RSA NetWitness Logs

Event Source Log Configuration Guide

RSA Data Loss Prevention Suite

Last Modified: Wednesday, November 8, 2017

Event Source Product Information:

Vendor: RSA, The Security Division of EMC
Event Source: Data Loss Prevention
Versions: 7.0.0, 8.0, 8.0 SP1, 8.5, 8.8, 9.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: rsadlp
Collection Method: Syslog
Event Source Class.Subclass: Security.DLP

To configure the RSA Data Loss Prevention Suite event source, you must:

I. Configure Syslog Output on RSA Data Loss Prevention Suite

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Syslog Output on RSA Data Loss Prevention Suite

Depending on your version, see the following section:

- Configure Syslog Output on RSA DLP 8.x, and 9.x, or
- Configure Syslog Output on RSA DLP 7

Configure Syslog Output on RSA DLP Version 8.x and 9.x

To configure Syslog output on RSA Data Loss Prevention Suite 8.x, 9.0, 9.5, and 9.6 SP1 you must complete these tasks:

- Configure RSA DLP to send DLP incidents to RSA NetWitness
- Configure RSA DLP to send System Alerts RSA NetWitness

To configure RSA DLP to send DLP incidents RSA NetWitness:

1. From within RSA DLP, select the **Admin** tab.
2. Select **Settings > SIEM Configuration**.
3. Click **New**.
4. In the **Syslog Host/IP** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
5. Click **Save**.

To configure RSA DLP to send System Alerts logging to RSA NetWitness:

1. From within RSA DLP, select the **Admin** tab.
2. Select **Settings > System Alerts Configuration**.
3. Click **New** or **Edit** to update the configuration.
4. Select **Syslog** for **Enterprise Manager**, **Network**, and **Datacenter**.
5. Click **Save**.

DLP Table

For RSA DLP 8.0 SP1, RSA has added several columns and variables to the DLP table. These new columns are described in the following table.

Field	Description	Values	RSA NetWitness Mapping
Severity	Denotes the severity of the DLP event.	• CRITICAL • HIGH • MEDIUM • LOW • IGNORE	Column: Severity Variable: <severity>
RiskFactor	Numeric representation of risk, determined by the policy that was violated.	Scale of 1 - 100, 100 being the highest risk.	Column: Risk Variable: <risk_num>
MatchCount	Number of (content) matches found for the primary policy that was violated.	Positive integer	Column: Counter1 Variable: <dclass_counter1>

Configure Syslog Output on RSA DLP 7

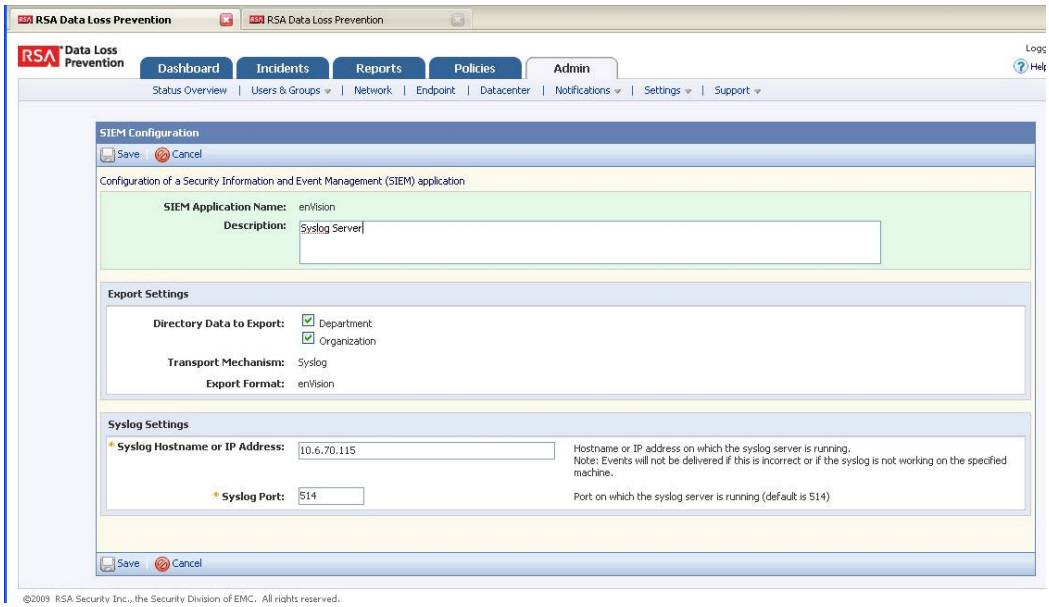
To configure Syslog output on RSA Data Loss Prevention Suite 7.0, you must complete these tasks:

- Configure RSA DLP to send DLP incidents to RSA NetWitness
- Change the default multi-value field delimiters in the DLP Enterprise Manager

> **Note:** RSA recommends that an RSA Professional Services Engineer perform this procedure.

Configure RSA DLP to send DLP incidents to RSA NetWitness:

1. From within RSA DLP, select the **Admin** tab.



2. Select **Settings > SIEM Configuration**.
3. Click **New**.
4. In the **Syslog Host/IP** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
5. In the **Syslog Port** field, enter the IP address for the RSA NetWitness Suite server.
6. Click **Save**.

Change the default multi-value field delimiters in the DLP Enterprise Manager

Additionally, for the RSA NetWitness Log Decoder or Remote Log Collector to recognize the RSA DLP data, you need to change the default multi-value field delimiters in the DLP Enterprise Manager. RSA recommends that a qualified RSA Professional Services Engineer perform this procedure.

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 **rsadlp**.

Configure Syslog Collection

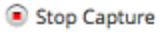
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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.

Trademarks