RSA NetWitness Logs

Event Source Log Configuration Guide

McAfee Email Gateway

Last Modified: Wednesday, November 8, 2017

Event Source Product Information:

Vendor: McAfee
Event Source: Email Gateway (formerly known as CipherTrust IronMail)
Versions: 5.5, 7.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: ironmail
Collection Method: Syslog, SNMP
Event Source Class.Subclass: Security.Antivirus

To configure the McAfee Email Gateway event source, you must:

I. Configure Syslog Output on McAfee Email Gateway

II. Configure RSA NetWitness Suite for Syslog Collection

III. Configure SNMP Event Sources on the RSA NetWitness Suite

Note: McAfee Email Gateway logs some events in Syslog format, and others in SNMP traps, so you must configure both formats to send all events to the RSA NetWitness Suite.

Configure Syslog Output on McAfee Email Gateway

Depending on your version:

- Configure McAfee Email Gateway version 7.x, or
- Configure McAfee Email Gateway version 5.5

Configure McAfee Email Gateway 7.x

1. Log on to the McAfee Email Gateway web interface with administrator credentials.
2. Click on the **System** icon.
3. From the **Logging, Alerting and SNMP** menu, click on the **SNMP Alert Settings** tab.
   a. Check the **Enable SNMP alerts** box.
   b. Under **Send alerts to the trap manager for the following event types**, check the boxes for all event types.
   c. Complete the following fields in **Trap Manager Settings**:

Field	Value
Trap manager	Enter the IP address of the RSA NetWitness Suite Log Collector.
Community name	public
Protocol version	v1

   d. Select **Apply configuration changes**.

4. Click on the **SNMP Monitor Settings** tab.
   a. Check the **Enable SNMP monitor** box.
   b. Complete the following fields in **Basic Settings**:

Field	Value
Protocol version	v1/v2c
Community name	public

   c. From the **Access control list** field, select **Allow all hosts / networks**.
   d. Click the green checkmark labeled **Apply configuration changes**.
5. Click on the **System Log Settings** tab.
   a. Check the **Enable system log events** box.
   b. Under **Log events to the syslog for the following event types**, check the boxes for all event types.
   c. For **Logging format**, select **Original**.
   d. Complete the following fields in **Off-box system log**:

Field	Value
Receiving server	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	514
Protocol	UDP

   e. Select **Apply configuration changes**.

Configure McAfee Email Gateway 5.5

To configure McAfee Email Gateway 5.5 - Alert Notification Configuration:

1. Log on to the McAfee Email Gateway web interface with administrator credentials.
2. Click the **Reporting** tab.
3. From the menu, expand **Alert Manager** and select **Alert Class**.

4. Click **Add** to create an Alert Class that contains all the services you want to monitor.
5. From the menu, expand **Alert Manager** and select **Alert Mechanism**.
6. Select the following values from the drop down fields and then click **Add**:
   - Alert Class - Manage: select the Alert Class that contains the services you want to monitor
   - Alert Type: **INFORMATION**
   - Alert Mode: **SNMP**
7. Fill in the following fields and click **Submit**:
   - Server Name: IP address of the RSA NetWitness Suite Log Collector
   - Version: **2**
   - Port: **162**
8. Repeat steps **5** and **6** for these Alert Types:
   - NOTIFICATION
   - WARNING
   - ERROR
   - CRITICAL

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 **ironmail**.

Configure Syslog Collection

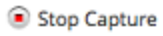
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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 

, click the icon to start capturing Syslog.
- If you see 

, 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.

Configure SNMP Event Sources on NetWitness Suite

To set up SNMP on RSA NetWitness Suite, perform the following tasks:

I. Add the SNMP Event Source Type

II. Configure SNMP Users

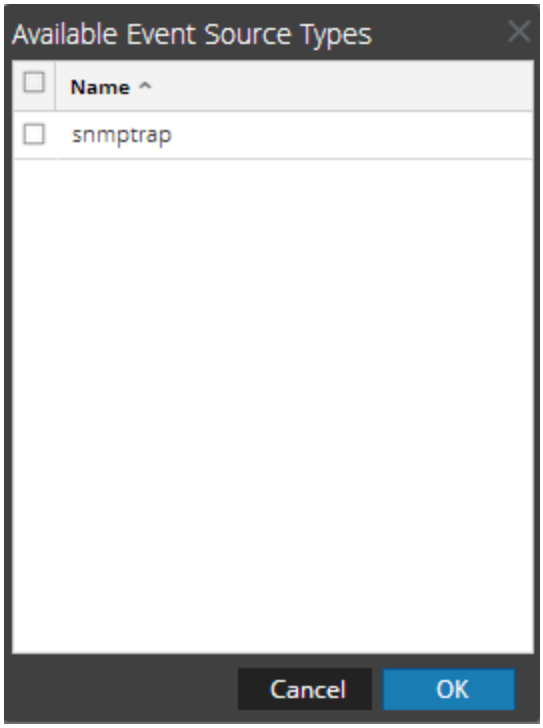
Add the SNMP Event Source Type

Note: If you have previously added the **snmptrap** type, you cannot add it again. You can edit it, or manage users.

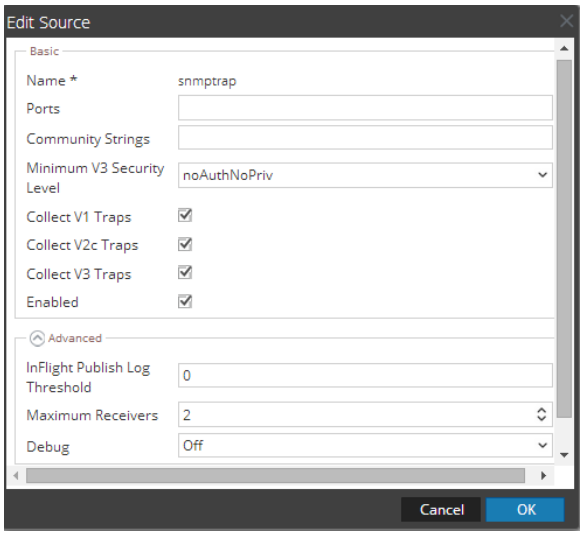
Add the SNMP Event Source Type:

1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

   The Sources panel is displayed with the existing sources, if any.
5. Click + to open the **Available Event Source Types** dialog.



6. Select **snmptrap** from the Available Event Source Types dialog and click **OK**.
7. Select **snmptrap** in the Event Categories panel.
8. Select **snmptrap** in the Sources panel and then click the Edit icon to edit the parameters.



9. Update any of the parameters that you need to change.

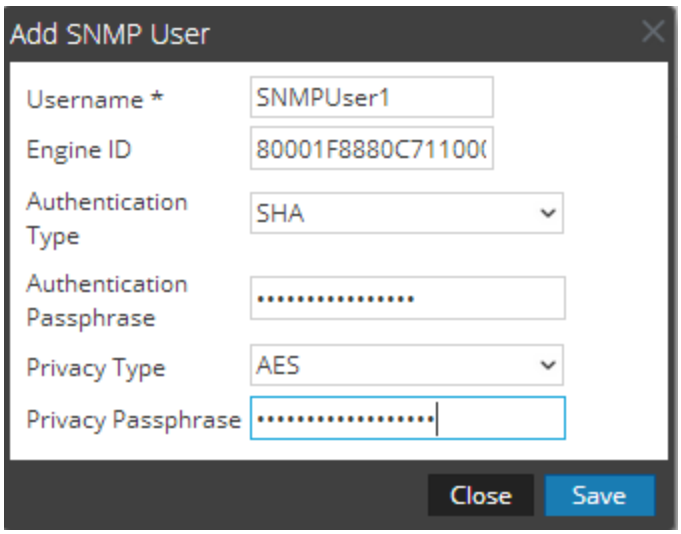
(Optional) Configure SNMP Users

If you are using SNMPv3, follow this procedure to update and maintain the SNMP v3 users.

Configure SNMP v3 Users

1. In the **RSA NetWitness Suite** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View** > **Config**.
4. In the Log Collector **Event Sources** tab, select **SNMP/SNMP v3 User Manager** from the drop-down menu.

   The SNMP v3 User panel is displayed with the existing users, if any.
5. Click + to open the **Add SNMP User** dialog.



6. Fill in the dialog with the necessary parameters. The available parameters are described below.

SNMP User Parameters

The following table describes the parameters that you need to enter when you create an SNMP v3 user.

Parameter	Description
Username *	User name (or more accurately in SNMP terminology, security name). RSA NetWitness Suite uses this parameter and the **Engine ID** parameter to create a user entry in the SNMP engine of the collection service. The **Username** and **Engine ID** combination must be unique (for example, **logcollector**).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id.
Authentication Type	(Optional) Authentication protocol. Valid values are as follows: • **None** (default) - only security level of **noAuthNoPriv** can be used for traps sent to this service • **SHA** - Secure Hash Algorithm • **MD5** - Message Digest Algorithm
Authentication Passphrase	Optional if you do not have the **Authentication Type** set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are as follows: • **None** (default) • **AES** - Advanced Encryption Standard • **DES** - Data Encryption Standard
Privacy Passphrase	Optional if you do not have the **Privacy Type** set. Privacy passphrase.
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

Trademarks