

# RSA NetWitness Logs

## Event Source Log Configuration Guide



## Entrust Identity Guard

Last Modified: Friday, May 12, 2017

### Event Source Product Information:

**Vendor:** [Entrust](#)

**Event Source:** Identity Guard

**Versions:** 10.1

### RSA Product Information:

**Supported On:** NetWitness Suite 10.0 and later

**Event Source Log Parser:** entrustig

**Collection Method:** Syslog

**Event Source Class.Subclass:** Security.Access Control

# Configure Entrust Identity Guard

---

To configure Syslog collection for the Entrust event source, you must:

- I. Configure Syslog Output on Entrust Identity Guard
- II. Configure RSA NetWitness Suite for Syslog Collection

## Configure Syslog Output on Entrust Identity Guard

Entrust Identity Guard uses the log4J logging service to generate both audit logs and general system logs. RSA NetWitness Suite can collect both system and audit logs from the Entrust event source.

**Note:** RSA NetWitness Suite currently supports events from Entrust Identity Guard running on Windows platforms only.

### To configure the Entrust Identity Guard event source:

1. You use the Properties Editor to store the log files.
  - a. Start the Entrust Properties Editor.
  - b. On the Table of Contents, select **General Logging Configuration**.
  - c. If you want to store the log files in the Base Logger, set the **Base Logger Messages Also Go to Root Logger** to **True**.
  - d. RSA recommends that you accept the default values for the other fields in the dialog.
  - e. If you made any changes, click **Validate & Save**.
2. Configure the audit logging properties.
  - a. If you have exited the Entrust Properties Editor, restart it.
  - b. On the Table of Contents, select **Audit Logging Appenders**.
  - c. In the **AUDIT\_SYSLOG Host Name** field, enter the IP address of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
  - d. Optionally, you can change the **AUDIT\_SYSLOG Facility** value. Or, accept the default value of **Local1**.
  - e. Click **Validate & Save**.
3. Configure the system logging properties.

- a. If you have exited the Entrust Properties Editor, restart it.
- b. On the Table of Contents, select **System Logging Appenders**.
- c. In the **AUDIT\_SYSLOG Host Name** field, enter the IP address of the RSA NetWitness Suite Log Decoder or RSA NetWitness Suite Remote Log Collector.
- d. Optionally, you can change the **AUDIT\_SYSLOG Facility** value. Or, accept the default value of **Local1**.
- e. Click **Validate & Save**.



For more details on Entrust logging, see the *Entrust® IdentityGuard Server Administration Guide*.

## Configure RSA NetWitness Suite for 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.