

RSA NetWitness Platform

Event Source Log Configuration Guide



McAfee Database Security

Last Modified: Thursday, August 16, 2018

Event Source Product Information:

Vendor: [McAfee](#)

Event Source: Database Security

Version: 4.2, 5.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.

Additional Download: server-custom.properties

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: mcafeeds

Collection Method: Syslog

Event Source Class.Subclass: Security Application Firewall

To configure the McAfee Database Security event source, you must:

- I. Configure Syslog Output on McAfee Database Security
- II. Configure NetWitness Platform for Syslog Collection

Configure Syslog Output on McAfee Database Security

To configure the McAfee Database Security event source, you must complete these tasks:

- I. Edit the McAfee Database Security Properties File
- II. Configure the Syslog Settings
- III. Configure System Messages Via Syslog
- IV. Configure System Rules Via Syslog

Edit the McAfee Database Security Properties File

The security properties file specifies the log information for the RSA NetWitness Platform platform to capture.

Download the Properties File from RSA Link

To edit the McAfee Database Security properties file:

1. Navigate to the [Downloads](#) space on [RSA Link](#), and select the [McAfee Database Security downloads page](#).
2. Download the **server-custom.properties** file.
3. Copy the string in the downloaded properties file that you downloaded, and insert it into your **server-custom.properties** file, located in the **conf** folder where you installed McAfee Database Security.
4. Save and close your file.

Note: Go to Step 5 in the "Configuring the Syslog Settings" section to verify if you correctly edited the properties file.

Properties File Details

The **server-custom.properties** file contains a **log.format.body.custom** entry. This entry lists the McAfee Database Security fields to include in the log file. McAfee provides the flexibility of limiting the size of each of its fields. It is possible to specify a maximum length for the field as follows:

`$fieldName:size$`

where:

- *fieldName* is the name of the field
- *size* is the maximum length for that field

For example, the following field information is in the **server-custom.properties** file:

`$rules.name:100$`

This limits the `rules.name` field to 100 characters.

RSA has limited several fields in this manner. It is recommended that you keep these limitations when you edit the **server-custom.properties** file and copy it to the McAfee Database Security properties file.

Configure the Syslog Settings

To configure the McAfee Database Security Syslog settings:

1. Log on to McAfee Database Security with administrative credentials.
2. In the navigation bar at the top, click **System**.
3. Click **Interface > Syslog**.
4. From the Syslog Configuration page, select **Use Syslog** and complete the fields follows:

Field	Action
Host	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Port	Type 514 .
Transport	From the drop-down list, select UDP .
Max Packet Length	Type 64 .
Facilities	From the drop-down list, select Local0 .
Format	From the drop-down list, select Custom .

Note: RSA NetWitness Platform only supports custom formats. If you select any other format, your messages will be undefined.

5. In the **Alert Format Details** section, ensure that the string is the same as the string that you added when you edited the McAfee Database Security properties file.

Note: If you cannot find the string, ensure that you correctly completed the steps in the [Edit the McAfee Database Security Properties File](#) section.

Configure System Messages Via Syslog

To configure system messages via Syslog:

1. Log on to McAfee Database Security with administrative credentials.
2. In the navigation bar at the top, click **System**.
3. Click **Messages > Configuration**.
4. Ensure that **Send system message to syslog** is selected, and from the drop-down list, select any level except **Trace** or **Debug**.
5. Click **Save**.

Configure System Rules Via Syslog

To configure McAfee Database Security system rules via syslog:

1. Log on to McAfee Database Security with administrative credentials.
2. In the navigation bar at the top, click **Rules**.
3. Depending on the type of rule that you want to edit, click **vPatch Rules** or **Custom Rules**.
4. Click the **Edit** icon of a rule.
5. In the **Action** section, ensure that **Syslog** is selected, and from the drop-down list, select any level except **Trace** or **Debug**.
6. Click **Save**.

Configure NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform 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 **mcafeeds**.



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 © 2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.