

RSA NetWitness Platform

Event Source Log Configuration Guide



RSA SecurID Access

Last Modified: Thursday, February 25, 2021

Event Source Product Information:

Vendor: [RSA, The Security Division of Dell | EMC](#)

Event Sources: Authentication Manager, Identity Router, RSA SecurID Access (Cloud Authentication Service)

Supported On:

- Authentication Manager and Identity Router: RSA NetWitness Platform 10.0 and later
- Cloud Authentication Service:
 - RSA Security Analytics 10.6.6
 - RSA NetWitness Platform 11.2 and higher

Event Source Class.Subclass: Security.Access Control

RSA Product Information

| Component | Version | Collection Method | Parser |
|---|---------------------|-------------------|---|
| Authentication Manager | 8.x | Syslog | rsaacesrv |
| RSA Identity Router (previously Via Access) | All latest versions | Syslog | rsaviaaccess |
| RSA SecurID Access Cloud Authentication Service | All latest versions | Plugin Framework | cef, rsasecuridaccess for v11.5&beyond (device.type=rsasecuridaccess) |

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.

Note: For 11.5.x and beyond, NetWitness can now parse JSON event data directly on the Log Decoder and there is no need to transform logs into CEF. Previously, plugins had to be tailored to each JSON schema individually. Now, all of the raw JSON event data can be sent straight to the Log Decoder. In v11.5, the plugin can collect logs in JSON event data and will pass them through to Log decoder directly in RFC 5424 format by adding a header, and it will be parsed by the JSON parser instead of the CEF parser (based on Raw JSON Event Parameter setting).

RSA SecurID Access provides the benefits and functionality of RSA Authentication Manager and Cloud Authentication Service combined into one product. This integration enables new capabilities for existing RSA Authentication Manager Enterprise and Premium Edition customers.

RSA NetWitness Platform can consume Admin activity logs from RSA SecurID Access Log Events API via the RSA Netwitness plugin framework.

Components

RSA SecurID Access is comprised of the following components:

- **RSA Authentication Manager**

RSA Authentication Manager is an on-premise multifactor, authentication solution that helps secure access to network and web-accessible applications, such as SSL-VPNs and web portals. RSA Authentication Manager supports syslog collection.

- **Identity Router**

The identity router is an on-premise virtual appliance that communicates with the Cloud Authentication Service and enforces authentication and access for users of protected resources. The RSA Identity Router supports syslog for log collection.

- **Cloud Authentication Service**

The Cloud Authentication Service is an access and authentication platform with a hybrid on-premise and cloud-based service architecture. The Cloud Authentication Service helps secure access to SaaS and on-premise web applications for users, with a variety of authentication methods that provide multifactor identity assurance. The Cloud Authentication Service supports a REST API for log collection.

For more information about RSA SecurID Access, please see [RSA SecurID Access Overview](#) on RSA Link.

Configuration Overview

Choose which components to configure, based on the needs of your organization.

- [Configure RSA Authentication Manager](#)
- [Configure Identity Router to Send Syslog](#)
- [Configure the SecurID Access Event Source](#)

Configure the RSA NetWitness Platform:

- [Configure RSA NetWitness Platform for Syslog](#)
- [Set Up the SecurID Event Source in NetWitness Platform](#)

Configure RSA Authentication Manager

Configure RSA Auth Manager 8.x to Send Syslog:

1. Log on to the RSA Authentication Manager Security Console, and navigate to **Setup > System Settings**.
2. In the **Basic Settings** section, select **Logging**.
3. Select the instance from which you want to collect logs, and click **Next**.
4. In the **Log Levels** section, complete the fields as follows:

| Field | Action |
|--------------------------|-------------------------|
| Administrative Audit Log | Select Success . |
| Runtime Audit Log | Select Success . |
| System Log | Select Warning . |

5. In the **Log Data Destination** section, complete the fields as follows:

| Field | Action |
|-------------------------------|---|
| Administrative Audit Log Data | Select Save to remote database and internal Syslog at the following hostname or IP address , and enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector. |
| Runtime Audit Log Data | Select Save to remote database and internal Syslog at the following hostname or IP address , and enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector. |
| System Log Data | Select Save to remote database and internal Syslog at the following hostname or IP address , and enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector. |

6. Click **Save** to save changes.

Configure Identity Router to Send Syslog

To configure the Identity Router component, perform the following steps:

1. Log onto RSA SecurID Access Admin Logging console using Super Administrator credentials.

The Identity Router dashboard is displayed.

2. On the Identity Router dashboard, click **Platform > Auditing**.

The Audit Logging screen is displayed.

3. On the Audit Logging screen, for the **Output Type** field, select **Send to syslog**.

4. In the Syslog Configuration section, for the **Server** field, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

5. Select the following items:

- For **Log user events**, check **Include authorization requests**.
- For **Log system events**, check **Include system error events**.

6. Click **Save** to save your changes, and return to the Dashboard.

7. In the Dashboard, click **Publish Changes**.

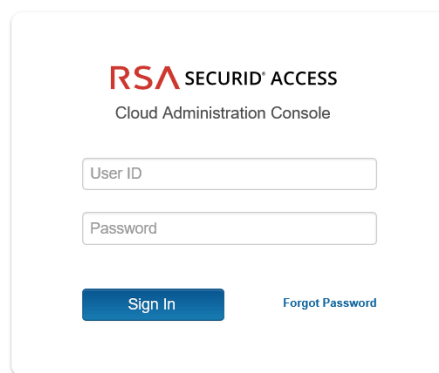
The toolbar changes from blue to green to indicate that your changes were successful, and Identity Router is now sending syslog according to your configuration settings.

Configure the SecurID Access Event Source

To configure the SecurID Access, you must generate an API key.

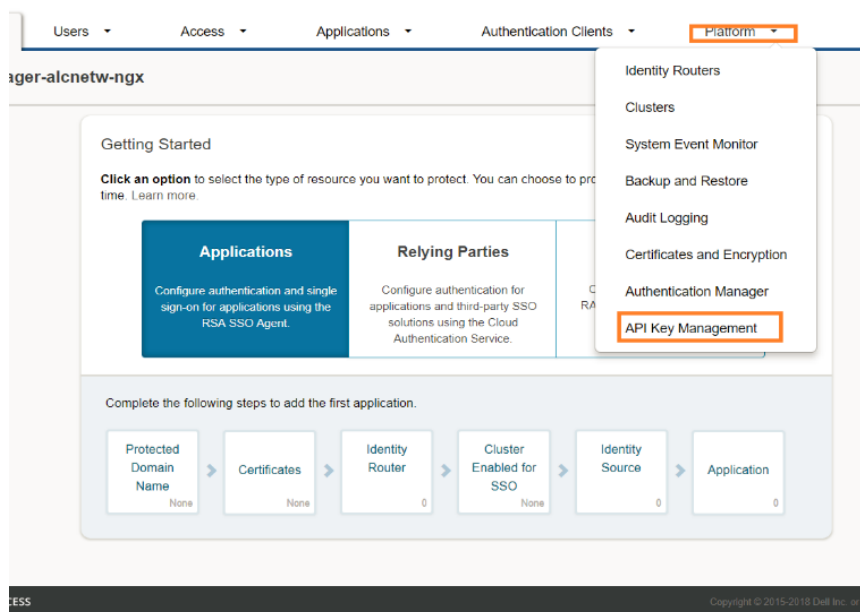
To generate an API Key:

1. Log onto the RSA SecurID Access Cloud Authentication Service console.
2. Enter user ID and password and click **Sign-in**.

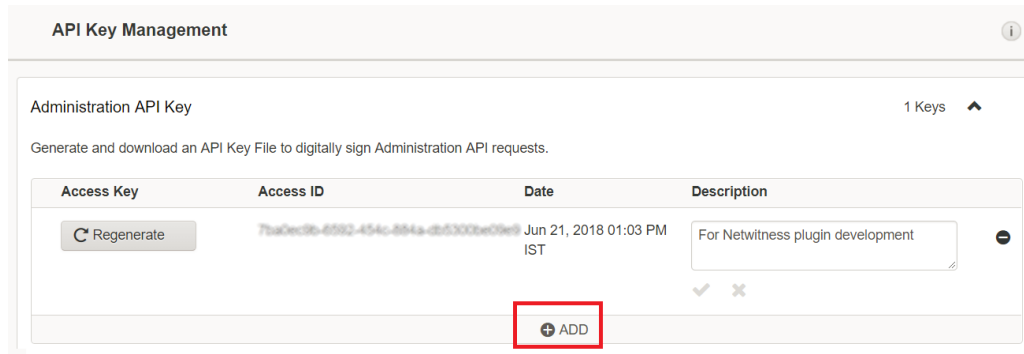


Copyright © 2015-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

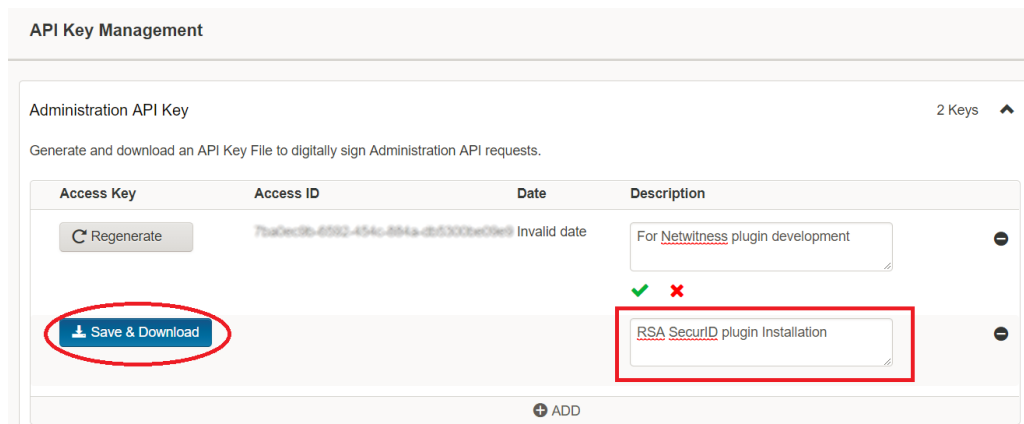
3. Click the **Platform** tab, then select **API key management** from the drop-down menu.



4. Click **ADD** to add an API key.



5. Fill in the key description and click **Save & Download**.



A key file in JSON is created and downloaded. The downloaded file contains API Access ID and Access Key shown below.

```
{
  "customerName": "Netwitness",
  "accessID": "7ba0ec9b-6592-454c-884a-d85300be09e9",
  "description": "",
  "accessKey": "-----BEGIN RSA PRIVATE
  KEY-----
  MIIEpAIBAAKCAQEA...
  -----END RSA PRIVATE
  KEY-----"
}
```

To complete configuration, see [Set Up the SecurID Event Source in NetWitness Platform](#).

Configure RSA NetWitness Platform for Syslog


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 RSANetWitness 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.
 - The required parser for RSA Authentication Manager is **rsaacesrv**.
 - The required parser for RSA Identity Router is **rsaviaaccess**.

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.

After 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.

Set Up the SecurID Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

- Deploy the SecurID package and CEF/rsasecuridaccess parser from Live.
- Configure the event source.

Deploy the SecurID Files from Live

SecurID requires resources available in Live in order to collect logs.

Note: For NetWitness 11.5.x and beyond, While Configuring the SecurID Event Source in the RSA NetWitness Platform, by default Enable Raw JSON Event parameter will be set to False.

Based on the value for the parameter “Enable Raw JSON Event” choose the appropriate parser.

1. If Enable Raw JSON Event set to false, then use cef parser. (Default setting)
2. If Enable Raw JSON Event set to true, then use rsasecuridaccess parser.

To deploy the SecurID content from Live:

1. Browse **Live** for the cef/rsasecuridaccess parser, using RSA Log Device as the Resource Type.
2. Select the **cef/rsasecuridaccess** parser from the list.
3. Click **Deploy** to deploy the cef/rsasecuridaccess parser to the appropriate Log Decoders, using the Deployment Wizard.
4. You also need to deploy the SecurID package. Browse **Live** for SecurID Log Collector configuration content, typing "SecurID" into the Keywords text box, then click **Search**.
5. Select the item returned from the search.
6. Click **Deploy** to deploy the SecurID log collection package to the appropriate Log Collectors, using the Deployment Wizard.
7. Restart the nwlogcollector service.

Note: The rsasecuridaccess parser can be used only for versions 11.5.x and beyond. Wherein cef parser can be used in versions 11.4.x and beyond.

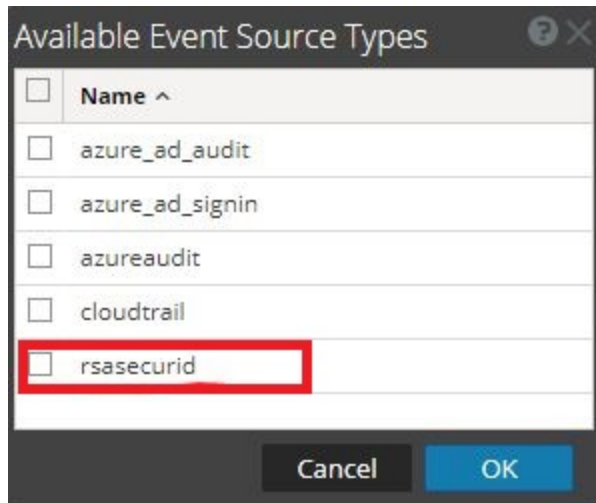
Note: If the RSA SecurID log collection package is updated from version 0.3 to 0.4, you must restart the Log Collection service.

For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the [Live Services Management Guide](#).

Configure the SecurID Event Source in the RSA NetWitness Platform

1. In the RSA NetWitness Platform menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View > Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.
The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click **+**.

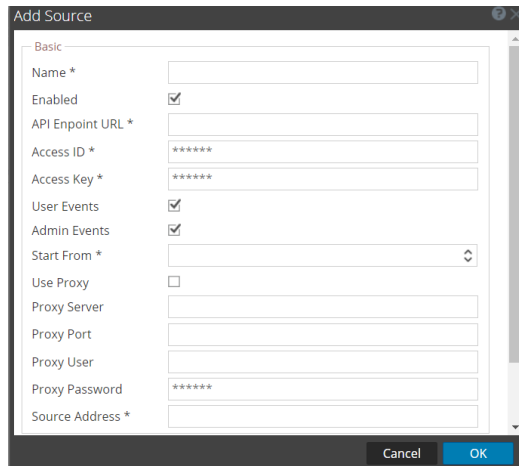
The Available Event Source Types dialog is displayed.



5. Select **rsasecurid** from the list, and click **OK**.
The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click **+** in the Sources panel toolbar.

The Add Source dialog is displayed.



7. Define parameter values, as described below, in [RSA SecurID Access Parameters](#).
8. Click **Test Connection**.

The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.
The new event source is displayed in the Sources panel.
10. Repeat steps 4–9 to add another SecurID plugin type.

RSA SecurID Access Parameters

The following table describes the parameters that you need to enter when you configure SecurID event source. Items marked with an asterisk (*) are required; all other parameters are optional.

Basic parameters

| Name | Description |
|-------------------------------|--|
| Name * | Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen. |
| Enabled | Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default. |
| API Endpoint URL * | The Endpoint URL for Secure ID Access Admin Logging Rest API. For example, https://xxx.securid.com/ |
| Access ID* | Access ID obtained from the API Key JSON file |
| Access Key* | The access Key obtained from the API key JSON file |
| User Events | Specifies whether or not to collect user events. By default, this is selected. Uncheck if you do not want to collect User Events |
| Admin Events | Specifies whether or not to collect admin events. By default, this is selected. Uncheck if you do not want to collect Admin Events |
| Start From (In Days) * | Starts collection from specified number of days in past from current time |
| Use Proxy | Check to enable proxy. |
| Proxy Server | If you are using a proxy, enter the proxy server address. |
| Proxy Port | Enter the proxy port. |
| Proxy User | Username for the proxy (leave empty if using anonymous proxy). |
| Proxy Password | Password for the proxy (leave empty if using anonymous proxy). |
| Source Address | A custom value chosen to represent the IP address for the SecurID Event Source in the customer environment. The value of this parameter is captured by the device.ip meta key |
| Enable Raw JSON | This parameter is applicable only on LC version 11.5 or above. Default behavior is that the raw events are transformed to cef format. Enabling |

| Name | Description |
|------------------------|---|
| Event | Raw JSON Event skips the transformation as the raw JSON events are sent to decoder in syslog 5424 format. To parse these logs collected in raw JSON format, need to deploy rsasecuridaccess parser from live. |
| Test Connection | Checks the configuration parameters specified in this dialog to make sure they are correct |

Advanced Parameters

| Parameter | Description |
|---------------------------|---|
| Polling Interval | Interval (amount of time in seconds) between each poll. The default value is 180. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy. |
| Max Duration Poll | Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600. |
| Max Events Poll | The maximum number of events per polling cycle (how many events collected per polling cycle). |
| Max Idle Time Poll | Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. |
| Command Args | Optional arguments to be added to the script invocation. |

| Parameter | Description |
|---------------------------|---|
| <p>Debug</p> | <div data-bbox="531 344 1417 520" style="border: 1px solid yellow; background-color: #ffffcc; padding: 5px;"> <p>Caution: Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector.</p> </div> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.</p> |
| <p>SSL Enabled</p> | <p>The check box is selected by default. Uncheck this box to disable SSL certificate verification.</p> |

© 2021 RSA Security LLC or its affiliates. All Rights Reserved.

November 2020

Trademarks

RSA Conference Logo, RSA, and other trademarks, are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.