Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Cisco IronPort Web Security Appliance File

Configuration Guide

March 15, 2017

Configuration Guide

SmartConnector for Cisco IronPort Web Security Appliance File

March 15, 2017

Copyright © 2007 – 2017 Hewlett Packard Enterprise Development LP

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 Packard 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 Packard 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 Packard Enterprise Development LP copyrights, trademarks and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026.

Revision History

Date	Description
03/15/2017	Added support for version 10 (Apache and Squid formats only).
11/30/2016	Updated installation procedure for setting preferred IP address mode.
11/17/2015	Added support for version 8.5 (Apache and Squid formats only).Support ending for AsyncOS versions 5.5, 6.4, and 7.1.
08/15/2014	Added support for version 8.0.5.
03/29/2013	Added mappings for connector and device severity.
05/15/2012	Added new installation procedure.
03/30/2012	Added support for version 7.1. Updated and added mappings.
09/24/2010	Added support for Web Security versions 5.5 and 6.3; support now generally available for version 6.1.
02/11/2010	Added support for FIPS Suite B and CEF File transport.
11/11/2009	Added beta support for IronPort Web Security version 6.1, including support for W3C Extended Log format.
06/30/2009	Added global update to installation procedure.

SmartConnector for Cisco IronPort Web Security Appliance File

This guide provides information for installing the SmartConnector for Cisco IronPort Web Security Appliance File and configuring the device for event collection. Support for IronPort AsyncOS 8.0, 8.5, and 10 for Cisco Web Security Appliance is provided. AsyncOS 8.5 and 10 are supported for Apache and Squid formats only.

Product Overview

The Cisco IronPort Web Security appliances combine a high-performance security platform with a new scanning technology that enables signature-based spyware filtering. Robust management and reporting tools deliver ease of administration and complete visibility into threat-related activity.

The Cisco IronPort Web Security appliances let you create custom reports, configure custom log files, and view interactive data that you can use to monitor system activity and manage runtime events. The appliance also supports an alert engine framework that generates messages describing error conditions and the severity of each event.

IronPort Web Security Logging

For complete information about IronPort Web Security appliance logging, see the *Web Security Appliance User Guide*.

Log Types Supported

The S-series appliance provides several options for creating custom log files and configuring log file retrieval; this SmartConnector supports using SCP and FTP. Logging includes options for standard log types such as Apache, Squid, and Squid Detailed.

The ArcSight SmartConnector for Cisco IronPort Web Security Syslog supports Apache and Squid log formats for Access Log events. Squid Detailed format is not currently supported.

Log Subscriptions

You can subscribe to a variety of log files and customize the type of information that is recorded in each log. Use `System Administration -> Log Subscriptions` to configure the access log subscriptions and customize its log file settings.

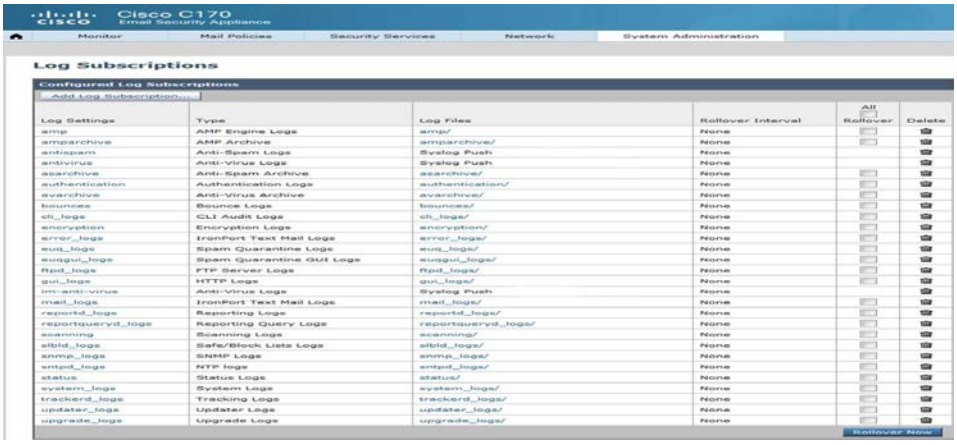
Note the location of the access log; this value will be needed during SmartConnector installation.

The S-series appliance can be configured to log various levels of system information. Options for logging include:

Level	Description
Critical	Logs error messages.
Warning	Logs system errors and system warnings.
Information	Provides a detailed record of system operations. This options is the default system setting for each log file.

Level	Description
Debug	Logs data that is useful for debugging system problems.
Trace	Provides a complete record of system operations and activity. This option is recommend for developers only.

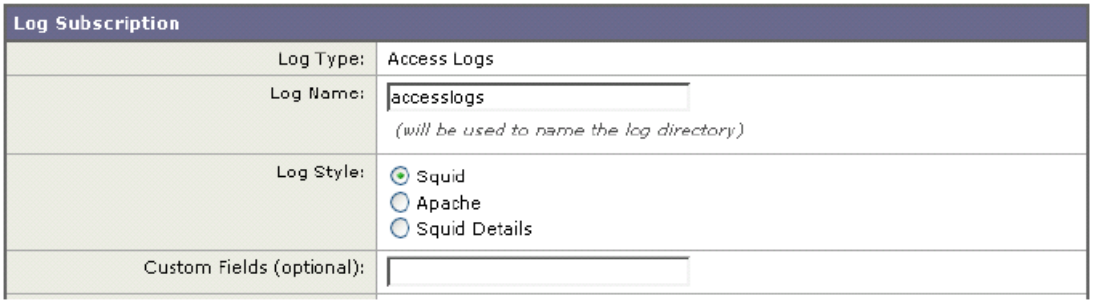
Use the `System Administration -> Log Subscriptions -> New Log Subscriptions` page to customize the level of information recorded in each log file.



Selecting the Log Format (Style)

Use the `System Administration -> Log Subscriptions -> Edit Log Subscription` page to configure custom formatting for access log file entries.

Click the log file name (`accesslogs`) on the **Log Subscriptions** page to access the Edit Log Subscription page.



Transaction Result Codes

The access log file provides a descriptive record of all Web Proxy filtering and scanning activity. Access log file entries display a record of how the appliance handled each transaction.

Transaction result codes in the access log file describe how the appliance resolves client requests. For example, if a request for an object can be resolved from the cache, the result code is TCP-HIT. However, if the object is not in the cache and the appliance pulls the object from an origin server, the result code is TCP_MISS. The following table describes transaction result codes. These codes are mapped to the ArcSight ESM Device Action field for each event.

Result Code	Description
TCP_HIT	The object requested was cached in memory.
TCP_IMS_HIT	The client sent an IMS (If-Modified-Since) request for an object and the object was found in the cache. The proxy responds with a 304 response.
TCP_MEM_HIT	The object was not found in the cache, so it was fetched from the origin server.
TCP_MISS	The object was not found in the cache and was fetched from an origin server.
TCP_REFRESH_HIT	The object was in the cache, but was stale. The proxy sent an IMS (If-Modified-Since) request to the origin server, the server confirmed that the object was not modified, and the stale object was served.
TCP_REFRESH_MISS	The object was in the cache, but was stale. The proxy sent an IMS request to the origin server and pulled a fresh copy of the object.
TCP_CLIENT_REFRESH	The client issued a Pragma: No-cache header and the object was pulled from the origin server.
TCP_DENIED	The client request was denied.
UDP_MISS	The object was fetched from the origin server.
NONE	There was an error in the transaction; for example, a DNS failure or a gateway timeout.

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.

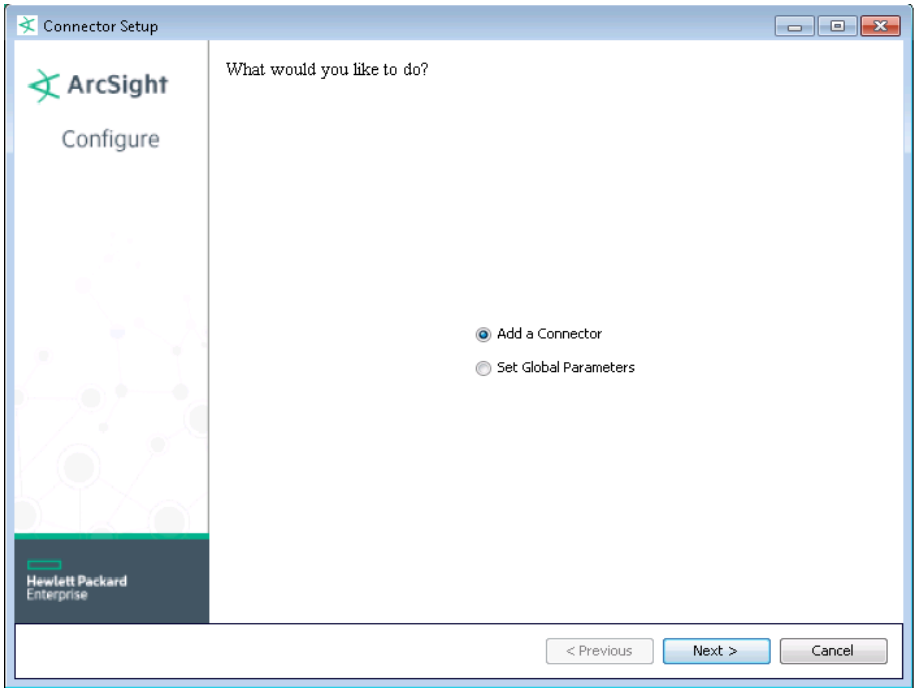
1 Download the SmartConnector executable for your operating system from the HPE SSO site.

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)

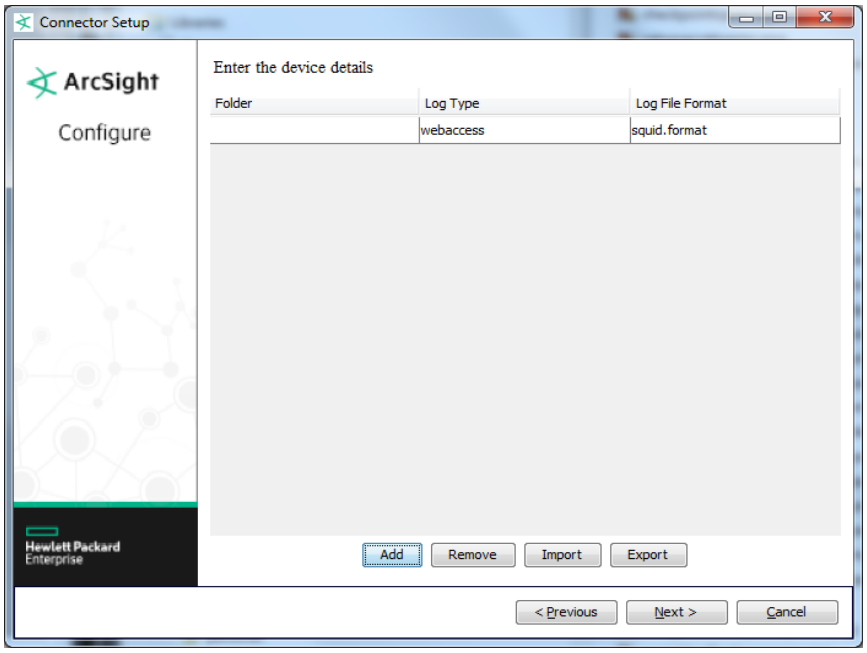
If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

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 **Cisco IronPort Web Security Appliance File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Enter the path to and name of the access log file folder.
Log Type	This SmartConnector currently supports 'webaccess' logs.
Log File Format	Enter the name of the log file format: squid.format, apache.format, or w3c_elf.format (W3C Extended Log Format). The default value is squid.format. (Version 8.5 and 10 support Apache and Squid formats only.)

You can click the 'Export' button to export the host name data you have entered into the able into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

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.

IronPort Web Security Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Additional data	threat-name
Additional data	threat-risk-ratio
Application Protocol	One of(protocol, request-line)
ArcSight (Connector) Severity	High = 400..603; Medium = 300..399; Low = 100..299, 000
Bytes In	total-bytes
Destination Host Name	One of (destination-hostname, data-source)
Destination Port	destination-port
Destination User Name	authenticated-user
Device Action	One of (action-taken, result-code)
Device Custom String 1	Referrer
Device Custom String 2	The URL category
Device Custom String 3	The Web Reputation Filter Score
Device Custom String 4	The Scanning Verdict information
Device Custom String 5	Hierarchy Retrieval
Device Custom String 6	Error Type
Device Event Class ID	http-response-code
Device Product	'IronPort Web Security Appliance'
Device Receipt Time	OneOfDateTime(timestamp,apache-timestamp)
Device Severity	http-response-code
Device Vendor	'CISCO'
External ID	transaction-id
File Type	content-type
Message	request-line
Name	One of (action-taken, result-code)
Request Client Application	user-agent
Request Cookies	cookie
Request Method	request-line
Request URL	request-line
Source Address	client-ip
Source User Name	x-suspect-user-agent

IronPort W3C Extended Log Format Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	One of (protocol, cs-protocol)
Bytes In	cs-bytes
Bytes Out	One of (sc-bytes, sc-body-size)
Destination Address	One of (cs-ip, s-ip)

ArcSight ESM Field	Device-Specific Field
Destination Host Name	s-computername
Device Action	sc-result-code
Device Event Class ID	sc-result-code
Device Process Name	s-sitename
Device Product	'IronPort Web Security Appliance'
Device Receipt Time	date, time
Device Vendor	'CISCO'
File Path	cs-uri-stem
Name	sc-result-code
Request Client Application	cs(User-Agent)
Request Method	cs-method
Request URL	cs-url
Source Address	c-ip
Source User Name	One of (cs-username, x-cache-user)