



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Cisco Mobility Services Engine Syslog SmartConnector

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 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

- Configuration Guide for Cisco Mobility Services Engine Syslog SmartConnector 4
- Product Overview 5
- Configuration 6
 - Configuring the Device to Send Events 6
 - Additional Information 14
 - Configuring for the Syslog SmartConnectors 15
- Installing the SmartConnector 18
 - Preparing to Install the SmartConnector 18
 - Installing and Configuring the SmartConnector 18
- Device Event Mapping to ArcSight Fields 22
 - Cisco Mobility Services Engine Event Mappings 22
- Send Documentation Feedback 23

Configuration Guide for Cisco Mobility Services Engine Syslog SmartConnector

This guide provides information for installing the SmartConnector for Cisco Mobility Services Engine Syslog 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

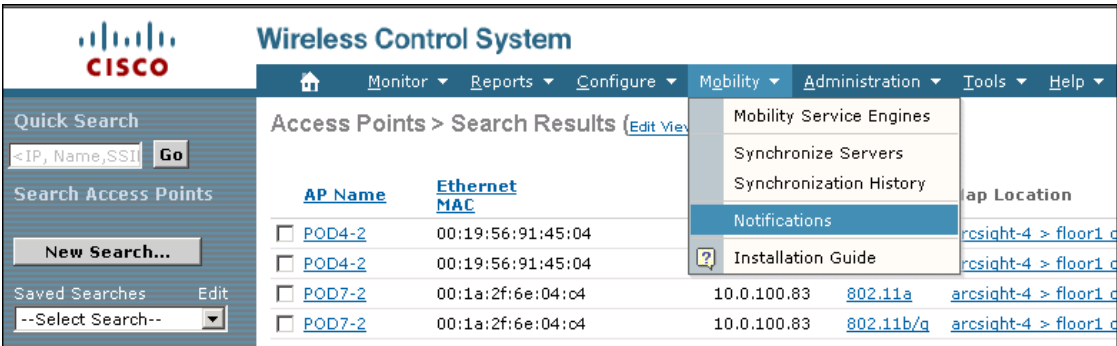
The Cisco 3300 Series Mobility Services Engine is an appliance solution that transforms existing wireless LANs into mobility networks. The centrally managed and provisioned Cisco 3300 Series Mobility Services Engine software suite includes Cisco Context-Aware Software, Cisco Mobile Intelligent Roaming, and Cisco Adaptive Wireless IPS.

Configuration

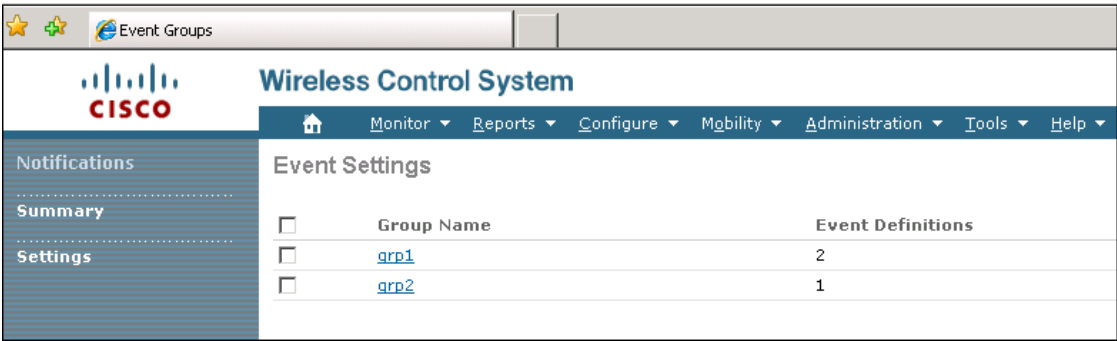
Configuring the Device to Send Events

Coplete the following steps to configure your Cisco device to send events through syslog:

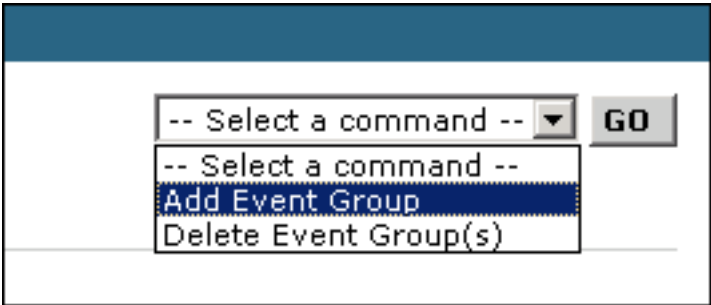
- 1. Log in to Cisco Wireless Control System.
- 2. From the **Mobility** menu, select **Notifications**.



- 3. From the left pane, click **Settings**.



- 4. From the right side of the right pane, select **Add Event Group** from the -- Select a command -- drop-down box and click **GO**.



- 5. Enter a name for the new group and click **Save**.

Wireless Control System

Monitor ▾

Reports ▾

Configure ▾

Mobility ▾

Admin ▾

Event Group > New

Group Name

Save

Cancel

6. The new group (SecurityGroupA in the example) is added to the list. Click the name of the new group.

Wireless Control System

Monitor ▾

Reports ▾

Configure ▾

Mobility ▾

Administration ▾

Tools ▾

Help ▾

Event Settings

| <input type="checkbox"/> | Group Name | Event Definitions |
|--------------------------|--------------------------------|-------------------|
| <input type="checkbox"/> | SecurityGroupA | 0 |
| <input type="checkbox"/> | grp1 | 2 |
| <input type="checkbox"/> | grp2 | 1 |

7. From the -- Select a command -- drop-down menu, select **Add Event Definition** and click **GO**.

Wireless Control System

Monitor ▾

Reports ▾

Configure ▾

Mobility ▾

Administration ▾

Tools ▾

Help ▾

Event Settings > 'SecurityGroupA'

No Events Definitions found in this group.

-- Select a command -- ▾

-- Select a command --

Add Event Definition

Delete Event Definition(s)

Test - Fire Event Definition(s)

GO

8. Enter an **Event Definition Name** and click **Save**.

The screenshot shows the 'Wireless Control System' interface. The breadcrumb trail is 'Event Settings > SecurityGroupA > New Event Definition'. There is a text input field for 'Event Definition Name'. Below the field are 'Save' and 'Cancel' buttons.

9. On the **General** tab, check the **Enabled** box across from **Admin Status**.

The screenshot shows the 'Wireless Control System' interface. The breadcrumb trail is 'Event Settings > SecurityGroupA > Event Definition Sec Event 1'. There are three tabs: 'General', 'Conditions', and 'Destination And Transport'. The 'General' tab is active. It contains the following fields:

- Name: Sec Event 1
- Admin Status: ☒ Enabled
- Last Modified On: Thu Dec 11 14:56:59 PST 2008
- Priority: 0 (dropdown menu)
- Activate: ☒ All the time

At the bottom are 'Save' and 'Cancel' buttons.

10. Click the **Conditions** tab.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

Event Settings > SecurityGroupA > Event Definition 'Sec Event 1'

General Conditions Destination And Transport

Add Delete

| Trigger If | Apply To | Match by |
|------------|----------|----------|
|------------|----------|----------|

11. Click **Add** to add conditions for the event.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

Event Settings > SecurityGroupA > Event Definition 'Sec Event 1'

General Conditions

Add/Edit Condition

Condition Type Location Change ▾

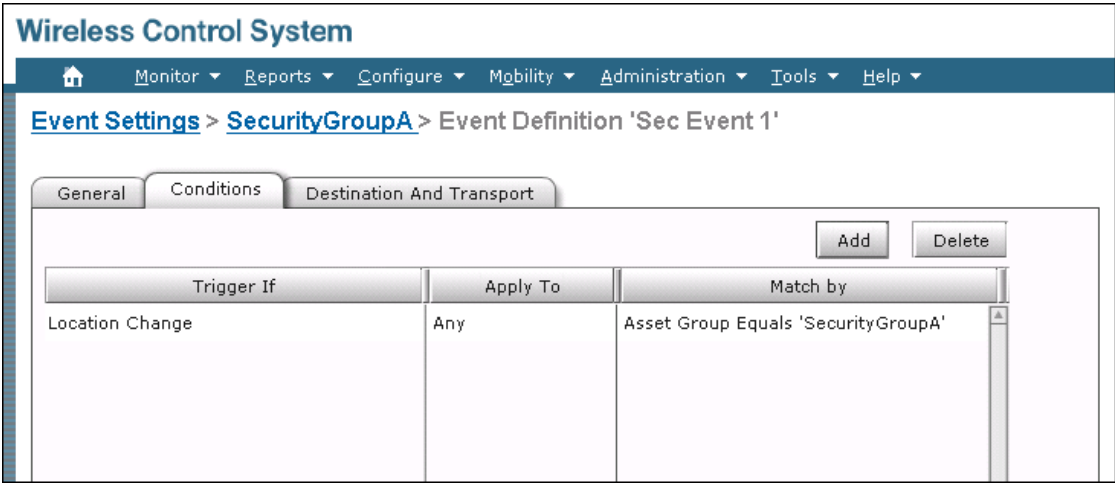
Trigger If Changes Location

Apply To Any ▾

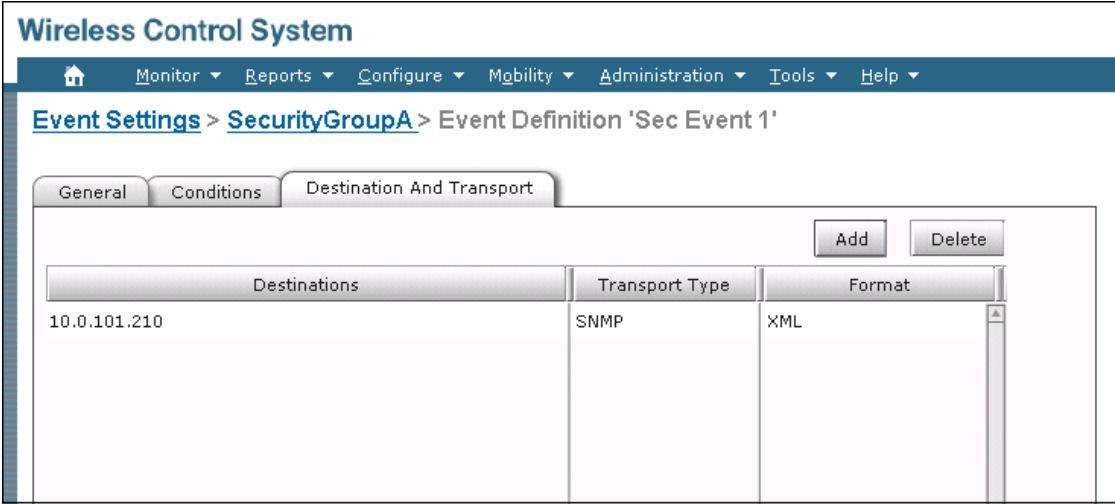
Match By Asset Group ▾ Equals ▾ SecurityGroupA

Add Cancel

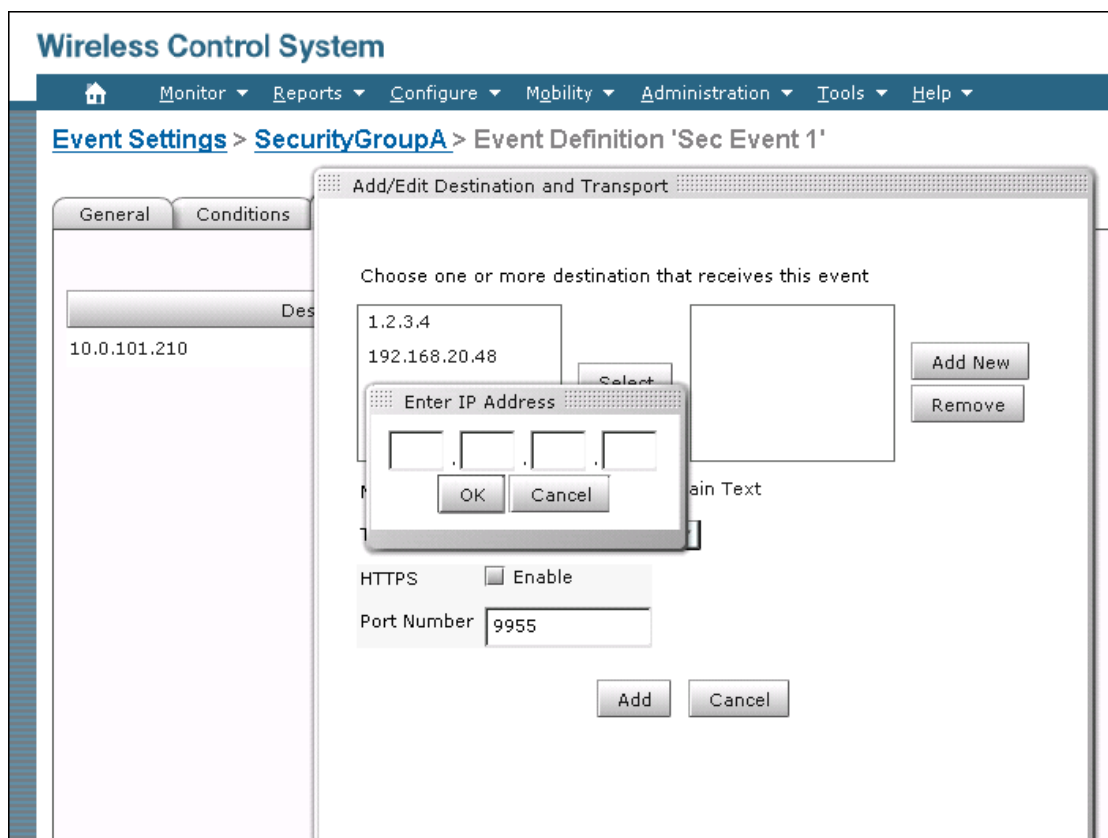
12. Select your conditions from the **Condition Type**, **Apply to**, and **Match By** drop-down selections. Click **Add** and the condition is added as a **Trigger** on the **Conditions** tab.



13. Click the **Destination and Transport** tab.



14. Click **Add**. On the **Add/Edit Destination and Transport** window, click **Add New** and enter the IP address in the pop-up window. Click **OK**.



15. For **Message Format**, select **XML**. For **Transport Type**, select **SysLog**. Enter the syslog **Priority**, **Facility**, and **Port Number**.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

[Event Settings](#) > [SecurityGroupA](#) > Event Definition 'Sec Event 1'

General Conditions

Destinations

10.0.101.210

Choose one or more destination that receives this event

1.2.3.4
192.168.20.48
10.0.101.210

Select

1.12.13.14

Add New
Remove

Message Format ☒ XML ☐ Plain Text

Transport Type SysLog ▾

Priority 2

Facility 2

Port Number 514

Add Cancel

16. Click **Add**. The new destination is listed on the **Destination and Transport** tab.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

[Event Settings](#) > [SecurityGroupA](#) > Event Definition 'Sec Event 1'

General Conditions Destination And Transport

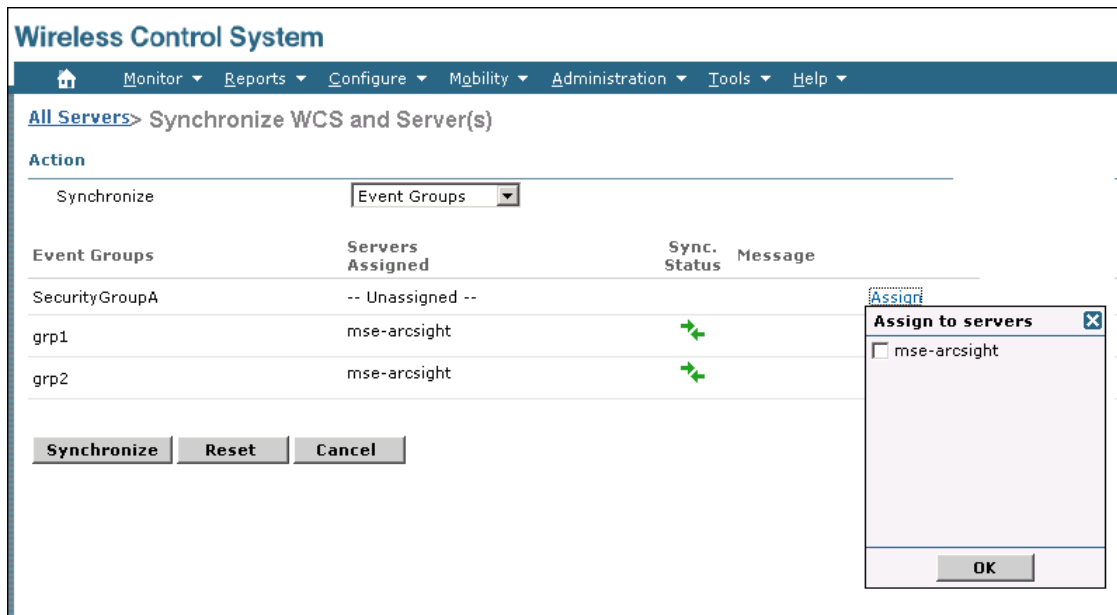
Add Delete

| Destinations | Transport Type | Format |
|--------------|----------------|--------|
| 10.0.101.210 | SNMP | XML |
| 1.12.13.14 | SysLog | XML |

17. Return to the **General** tab and click **Save**.
18. From the **Mobility** menu, select **Synchronize Servers**.



19. Under **Action**, for **Synchronize**, select **Event Groups** from the drop-down. The new group is not yet assigned to a server. Click on **Assign** for the Event Group you just created and check the server to which the group is to be assigned. Click **OK**.



20. An asterisk is displayed next to the word **Assign** and the **Servers Assigned** field displays -- **Unassigned** -- until you click the **Synchronize** button.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

[All Servers](#)> Synchronize WCS and Server(s)

Action

Synchronize

| Event Groups | Servers Assigned | Sync. Status | Message |
|----------------|------------------|--------------|--------------------------|
| SecurityGroupA | -- Unassigned -- | | Assign * |
| grp1 | mse-arcsight | → | Assign |
| grp2 | mse-arcsight | → | Assign |

21. After the synchronization is complete, the Event Group is successfully assigned to the server.

Wireless Control System

Monitor ▾ Reports ▾ Configure ▾ Mobility ▾ Administration ▾ Tools ▾ Help ▾

[All Servers](#)> Synchronize WCS and Server(s)

Action

Synchronize

| Event Groups | Servers Assigned | Sync. Status | Message |
|----------------|------------------|--------------|------------------------|
| SecurityGroupA | mse-arcsight | → | Assign |
| grp1 | mse-arcsight | → | Assign |
| grp2 | mse-arcsight | → | Assign |

Additional Information

For more information about the Cisco Wireless system, see the following Cisco documentation.

- [Cisco MSE - Context Aware Mobility Software Configuration Guide](#)
- [Cisco MSE - Context Aware Mobility Solution Deployment Guide](#)
- [Cisco Wireless Control System \(WCS\)](#)
- [Cisco WLAN Design for Location - Best Practices](#)
- [Cisco WLAN Controller Configuration Guide](#)

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Daemon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as messages.log rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the */etc/rsyslog.conf* file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug | /var/tmp/syspipe
```

3. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:
 - a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

Installing the SmartConnector

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

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

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

Installing and Configuring the SmartConnector

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|--------------|---|
| Network port | The SmartConnector for Syslog Daemon listens for syslog events from this port. |
| IP Address | The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses. |
| Protocol | Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning. |
| Forwarder | This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None . |

- b. Click **Next**.
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, then specify the following parameters:

| Parameters | Description |
|-------------------------|--|
| Pipe Absolute Path Name | Specify an absolute path to the pipe, or accept the default value: <code>/var/tmp/syspipe</code> . |
| File Absolute Path Name | <p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none">• Solaris: <code>\var\adm\messages</code>• Linux: <code>\var\log\messages</code> <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none">• Date format log rotation: The device creates a new log at a specified time in the with the naming convention <code>filename.timestamp.log</code>. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new <code>filename.timestamp.log</code> and begins processing that file. To enable this log rotation, specify timestamp in <code>yyyy-MM-dd</code> date format. For example, <code>filename.yyyy-MM-dd.log</code>• Index log rotation: The device writes to indexed files in the following format: <code>filename.log.001</code>, <code>filename.log.002</code>, <code>filename.log.003</code>, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example: <code>filename'%d,1,99,true'.log</code>; Specifying <code>true</code> indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of <code>true</code> is optional. |

| Parameters | Description |
|---|---|
| Reading Events Real Time or Batch | Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning. |
| Action Upon Reaching EOF | This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None . |
| File Extension If Rename Action | This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a <code>.processed</code> extension. |

b. Click **Next**.

5. Select a [destination and configure parameters](#).
6. Specify a name for the connector.
7. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

8. Select whether you want to install the connector as a service or in the standalone mode.
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

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 Mobility Services Engine Event Mappings

| ArcSight ESM Field | Device-Specific Field |
|-------------------------|-------------------------------------|
| Destination Mac Address | entityID |
| Device Action | state |
| Device Custom Date 1 | LastSeen |
| Device Custom Number 1 | referenceObjectID |
| Device Custom Number 2 | containerObjectID |
| Device Custom Number 3 | missingFor |
| Device Custom String 1 | reference |
| Device Custom String 2 | containerID |
| Device Custom String 3 | containerType |
| Device Custom String 4 | floor |
| Device Custom String 5 | in |
| Device Custom String 6 | entityType |
| Device Event Category | type |
| Device Event Class Id | type |
| Device Product | 'MSE' |
| Device Vendor | 'CISCO' |
| Message | One of (emergencyReason, optionMsg) |
| Source Mac Address | chockpointMac |

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 Configuration Guide for Cisco Mobility Services Engine Syslog SmartConnector (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!