

RSA NetWitness Platform

Event Source Log Configuration Guide



McAfee Network Security Platform

Last Modified: Tuesday, September 3, 2019

Event Source Product Information:

Vendor: [McAfee](#)

Event Source: Network Security Platform (formerly Intrushield)

Versions: 2.1, 3.1, 4.1, 5.1, 6.1, 7.1, 8.x, 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.

Additional Downloads: mcafee_nsp.txt

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later

Event Source Log Parser: intrushield

Collection Method: Syslog, ODBC (for version 5.1)

Event Source Class.Subclass: Security.IDS

This document contains the following instructions:

To configure McAfee Network Security Platform 5.1 for ODBC collection, you must complete the following tasks:

- I. [Configure Network Security Platform 5.1 for ODBC Collection](#)
- II. [Configure NetWitness Platform for ODBC Collection](#)

To configure McAfee Network Security Platform for syslog collection, you must complete the appropriate task, depending on your version:

- I. Configure the Network Security Platform. Depending on your version, see the applicable section:
 - [Configure Network Security Platform 8.x or 9.x for Syslog Collection](#)
 - [Configure Network Security Platform 7.1 for Syslog Collection](#)
 - [Configure Network Security Platform 3.1, 4.1, 5.1, or 6.1 for Syslog Collection](#)
 - [Configure Network Security Platform 2.1 for Syslog Collection](#)
- II. [Configure NetWitness Platform for Syslog Collection](#)

Configure Network Security Platform 5.1 for ODBC Collection

To configure Network Security Platform 5.1 for ODBC collection:

1. Log on to the Network Security Platform system with administrator credentials.
2. Open a new command prompt, and change directories to where Network Security Platform is installed.
3. Change directories to the `\MySQL\bin` directory.
4. To connect to the MySQL database, type:

```
mysql --host=127.0.0.1 -u root --password=PASSWORD -p mysql
```

where:

- *root* is the user name created during the Network Security Platform install.
- *PASSWORD* is the password created during the Network Security Platform install.

Note: If prompted for a password, reenter the password.

5. Follow these steps to allow the RSA NetWitness Platform to connect to Network Security Platform:

- a. Type:

```
insert into mysql.user (host, user,password) values ('NODE','audit_reader',password('PASSWORD'));
```

where:

- *NODE* is the name of the RSA NetWitness Platform.
- *PASSWORD* is the user's password.

- b.

```
insert into mysql.db (host, db, user, select_priv) values ('<NODE>', 'lf', 'audit_reader', 'Y');
```

where *NODE* is the name of your RSA NetWitness Platform server.

- c. Type:

```
flush privileges;
```

- d. Type:

```
exit
```

Configure NetWitness Platform for ODBC Collection

To configure McAfee Network Security Platform for ODBC Collection on RSA NetWitness Platform, perform the following tasks on the RSA NetWitness Platform:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

For table reference, see [Reference Tables](#) below.

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 **ADMIN > 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 **intrushield**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN > 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 **ODBC/DSNs** from the drop-down

menu.

5. The DSNs panel is displayed with the existing DSNs, if any.
6. Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the hostname or IP Address of the Oracle database for McAfee Network Security Platform.
PortNumber	Specify the Port Number. The default port number is 1521
HostName	Specify the hostname or IP Address of the McAfee Network Security Platform event source.
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none"> • For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3ora27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3ora26.so

Add the Event Source Type

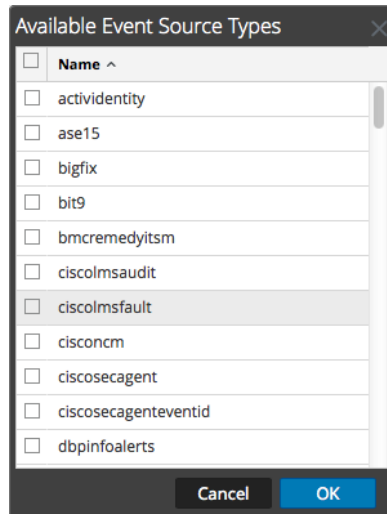
Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN > 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 **ODBC/Config** from the drop-down

menu.

The Event Categories panel is displayed with the existing sources, if any.

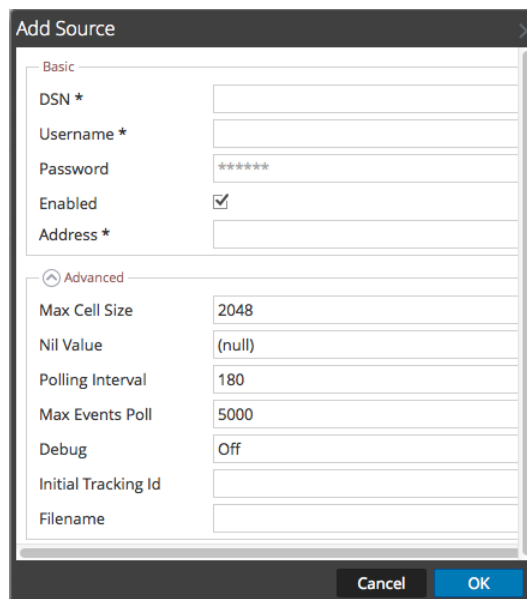
5. Click **+** to open the **Available Event Source Types** dialog.



6. Choose the log collector configuration type for your event source type and click **OK**.

Select **intrushield51** from the **Available Event Source Types** dialog.

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click **+** to open the **Add Source** dialog.



9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Reference Tables

This event source collects data from the **intrushield51.xml** table, using the following typespec files:

- lf.iv_alert
- lf.iv_signature
- lf.iv_alert_severity
- lf.iv_alert_type
- lf.iv_attack,lf.iv_sensor_port
- lf.iv_sensor
- lf.iv_subscriber
- lf.iv_result_set

Configure Network Security Platform 8.x or 9.x for Syslog Collection

To configure McAfee Network Security Platform 8.x or 9.x:

1. Log on to Network Security Platform with Administrator credentials.
2. Click the **Manage** tab.
3. On the left-hand menu, click **Setup > Notification > IPS Events > Syslog**
4. On the right-hand menu for **Enable Syslog Notification**, select **Yes**.
5. Under **Syslog Notification Profiles**, click **New**.
6. Set **Admin Domain** to **Current**.
7. Provide a **Notification Profile Name**.
8. Next to **Target Server**, click **New**.
 - a. In the **Add a Syslog Server Profile** menu, fill in the following information:

Field	Action
Target Server Profile Name	Set to RSA NetWitness Platform server name.
Syslog Server Name or IP Address	Enter your Log Decoder IP address.
Protocol	Set to UDP
Port	Type 514 .

- b. Click **Save**.
9. Set **Facility** to **Local user 7 (local7)**.
 10. For **Severity Mappings**, enter the following information:

Field	Action
Severity Mapping	Select Informational: informational messages .

Field	Action
Severity Mapping - Low to	Select Error .
Severity Mapping - Medium to	Select Warning: warning conditions .
Severity Mapping - High to	Select Emergency: system is unusable .
Notify for All Alerts	Leave Unchecked
Only Notify When	Check Severity Informational and Above
Notify on Quarantine Events	Check the box to enable.

11. In the **Message** field, type either of the following:

- You can enter the following string, exactly as shown, if you only need to collect the listed parameters:

```
Alert : |$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|
```

- Alternatively, you can enter any or all of the available variables as name-value pairs. Copy and paste text from the **mcafee_nsp.txt** file. Use the line below **Security Events**. This file is available on RSA Link as an Additional Download here: <https://community.rsa.com/docs/DOC-47132>.

Note: You can remove any name/value pairs that you do not need to collect. Also, the order does not matter: feel free to list the pairs in any order you like.

12. Click **Save**.

13. Enable the collection of Fault messages.

- On the left-hand panel, click **Setup > Notification > Faults > Syslog**.
- On the **Syslog** panel, click **Syslog Forwarder**, and complete the fields as follows.

Field	Action
Enable Syslog Notification	Select Yes .

Field	Action
Admin Domain	Select Current .
Syslog Server - Host IP address	Enter the Log Decoder IP address.
Port	type 514 .
Facilities	Select Local user 7 (local7) .
Severity Mapping - Informational to	Select Emergency: System is unusable .
Severity Mapping - Error to	Select Error .
Severity Mapping - Warning to	Select Emergency: system is unusable .
Severity Mapping - Critical to	Select Emergency: system is unusable .
Forward Faults	Select With severity level Informational and above .

c. In the **Message Preferences** field, select **Customized**.

d. Click **Edit**.

e. In the **Message** field, type:

```
Fault : |FAULT_TIME = $IV_FAULT_TIME$|ADMIN_DOMAIN = $IV_ADMIN_
DOMAIN$|SENSOR_NAME = $IV_SENSOR_NAME$|FAULT_LEVEL = $IV_FAULT_
LEVEL$|FAULT_TYPE = $IV_FAULT_TYPE$|FAULT_NAME = $IV_FAULT_
NAME$|FAULT_SOURCE = $IV_FAULT_SOURCE$|FAULT_COMPONENT = $IV_FAULT_
COMPONENT$|OWNER_ID = $IV_OWNER_ID$|OWNER_NAME = $IV_OWNER_
NAME$|SEVERITY = $IV_SEVERITY$|DESCRIPTION = $IV_DESCRIPTION$|ACK_
INFORMATION = $IV_ACK_INFORMATION$|
```

f. Click **Save**.

g. Click **Save** again.

14. Enable the collection of User Activity (earlier known as Audit logs until version 8.1.5.11) messages.

- a. On the left-hand menu, click **Setup > Notification > User Activity > Syslog**.
- b. On the **Syslog** menu, complete the fields as follows:

Field	Action
Enable Syslog Forwarder	Select Yes .
Admin Domain	Select Current .
Server Name or IP Address	Enter the Log Decoder IP address.
Port	Type 514 .
Facilities	Select Local user 7 (local7) .
Result Mapping	
Failed to	Select Error .
Successful to	Select Notice: normal but significant condition .
In Progress to	Select Informational: informational messages .
Forward Alerts	Select Allow All Auditlogs .

- c. In the **Message Preferences** field, select **Customized**.
 - d. Click **Edit**, and enter the following in the **Message** field:


```
Audit : |AUDIT_TIME = $IV_AUDIT_TIME$|AUDIT_CATEGORY = $IV_AUDIT_CATEGORY$|AUDIT_DOMAIN = $IV_AUDIT_DOMAIN$|AUDIT_USER = $IV_AUDIT_USER$|AUDIT_RESULT = $IV_AUDIT_RESULT$|AUDIT_ACTION = $IV_AUDIT_ACTION$|AUDIT_MSG = $IV_AUDIT_MESSAGE$ |
```
 - e. Click **Save**.
 - f. Click **Apply**.
15. Enable the collection of Firewall Access Events (previously known as Audit Notification) messages.
- a. On the left-hand menu, click **Setup > Notification > Firewall Access Events > Syslog**.

- b. To configure Network Security Platform to send syslog data to RSA NetWitness Platform, complete the fields as follows.

Field	Action
Enable Syslog Notification	Select Yes .
Admin Domains	Select Current .
Server Name or IP Address	Enter the Log Decoder IP address.
Port	Type 514 .
Facility	Select Local user 7 (local7) .
Severity	Select Emergency: system is unusable .

- c. In the **Message Preferences** field, select **Customized**.

- d. Click **Edit**.

- e. In the **Message** field, type:

```
ACL : |SENSOR_NAME=$SENSOR_NAME$|ALERT_DIRECTION=$ALERT_
DIRECTION$|ACL_RULE=$ACL_POLICY$|ACL_RULE_NUMBER=$ACL_RULE_
NUMBER$|SRC_IP_PORT=$SOURCE_IP$:$SOURCE_PORT$|DST_IP_
PORT=$DESTINATION_IP$:$DESTINATION_PORT$|ACL_ACTION=$ACL_ACTION$|APP_
PROTOCOL=$APPLICATION_
PROTOCOL$|APP=$APPLICATION$|INTERFACE=$INTERFACE$|NET_
PROTOCOL=$NETWORK_PROTOCOL$|ALERT_DURATION=$ALERT_DURATION$|
```

- f. Click **Save**.

- g. Click **Save** again.

Configure Network Security Platform 7.1 for Syslog Collection

To configure McAfee Network Security Platform 7.1:

1. Log on to Network Security Platform with Administrator credentials.
2. Click **Configure**.
3. Select the appropriate Admin Domain.
4. Select **IPS Settings**.
5. Enable the collection of Alert messages.
 - a. On the **Alert Notification** tab, Select the **Syslog** tab.
 - b. To configure Network Security Platform to send syslog data to RSA NetWitness Platform, complete the fields as follows.

Field	Action
Enable Syslog Notification	Select Yes .
Admin Domain	Select Current .
Server Name or IP address	Enter the Log Decoder IP address.
UDP Port	Type 514 .
Facility	Select Local user 7 (local7) .
Severity Mapping	Select Informational: informational messages .
Severity Mapping - Low to	Select Error: error conditions .
Severity Mapping - Medium to	Select Warning: warning conditions .
Severity Mapping - High to	Select Emergency: system is unusable .

Field	Action
Send Notification If	Select Severity: Informational and above.
Notify on IPS Quarantine	Select Yes.

c. In the **Message Preferences** field, select **Customized.**

d. Click **Edit.**

e. In the **Message** field, type:

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"  
|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_  
ATTACK_CONFIDENCE$  
  
|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_  
IP$|$IV_SOURCE_PORT$  
|$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|
```

Warning: If you are using McAfee Network Security Platform with Content 2.0, add **\$IV_RESULT_STATUS\$|IV_CATEGORY\$^IV_ATTACK_COUNT\$** at the end of this string.

f. Click **Save.**

g. Click **Apply.**

6. Enable the collection of Fault messages.

a. On the **Fault Notification** tab, click **Syslog Forwarder**, and complete the fields as follows.

Field	Action
Enable Syslog Notification	Select Yes.
Admin Domain	Select Current Admin Domain.
Syslog Server - Host IP address	Enter the Log Decoder IP address.
Syslog Server - Port	Select 514.
Facilities	Select Local user 7 (local7).

Field	Action
Severity Mapping - Informational to	Select Informational: informational messages.
Severity Mapping - Error to	Select Error: error conditions.
Severity Mapping - Warning to	Select Warning: warning conditions.
Severity Mapping - Critical to	Select Emergency: system is unusable.
Forward Faults	Select By severity With severity Informational and above.

b. In the **Message Preferences** field, select **Customized**.

c. Click **Edit**.

d. In the **Message** field, type:

```
Fault : |FAULT_TIME = $IV_FAULT_TIME$|ADMIN_DOMAIN = $IV_ADMIN_
DOMAIN$|SENSOR_NAME = $IV_SENSOR_NAME$|FAULT_LEVEL = $IV_FAULT_
LEVEL$|FAULT_TYPE = $IV_FAULT_TYPE$|FAULT_NAME = $IV_FAULT_NAME$|FAULT_
SOURCE = $IV_FAULT_SOURCE$|FAULT_COMPONENT = $IV_FAULT_COMPONENT$|OWNER_
ID = $IV_OWNER_ID$|OWNER_NAME = $IV_OWNER_NAME$|SEVERITY = $IV_
SEVERITY$|DESCRIPTION = $IV_DESCRIPTION$|ACK_INFORMATION = $IV_ACK_
INFORMATION$|
```

e. Click **Save**.

f. Click **Apply**.

7. Enable the collection of Audit messages.

- a. On the **Audit Notification** tab, complete the fields as follows:

Field	Action
Enable Syslog Forwarder	Select Yes .
Admin Domain	Select Current .
Server Name or IP Address	Enter the Log Decoder IP address.
Port	Type 514 .
Facilities	Select Local user 7 (local7) .
Result Mapping	
Failed to	Select Error: error conditions .
Successful to	Select Notice: normal but significant condition .
In Progress to	Select Informational: informational messages .
Forward Alerts	Select Allow All Auditlogs .

In the **Message Preferences** field, select **Default** or **Customized**.

If you selected **Default**, skip to step 19. If you selected **Customized**, perform the following tasks:

- b. Click **Edit**.
 - c. In the **Message** field, type:


```
Audit : |AUDIT_TIME = $IV_AUDIT_TIME$|AUDIT_CATEGORY = $IV_AUDIT_CATEGORY$|AUDIT_DOMAIN = $IV_AUDIT_DOMAIN$|AUDIT_USER = $IV_AUDIT_USER$|AUDIT_RESULT = $IV_AUDIT_RESULT$|AUDIT_ACTION = $IV_AUDIT_ACTION$|AUDIT_MSG = $IV_AUDIT_MESSAGE$ |
```
 - d. Click **Save**.
 - e. Click **Apply**.
8. Enable the collection of ACL messages.

- a. On the **Firewall** tab, click **Rule Match Notification**.
- b. To configure Network Security Platform to send syslog data to RSA NetWitness Platform, complete the fields as follows.

Field	Action
Enable Syslog Forwarder	Select Yes .
Admin Domain	Select Current .
Server Name or IP Address	Enter the Log Decoder IP address.
Port	Type 514 .
Facility	Select Local user 7 (local7) .
Severity	Select Informational: informational messages .

- c. In the **Message Preferences** field, select **Customized**.
- d. Click **Edit**.
- e. In the **Message** field, type:

```
ACL : |SENSOR_NAME=$SENSOR_NAME$|ALERT_DIRECTION=$ALERT_DIRECTION$|ACL_
RULE=$ACL_POLICY$|ACL_RULE_NUMBER=$ACL_RULE_NUMBER$|SRC_IP_
PORT=$SOURCE_IP$:$SOURCE_PORT$|DST_IP_PORT=$DESTINATION_
IP$:$DESTINATION_PORT$|ACL_ACTION=$ACL_ACTION$|APP_
PROTOCOL=$APPLICATION_
PROTOCOL$|APP=$APPLICATION$|INTERFACE=$INTERFACE$|NET_
PROTOCOL=$NETWORK_PROTOCOL$|ALERT_DURATION=$ALERT_DURATION$|
```

- f. Click **Save**.
- g. Click **Apply**.

Configure Network Security Platform 3.1, 4.1, 5.1, or 6.1 for Syslog Collection

To configure McAfee Network Security Platform 3.1, 4.1, 5.1, or 6.1:

1. Log on to Network Security Platform with Administrator credentials.
2. Click **Configure**.
3. Select the appropriate Admin Domain.
4. If you are configuring Network Security Platform 5.1, select **IPS Settings**.
5. On the **Alert Notification** tab, click **Syslog Forwarder**.
6. If you are configuring Network Security Platform 5.1, select the **Syslog** tab.
7. To configure Network Security Platform to send syslog data to RSA NetWitness Platform, complete the fields as follows.

Field	Action
Enable Syslog Forwarder	Select Yes .
Enable Domain Notification	Select Current Admin Domain .
Syslog Server - Host IP address	Enter the Log Decoder IP address.
Syslog Server - Port	Type 514 .
Facilities	Select Local user 7 (local7) .
Severity Mapping - Informational to	Select Informational: informational messages .
Severity Mapping - Low to	Select Error: error conditions .
Severity Mapping - Medium to	Select Warning: warning conditions .
Severity Mapping - High to	Select Emergency: system is unusable .

Field	Action
Forward Alerts	Select By severity With severity Informational and above.

8. In the **Message Preferences** field, select **Customized**.
9. Click **Edit**.
10. In the **Message** field, type:

Warning: If you are using McAfee Network Security Platform with Content 2.0, add **\$IV_RESULT_STATUS\$|IV_CATEGORY\$** at the end of this string.

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|"$IV_ATTACK_NAME$"  
|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_SIGNATURE$|$IV_ATTACK_  
CONFIDENCE$  
  
|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_INTERFACE$|$IV_SOURCE_IP$|$IV_  
SOURCE_PORT$  
|$IV_DESTINATION_IP$|$IV_DESTINATION_PORT$|
```

11. Click **Save**.
12. Click **Apply**.

Configure Network Security Platform 2.1 for Syslog Collection

To configure McAfee Network Security Platform 2.1:

1. Log on to the Network Security Platform with Administrator credentials.
2. Click **Configure**.
3. In the System Configuration window, follow these steps to configure the Syslog Forwarder:
 - a. From the list, select **Organization name**.
 - b. On the **Alert notification** tab, click **Syslog Forwarder**.
 - c. In the Syslog Server window, enter the IP address or hostname of the LogSmart collector.
 - d. Select **Enable Syslog forwarder**.
 - e. Ensure the default port is **514**.
 - f. Under **Facilities**, select **Local user 7 (local 7)**.
 - g. In the **Severity Mapping** section, set the following settings.

Field	Action
Informational	Select Informational: informational messages .
Low	Select Error: error conditions .
Medium	Select Warning: warning conditions .
High	Select Emergency: system unusable .

- h. From the drop-down list, select **Forward alerts with severity**.
 - i. Click **Apply**.
4. Follow these steps to configure Syslog Message:

a. In the **Message Preference** field, select **Customized**.

b. Click **Edit**.

c. Click **Customize** to create a message.

d. Click **Edit**.

e. In the **Message** field, type:

```
|$IV_ALERT_ID$|$IV_ALERT_TYPE$|$IV_ATTACK_TIME$|  
"$IV_ATTACK_NAME$"$|$IV_ATTACK_ID$|$IV_ATTACK_SEVERITY$|$IV_ATTACK_  
SIGNATURE$  
|$IV_ATTACK_CONFIDENCE$|$IV_ADMIN_DOMAIN$|$IV_SENSOR_NAME$|$IV_  
INTERFACE$  
|$IV_SOURCE_IP$|$IV_SOURCE_PORT$|$IV_DESTINATION_IP$|$IV_DESTINATION_  
PORT$|
```

f. Click **Save**.

g. Click **Apply**.

Configure NetWitness Platform for Syslog Collection

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 **ADMIN > 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 **intrushield**.



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 **ADMIN > 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 **ADMIN > 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 © 2019 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.