgman.

# Install the SmartConnector

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

> Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

## 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). This configuration guide takes you through the installation process with **ArcSight Manager (encrypted)** as the destination.

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:
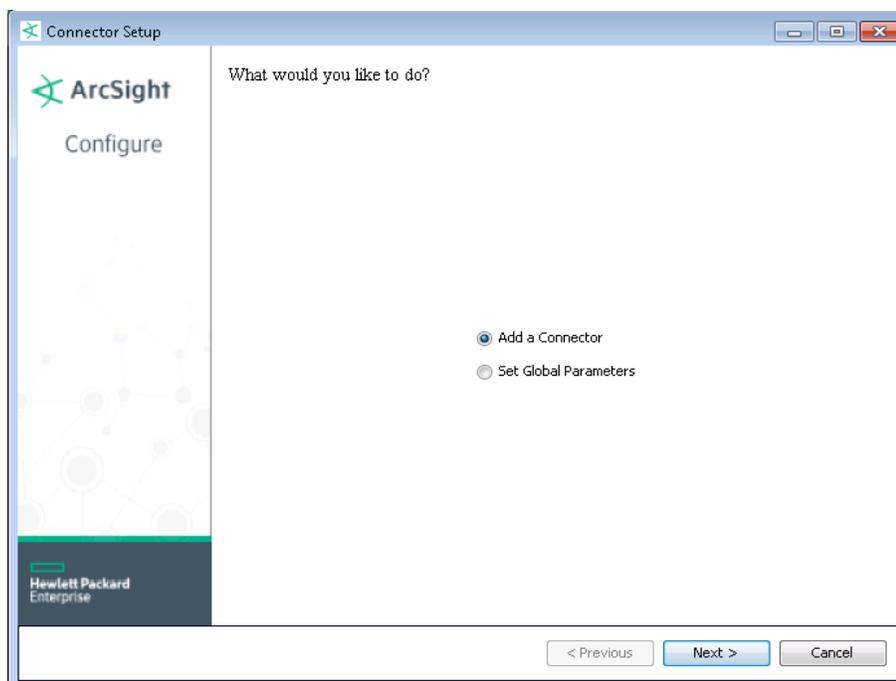


## Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, 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 **Squid Web Proxy Server File** and click **Next**.

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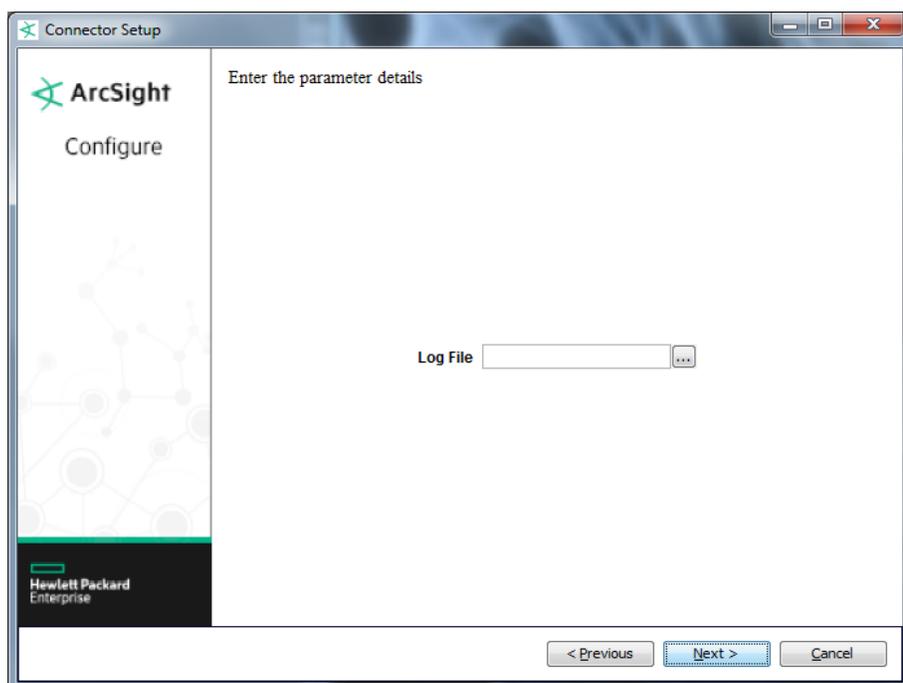


| Parameter | Description |
| --- | --- |
| Log File | Enter the path to and name of log file to be accessed by the SmartConnector. |

## Select a Destination

1   The next window asks for the destination type; make sure **ArcSight Manager (encrypted)** is selected and click **Next**. (For information about this destination or any of the other destinations listed, see the *ArcSight SmartConnector User Guide*.)

2   Enter values for the **Manager Host Name**, **Manager Port**, **User** and **Password** required parameters. This is 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**  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 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.

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.

### Squid Web Proxy Server Mappings to ArcSight ESM Fields

| ArcSight ESM Field | Device-Specific Field |
| --- | --- |
| ArcSight Severity | High when Device Severity = 400 – 599; Medium when Device Severity = 000,300 – 399; Low when Device Severity = 100 – 299 |
| Bytes Out | ReplySize |
| Destination Host Name | ServerIPOrPeerName |
| Destination User Name | UserName |
| Device Custom Number 1 | ResponseTime |
| Device Custom String 1 | SquidHierarchyStatus |
| Device Event Class ID | HTTPStatusCode |
| Device Product | 'Squid Web Proxy Server' |
| Device Receipt Time | Timestamp |
| Device Severity | HTTPStatus Code |
| Device Vendor | 'Squid' |
| File Type | MIMEContentType |
| Name | SquidRequestStatus |
| Request Method | RequestMethod |
| Request URL | RequestURL |
| Source Address | ClientSourceIP |