RSA NetWitness Platform

Event Source Log Configuration Guide

Netskope Cloud Security Platform

Last Modified: Monday, September 17, 2018

Event Source Product Information:

Vendor: Netskope Security Cloud
Event Source: Netskope Cloud Security Platform
Versions: API v1.0

RSA Product Information:

Supported On:

- Security Analytics 10.6.4 and later
- NetWitness Platform 11.0 and later

Event Source Log Parser: cef

Note: The CEF parser parses this event source as **device.type=netskopecloudsecurityplatform**.

Collection Method: Plugin Framework
Event Source Class.Subclass: Host.Cloud

To configure Netskope Cloud Security Platform, you must complete these tasks:

I. Configure the Netskope Cloud Security Platform event source

II. Set Up the Netskope Event Source in RSA NetWitness

About Netskope Cloud Security Platform

The Netskope Security Cloud helps organizations take advantage of the cloud and web without sacrificing security. Their Cloud XD technology targets and controls activities across thousands of cloud services and millions of websites. Netskope provides 360-degree data protection that guards data everywhere and advanced threat protection that stops elusive attacks.

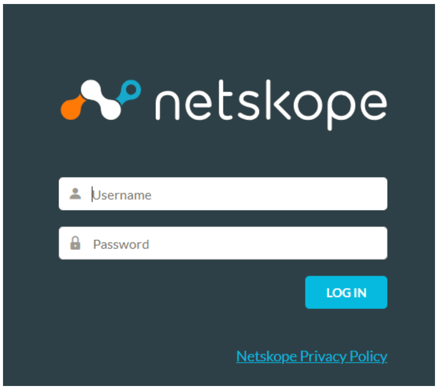
Netskope provides different kinds of alerts and different kinds of events like page events, application events, audit events and infrastructure events. Additionally, Netskope provides the API support to fetch all these kinds of alerts and events.

Configure the Netskope Cloud Security Platform event source

To configure the Netskope Cloud Security Platform, you must generate an API Key.

To generate an API Key:

1. At the Netskope Cloud Security Platform login page, enter your credentials and click LOG IN.



2. Perform the following steps to create administrators.

   a. Login to the Netskope tenant UI as the tenant administrator.

   b. Navigate to **Settings** > **Administration** > **Admins**.

   c. Click **New Admin**.

   d. Enter an email address (username) and for password, choose to generate a password automatically or create one. If you create a password, note the password requirements.

   e. Select the radio button for how to provide the password for the new admin.

      - Note the username and password if you opt to manually provide the password.
      - Note the password restrictions for the admin user.
      - If you use the default selection to generate a new password, the administrator is prompted to change the password upon first log in.
      - You can delete the admin user any time.

   f. Select the tenant admin role to assign the new admin. This is a top-level admin that has all privileges, including the ability to view the API token and generate new tokens as needed.

   g. Click Create to notify the new tenant admin.

3. Find and copy your REST API token. This screen is ONLY viewable to the tenant admin. However, the API token, once copied, may be used regardless of login credentials (it acts as its own user identity).

   a. Navigate to the API section of the Netskope UI: **Settings > Tools > Rest API**.

   b. Copy the existing token to your clipboard. Alternatively, you can generate a new token and copy it to your clipboard.

Set Up the Netskope Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

I. Deploy the CEF parser from Live

II. Configure the event source.

Deploy the CEF Parser from Live

Netskope Cloud Security Platform requires resources available in Live in order to collect logs.

To deploy the cef parser from Live:

1. In the RSA NetWitness Platform menu, select **CONFIGURE**.

   The **Live Content** tab is displayed.

2. Browse Live Content for the **Common Event Format (cef)** parser, using **Log Device** as the **Resource Type**.
3. Select the **cef** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.
4. You also need to deploy the Netskope package. Browse Live for Netskope content, typing "netskope" into the Keywords text box, then click **Search**.
5. Select the item returned from the search.
6. Click **Deploy** to deploy the Netskope Log Collection package to the appropriate Log Collectors, using the Deployment Wizard.
7. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Services Management Guide*.

Configure the Event Source

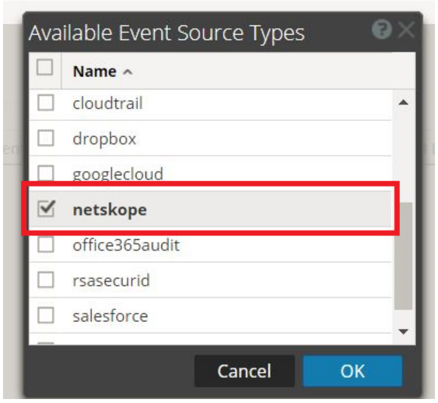
This section contains details on setting up the event source in RSA NetWitness Platform.

To configure the Netskope Event Source:

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.



Available Event Source Types

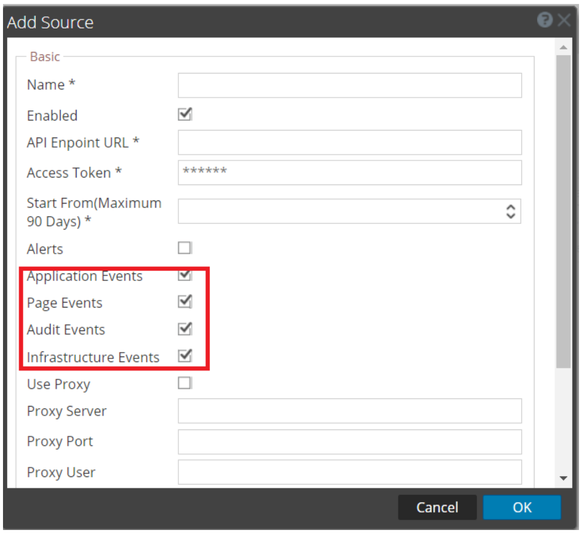
□	**Name** ^
□	cloudtrail
□	dropbox
□	googlecloud
☑	**netskope**
□	office365audit
□	rsasecurid
□	salesforce

5. Select **netskope** 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. You need to create 2 instances:
   - One instance collects events (page, application, audit and infrastructure)
   - Second instance collects Netskope Cloud Security Platform alerts

   a. For collecting Events, create an instance, then uncheck the **Alerts** checkbox and check the Event types you want to collect (choose from **Application**, **Page**, **Audit** and **Infrastructure**).



Name *	
Enabled	☑
API Enpoint URL *	
Access Token *	******
Start From(Maximum 90 Days) *	
Alerts	☐
Application Events	☑
Page Events	☑
Audit Events	☑
Infrastructure Events	☑
Use Proxy	☐
Proxy Server	
Proxy Port	
Proxy User	

b. Define parameter values, as described in Netskope Collection Configuration Parameters.

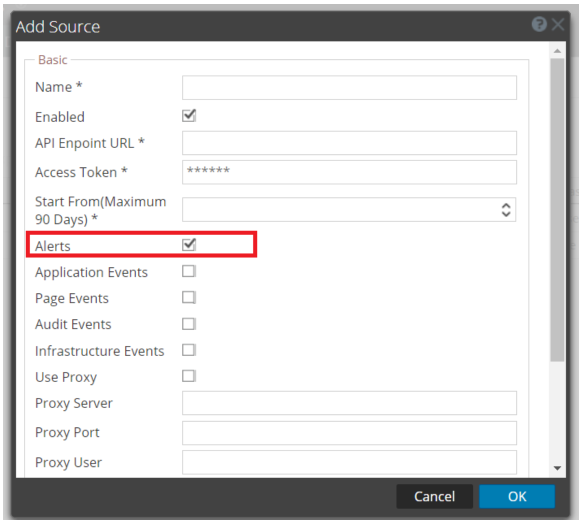
c. Click **Test Connection**.

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.

d. If the test is successful, click **OK**. The new event source is displayed in the Sources panel.

e. Repeat steps a–d to create an instance for Alerts. In this case you need to uncheck the **Application**, **Page**, **Audit**, **Infrastructure** boxes and select only the **Alerts** checkbox.



Add Source

Basic

Name *

Enabled ☑

API Enpoint URL *

Access Token * ******

Start From(Maximum 90 Days) *

Alerts ☑

Application Events □

Page Events □

Audit Events □

Infrastructure Events □

Use Proxy □

Proxy Server

Proxy Port

Proxy User

Netskope Collection Configuration Parameters

The following tables describe the configuration parameters for the Netskope Cloud Security Platform integration with RSA NetWitness Platform. Fields marked with an asterisk (*) are required.

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 box to enable the event source configuration to start collection. The box is selected by default.
API Endpoint URL *	The Endpoint URL for Netskope Cloud Security Platform Admin Logging REST API. For example: `https://XXX.goskope.com/`
Access Token *	Access token obtained from admin interface.
Start From (In Days) *	Specifies the number of days prior to the current time, from which log collection should start.
Alerts	Select to collect the alerts. Clear to collect events. This box is selected by default.
Page Events	Select to collect the Page events.
Application Events	Select to collect the Application events.
Audit Events	Select to collect the Audit events.
Infrastructure Events	Select to collect the Infrastructure events.
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.

Name	Description
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 Netskope Cloud Security Platform Event Source in the customer environment. The value of this parameter is captured by the **device.ip** meta key.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Note: Please avoid using special characters in the **Proxy User** and **Proxy Password** sections.

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
Debug	**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. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. 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.
SSL Enabled	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

Trademarks

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