

RSA NetWitness Logs

Event Source Log Configuration Guide



Cisco 3300 Series Mobility Services Engine

Last Modified: Thursday, July 27, 2017

Event Source Product Information:

Vendor: [Cisco](#)

Event Source: Mobility Services Engine (MSE)

Versions: 5.2.91.0, 6.0.97.0, 7.0.105.0

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: ciscomse

Collection Method: Syslog

Event Source Class.Subclass: Network.Wireless Devices

To configure the Cisco 3300 Series Mobility Services Engine event source, you must:

- I. Configure Syslog Output on Cisco 3300 Series Mobility Services Engine
- II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on Cisco 3300 Series Mobility Services Engine

The following procedures describes how to configure Syslog output on your device, depending on your version of the Cisco 3300 Series Mobility Services Engine event source.

Configure Version 6.0.97.0 and 7.0.105.0

To configure Cisco Mobility Services Engine 6.0.97.0 and 7.0.105.0:

1. Log on to the Cisco Wireless Control System web console.
2. In the top menu, click **Services > Context Aware Notifications**.
3. In the Notifications pane, click **Notification Settings**.
4. If you have already configured an event group and event definition, go to step 5. To configure an event group and event definition, follow these steps:
 - a. From the Select a command drop-down list, select **Add Event Group**, and click **Go**.
 - b. In the New Event Group window, enter the event group name into the **Group Name** field, and click **Save**.
 - c. In the Event Settings window, click on the event group created in step b.
 - d. From the **Select a command** drop-down list, select **Add Event Definition**, and click **Go**.
 - e. In the **Event Definition Name** field, enter the definition name, and click **Save**.
5. To set the Destination and Transports settings, follow these steps:
 - a. If the Event Definition window is open, go to step b. To open the Event Definition window, in the Event Settings window, click the event group, and then click the event definition.
 - b. In the Event Definition window, click the **Destination and Transport** tab.
 - c. Click **Add**.

- d. In the Add/Edit Destination and Transport window, click **Add New**.
- e. In the Enter IP Address window, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector and click **OK**.
- f. In the Add/Edit Destination and Transport window, complete the fields as follows.

Field	Action
Message Format	Select XML .
Transport Type	From the drop-down list, select SysLog .
Port Number	Ensure the port number is set to 514 .

- g. Click **Add**.
6. To enable the event definition, follow these steps:
 - a. In the Event Definition window, click the **General** tab.
 - b. Click **Save**.

Note: In order to enable the event definition, you must have at least one condition configured through the **Conditions** tab.

- c. In the Admin Status field, select **Enabled**.
 - d. Click **Save**.
7. To synchronize the event group, follow these steps:
 - a. In the top menu, click **Services > Synchronize Services**.
 - b. Click the **Event Groups** tab.
 - c. Click **Synchronize**.

Configure Cisco Mobility Services Engine 5.2.91.0

To configure Cisco Mobility Services Engine 5.2.91.0:

1. Log on to the Cisco Wireless Control System web console.
2. In the top menu, click **Mobility > Notifications**.
3. In the left pane, click **Settings**.

4. If you have already configured an event group and event definition, go to step 5. To configure an event group and event definition, follow these steps:
 - a. From the **Select a command** drop-down list, select **Add Event Group**, and click **Go**.
 - b. In the **Group Name** field, enter the event group name, and click **Save**.
 - c. Click the event group that you created in step b.
 - d. From the **Select a command** drop-down list, select **Add Event Definition**, and click **Go**.
 - e. In the **Event Definition Name** field, enter the definition name, and click **Save**.
5. To set the Destination and Transport settings, follow these steps:
 - a. If the Event Definition window is open, go to step b. To open the Event Definition window, in the Event Settings window, click the event group, and then click the event definition.
 - b. Click the **Destination and Transport** tab.
 - c. Click **Add**.
 - d. In the Add/Edit Destination window, click **Add New**.
 - e. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector, and click **OK**.
 - f. In the Add/Edit Destination window, complete the fields as follows.

Field	Action
Message Format	Select XML .
Transport Type	From the drop-down list, select SysLog .
Port Number	Ensure the port number is set to 514 .

- g. Click **Add**.
6. To enable the event definition, follow these steps:
 - a. In the **General** tab, click **Save**.

Note: In order to enable the event definition, you must have at least one condition configured through the **Conditions** tab.

- b. In the **Admin Status** field, select **Enabled**.
 - c. Click **Save**.
7. To synchronize the event group, follow these steps:
 - a. In the top menu, click **Mobility > Synchronize Services**.
 - b. Click the **Event Groups** tab.
 - c. Click **Synchronize**.

Configure RSA NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **ciscomse**.



Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:

- If you see  **Start Capture**, click the icon to start capturing Syslog.
- If you see  **Stop Capture**, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View > Config > Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

The Event Categories panel displays the Syslog event sources that are configured, if any.

4. In the Event Categories panel toolbar, click **+**.

The Available Event Source Types dialog is displayed.

5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.