



ArcSight SmartConnectors

Software Version: 8.4.3

SmartConnector for Cisco IronPort Web Security Appliance File

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2007 – 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

- SmartConnector for Cisco IronPort Web Security Appliance File 4
- Product Overview 5
- IronPort Web Security Logging 6
 - Log Types Supported 6
 - Log Subscriptions 6
 - Selecting the Log Format (Style) 7
 - Transaction Result Codes 8
- Install the SmartConnector 10
 - Prepare to Install Connector 10
 - Install Core Software 11
 - Set Global Parameters (optional) 11
 - Select Connector and Add Parameter Information 13
 - Select a Destination 13
 - Complete Installation and Configuration 14
- Run the SmartConnector 15
- Device Event Mapping to ArcSight Fields 16
 - IronPort Web Security Mappings to ArcSight ESM Fields 16
 - IronPort W3C Extended Log Format Mappings 17
- Send Documentation Feedback 19

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.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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.
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.


Cisco C170
 Email Security Appliance

[Monitor](#)
[Mail Policies](#)
[Security Services](#)
[Network](#)
[System Administration](#)

Log Subscriptions

Configured Log Subscriptions
[Add Log Subscription...](#)

Log Settings	Type	Log Files	Rollover Interval	<input type="checkbox"/> All <input type="checkbox"/> Rollover	<input type="checkbox"/> Delete
amp	AMP Engine Logs	amp/	None	<input type="checkbox"/>	<input type="checkbox"/>
amparchive	AMP Archive	amparchive/	None	<input type="checkbox"/>	<input type="checkbox"/>
antispam	Anti-Spam Logs	Syslog Push	None	<input type="checkbox"/>	<input type="checkbox"/>
antivirus	Anti-Virus Logs	Syslog Push	None	<input type="checkbox"/>	<input type="checkbox"/>
asarchive	Anti-Spam Archive	asarchive/	None	<input type="checkbox"/>	<input type="checkbox"/>
authentication	Authentication Logs	authentication/	None	<input type="checkbox"/>	<input type="checkbox"/>
avarchive	Anti-Virus Archive	avarchive/	None	<input type="checkbox"/>	<input type="checkbox"/>
bounces	Bounce Logs	bounces/	None	<input type="checkbox"/>	<input type="checkbox"/>
cli_logs	CLI Audit Logs	cli_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
encryption	Encryption Logs	encryption/	None	<input type="checkbox"/>	<input type="checkbox"/>
error_logs	IronPort Text Mail Logs	error_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
euq_logs	Spam Quarantine Logs	euq_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
euqgui_logs	Spam Quarantine GUI Logs	euqgui_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
ftpd_logs	FTP Server Logs	ftpd_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
gui_logs	HTTP Logs	gui_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
im-anti-virus	Anti-Virus Logs	Syslog Push	None	<input type="checkbox"/>	<input type="checkbox"/>
mail_logs	IronPort Text Mail Logs	mail_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
reportd_logs	Reporting Logs	reportd_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
reportqueryd_logs	Reporting Query Logs	reportqueryd_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
scanning	Scanning Logs	scanning/	None	<input type="checkbox"/>	<input type="checkbox"/>
slbld_logs	Safe/Block Lists Logs	slbld_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
snmp_logs	SNMP Logs	snmp_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
sntpd_logs	NTP logs	sntpd_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
status	Status Logs	status/	None	<input type="checkbox"/>	<input type="checkbox"/>
system_logs	System Logs	system_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
trackerd_logs	Tracking Logs	trackerd_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
updater_logs	Updater Logs	updater_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>
upgrade_logs	Upgrade Logs	upgrade_logs/	None	<input type="checkbox"/>	<input type="checkbox"/>

Rollover Now

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.

Log Subscription	
Log Type:	Access Logs
Log Name:	<input type="text" value="accesslogs"/> <i>(will be used to name the log directory)</i>
Log Style:	<input checked="" type="radio"/> Squid <input type="radio"/> Apache <input type="radio"/> Squid Details
Custom Fields (optional):	<input type="text"/>

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.

Result Code	Description
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 OpenText SSO and Protect 724 sites.

- 1 Download the SmartConnector executable for your operating system from the OpenText 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, you can choose to specify the global parameters.

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:

Parameter	Setting
FIPS mode	Select 'Enabled' 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 'Disabled'.
Remote Management	Select 'Enabled' 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 'Disabled'.

Parameter	Setting
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	When 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. The initial setting is IPv4.

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the OpenText SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData.
Format Preserving Secret	Enter the secret configured for OpenText SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

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 proceed with "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 table 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,-50
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 Address	hostName
Device Custom Number2	total-bytes-used
Device Custom Number2 Label	Total Bytes Used
Device Custom String 1	referrer
Device Custom String 2	One of(thread-result-code,x-webcat-code-full,x-webcat-req-code-full)
Device Custom String 3	decoded-wbrs-score
Device Custom String 4	All of (thread-result-code, decoded-wbrs-score, verdict, threat-hname, threat-risk-ratio, spyid, trace-id)
Device Custom String 5	hierarchy-retrieval
Device Custom String 6	error-type
Device Event Class ID	http-response-code

ArcSight ESM Field	Device-Specific Field
Device Host Name	hostName
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)
Old File Name	x-req-dvs-scanverdict
Outcome	OneOf(Failure,Success,Null)
Reason	x-wbrs-threat-reason
Request Client Application	user-agent
Request Cookies	cookie
Request Method	request-line
Request URL	request-line
Source Address	client-ip
Source Port	source-port
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)
Destination Host Name	s-computername
Device Action	sc-result-code
Device Event Class ID	sc-result-code

ArcSight ESM Field	Device-Specific Field
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)

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on SmartConnector for Cisco IronPort Web Security Appliance File
(SmartConnectors 8.4.3)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!