Micro Focus Security ArcSight Connectors

SmartConnector for Cisco IronPort Email Security Appliance File

Configuration Guide

March 19

Configuration Guide

SmartConnector for Cisco IronPort Email Security Appliance File

March 19

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

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://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
03/19/2020	Added support for version 11.1.
10/17/2017	Added encryption parameters to Global Parameters.
06/15/2017	Added support for version 10.0.
02/15/2017	End of support for versions 7.5 and 7.6 due to end of support by vendor.
12/15/2016	Added support for version 9.7.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Added support for version 9.6.
09/30/2015	Added support for IronPort SyncOS for Email version 9.1. Support ending for SyncOS versions 4.7, 5.5, 6.1, 6.4, 7.0, and 7.5, due to end of life of these versions by vendor.
03/31/2015	Added support for version 8.5.
03/31/2014	Added support for version 8.0.
03/29/2013	Added GA support for version 7.6.
02/15/2013	Added support for version 7.5 and beta support for version 7.6. Updated mappings.
05/15/2012	Added new installation procedure.
09/24/2010	Added support for Email Security versions 6.4 and 7.0.

SmartConnector for Cisco IronPort Email Security Appliance File

This guide provides information for installing the SmartConnector for Cisco IronPort Email Security Appliance File and configuring the device for event collection. Cisco IronPort Email Security AsyncOS versions 8.0, 8.5, 9.6, 9.7, 10.0, and 11.1 are supported.

Product Overview

The Cisco IronPort Messaging Gateway appliance is designed to meet the email infrastructure needs of enterprise networks. The IronPort appliance eliminates spam and viruses, enforces corporate policy, secures the network perimeter, and reduces the Total Cost of Ownership (TCO) of enterprise email infrastructure. IronPort Systems combines hardware, a hardened operating system, application, and supporting services to produce a purpose-built, rack-mount server appliance dedicated for enterprise messaging.

Configuring the IronPort Device

For detailed information about Cisco IronPort appliance log files, see *IronPort AsyncOS Advanced User Guide for IronPort Appliances*.

Logfile Types

The following IronPort AsyncOS logfile types are supported by the SmartConnector for Cisco IronPort Email Security Multi-Folder:

IronPort Text Mail Logs

Text mail logs record information regarding the operations of the email system. For example, message receiving, message delivery attempts, open and closed connections, bounces, and others.

HTTP Logs

HTTP logs record information about the HTTP or secure HTTP services enabled on the interface. Because the graphical user interface (GUI) is accessed through HTTP, the HTTP logs are ostensibly the GUI equivalent of the CLI Audit logs. Session data (new session, session expired) and pages accessed in the GUI are recorded.

Log Retrieval

Log files can be retrieved based upon one of the following transfer protocols. You set the protocol while creating or editing the log subscription in the GUI or using the `logconfig` command during the log subscription process.

FTP Poll

This method involves a remote FTP client accessing the IronPort appliance to retrieve log files using an admin or operator user's username and password. When configuring a log

subscription to use the FTP poll method, specify the maximum number of log files to keep on hand. When the maximum number is reached, the system deletes the oldest file.

FTP Push

This method periodically pushes log files to an FTP server on a remote computer. The subscription requires a username, password, and destination directory on the remote computer. Log files are transferred based upon a rollover schedule you set.

SCP Push

This method periodically pushes log files to an SCP server on a remote computer. This method requires an SSH SCP server on a remote computer using the SSH1 or SSH2 protocol. The subscription requires a username, SSH key, and destination directory on the remote computer. Log files are transferred based upon a rollover schedule you set.

Filename and Directory Structure

IronPort AsynchOS creates a directory for each log subscription based upon the log subscription name. The actual name of the log file in the directory is composed of the log filename you specified, the timestamp when the log file was started, and a single-character status code. The filename of logs are made using the following formula:

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

Status codes can be `.c` (current) or `.s` (saved). Transfer only log files with the saved status.

Log Rollover and Transfer Schedule

Log subscriptions create and transfer (rollover) log files based upon the first user-specified limit reached: maximum file size or maximum time. Log subscriptions based upon the FTP poll transfer mechanism will create files and store them in the FTP directory on the IronPort appliance until they are retrieved or until the system needs more space for log files.

Log Subscriptions

Log subscriptions create log files that are rotated based upon a maximum time or maximum file size. A log subscription is either delivered to (pushed) or retrieved from (polled) another computer. The following list describes the fields on the Log Subscription window.

Log type

Defines the type of information recorded and the format of the log subscription.

Name

Nickname for the log subscription to be used for your future reference.

Log level

Sets the level of detail for each log subscription.

Retrieval method

Defines how the log subscription is to be transferred from the IronPort appliance.

Log filename
Used for the physical name of the file when written to disk. If multiple IronPort appliances are being used, the log filename should be unique to identify the system that generated the log file.

Maximum File Size
The maximum size the file can reach before rolling over.

Use the **Log Subscriptions** page on the **System Administration** tab (or the `logconfig` command in the CLI) to configure a log subscription.

Creating a Log Subscription in the GUI

To create a log subscription:

1. Chose **System Administration** > **Log Subscription**.
2. Select any of the log subscriptions from the **Log Settings** column.
3. Enter the **log name** (for the log directory) as well as the name for the log file itself.
4. Specify the **Rollover by File Size** maximum, **Rollover by Time** and the **Log Level**.
5. Configure the **Retrieval Method**.
6. Click **Submit**.
7. Click the **Commit Changes**.

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).

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

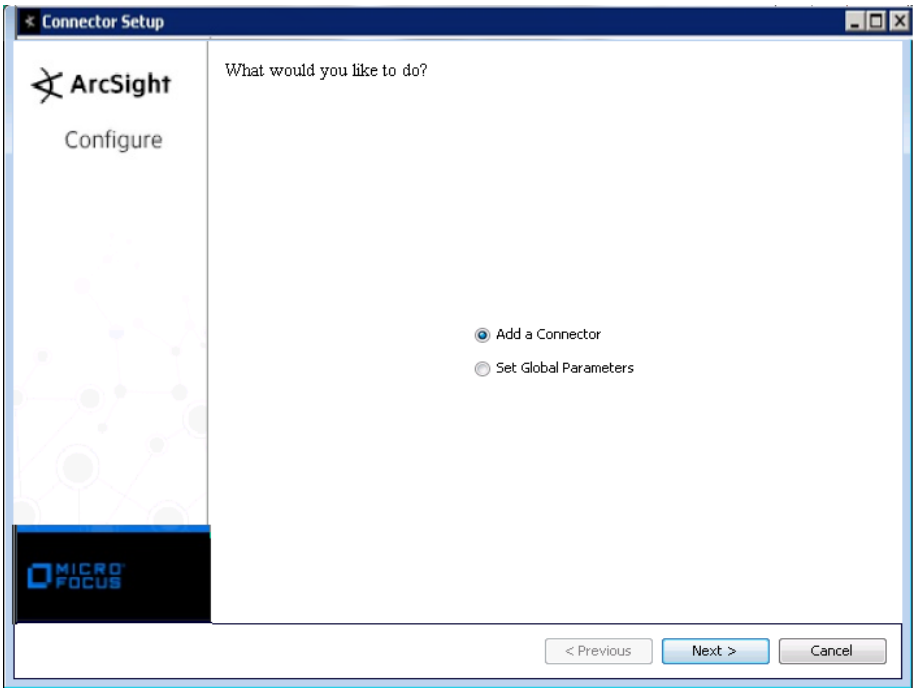
Install Core Software

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 Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus 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:

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'.
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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

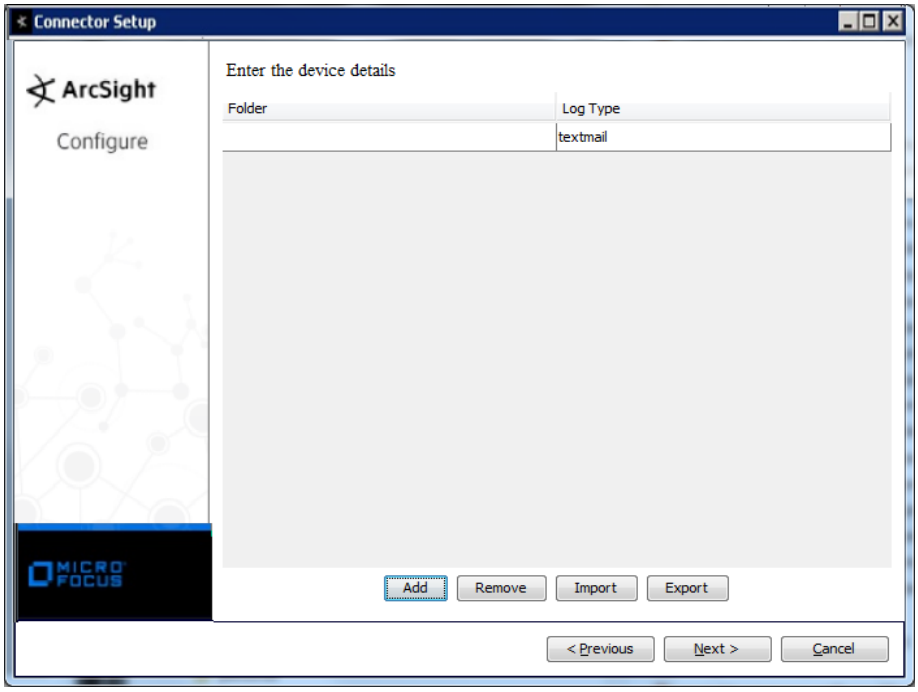
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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 Email Security Appliance File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder	Create a separate folder for each type of log (that is, one folder for the HTTP log, one for the textmail log).Enter the absolute path to the folder where the log files are stored.
Log Type	Select the type of log (HTTP log, textmail log, or both).

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.

Cisco IronPort Text Mail Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Critical; Medium = Warning; Low = LDAP, Info, Debug, Trace
Bytes In	Bytes
Destination User Name	One of(To, Concatenate(destinationUserName,",",To))
Device Custom Number 1	Message ID (MID)
Device Custom Number 2	Injection Connection ID (ICID)
Device Custom Number 3	Delivery Connection ID (DCID)
Device Custom String 1	Sender Group
Device Custom String 2	Policy
Device Custom String 3	SBRS
Device Custom String 4	Error Message
Device Custom String 5	Recipient IDs
Device Custom String 6	Subject
Device Product	'IronPort'
Device Receipt Time	Date
Device Severity	Severity

ArcSight ESM Field	Device-Specific Field
Device Vendor	'CISCO'
Message	Message
Source User Name	From

Cisco IronPort HTTP Log Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Critical; Medium = Warning; Low = Info, Debug, Trace
Device Custom String 3	'Session ID'
Device Product	'IronPort'
Device Receipt Time	Date
Device Severity	Severity
Device Vendor	'CISCO'
Message	Message