RSA NetWitness Platform

Event Source Log Configuration Guide

Google Workspace (G Suite)

Last Modified: Thursday, January 6, 2022

Event Source Product Information:

Vendor: Google
Product: Google Workspace (G Suite)
Event Source: G Suite Activity Reports API
Versions: API v1.0

RSA Product Information:

Supported On: NetWitness Platform 11.5 and later
Event Source Log Parser: googlesuite

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

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

To configure Google Workspace (G Suite), you must complete these tasks:

I. Configure the Google Workspace (G Suite) event source

II. Set Up Google Workspace (G Suite) Event Source in the RSA NetWitness Platform

About Google Workspace (G Suite)

Google Workspace (G Suite) is a brand of Google's productivity and collaboration tools. Google Workspace (G Suite) comprises Gmail, Hangouts, Calendar, Drive for storage; Docs, Sheets, Slides, Forms, and Sites for collaboration.

Google Workspace (G Suite) provides various activity reports to keep track of user and admin activities. These reports are classified into the following categories:

- **access_transparency** – The Google Workspace (G Suite) Access Transparency activity reports return information about different types of Access Transparency activity events.
- **admin** – The Admin console application's activity reports return account information about different types of administrator activity events.
- **calendar** – The Google Workspace (G Suite) Calendar application's activity reports return information about various Calendar activity events.
- **drive** – The Google Drive application's activity reports return information about various Google Drive activity events. The Drive activity report is only available for Google Workspace (G Suite) Business customers.
- **groups** – The Google Groups application's activity reports return information about various Groups activity events.
- **groups_enterprise** – The Enterprise Groups activity reports return information about various Enterprise group activity events.
- **login** – The Google Workspace (G Suite) Login application's activity reports return account information about different types of Login activity events.
- **mobile** – The Google Workspace (G Suite) Mobile Audit activity report return information about different types of Mobile Audit activity events.
- **rules** – The Google Workspace (G Suite) Rules activity report return information about different types of Rules activity events.
- **token** – The Google Workspace (G Suite) Token application's activity reports return account information about different types of Token activity events.
- **user_accounts** – The Google Workspace (G Suite) User Accounts application's activity reports return account information about different types of User Accounts activity events.

You can use the gsuite plugin to ingest these activity events into the NetWitness Platform.

Configure Google Workspace (G Suite) Event Source

You must configure Google Workspace (G Suite) to Perform Google Workspace (G Suite) Domain-Wide Delegation of Authority.

The domain administrator must grant domain-wide delegation of authority for NetWitness to programmatically access the Reports API without any manual intervention. Follow the steps provided in the following Google Workspace (G Suite) Admin SDK Reports API documentation:

- Get Started
- Perform Google Workspace (G Suite) Domain-Wide Delegation of Authority

Note: Save the service account's public/private key as a JSON file. You need the information provided in this file to fill in connection parameters later.

Set Up the Google Workspace (G Suite) Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

I. Deploy the Google Workspace (G Suite) files from Live

II. Configure the event source.

Deploy Google Workspace (G Suite) Files from Live

Google Workspace (G Suite) requires resources available in Live in order to collect logs.

To deploy the Google Workspace (G Suite) content from Live:

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

   The **Live Content** tab is displayed.

2. Browse Live Content for the **googlesuite** parser, using **Log Device** as the **Resource Type**.

3. Select the **googlesuite** parser from the list and click **Deploy** to deploy it to the appropriate Log Decoders, using the Deployment Wizard.

   > **Note:** Deploy **googlesuite** parser for parsing json formatted logs. (Refer Google Workspace (G Suite) Collection Configuration Parameters to enable JSON Event).

4. You also need to deploy the Google Workspace (G Suite) package. Browse Live for Gsuite EventLogs content, typing "gsuite" into the Keywords text box, then click **Search**.

5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

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

Configure the Event Source

To configure the Google Workspace (G Suite) Event Source:

1. In the RSA NetWitness Platform menu, select **ADMIN** > **Services**.

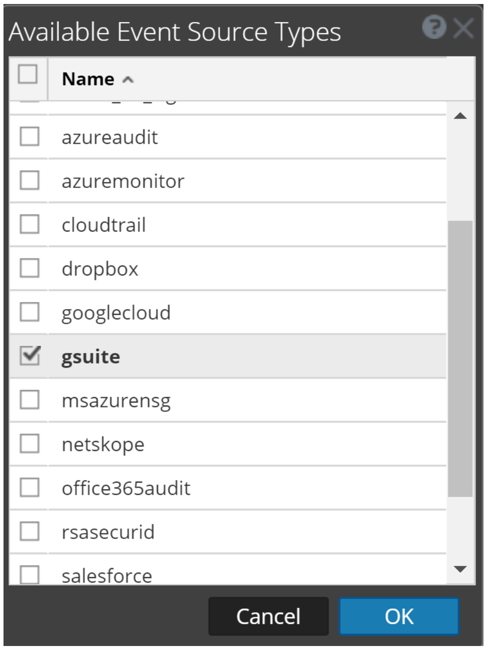
2. In the **Services** grid, select a Log Collector service, and from the **Actions** menu, choose **View** > **Config**.

3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel displays the configured File event sources, if any.

4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.



Available Event Source Types

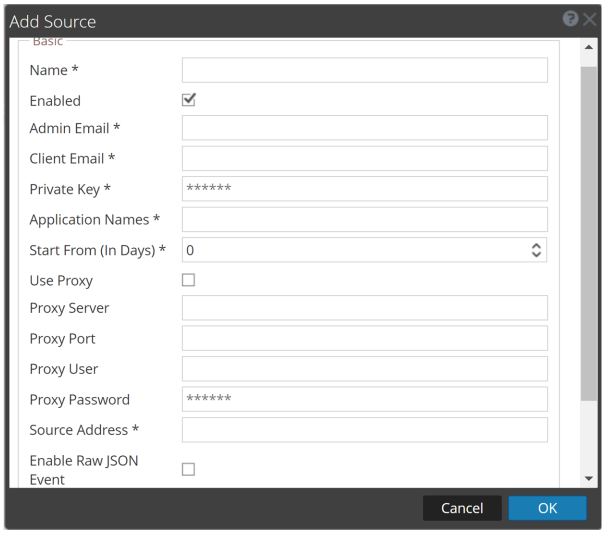
☐	Name ^
☐	azureaudit
☐	azuremonitor
☐	cloudtrail
☐	dropbox
☐	googlecloud
☑	**gsuite**
☐	msazurensg
☐	netskope
☐	office365audit
☐	rsasecurid
☐	salesforce

5. Select **gsuite** 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.



Add Source

Basic

Name *	
Enabled	☑
Admin Email *	
Client Email *	
Private Key *	******
Application Names *	
Start From (In Days) *	0
Use Proxy	☐
Proxy Server	
Proxy Port	
Proxy User	
Proxy Password	******
Source Address *	
Enable Raw JSON Event	☐

7. Define parameter values, as described in Google Workspace (G Suite) Collection Configuration Parameters.

8. Click **Test Connection**.

The test result 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. Click **OK** if the test is successful.

   The new event source is displayed in the Sources panel.

10. Repeat steps **4–9** to add another Google Workspace (G Suite) Event Source type.

Google Workspace (G Suite) Collection Configuration Parameters

The following table describes the configuration parameters for the Google Workspace (G Suite) integration with RSA NetWitness Platform.

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.
Client Email*	Client_email obtained from the downloaded service account JSON file.
Admin Email*	A Google Workspace (G Suite) domain admin email address.
Private Key*	The Private Key is obtained from the service account JSON file.
Application Names*	This is a comma-separated list of the event categories from which you want to collect. RSA recommends not to use a single instance of the plugin to collect all the categories. Allowed values: access_transparency, admin, login, token, calendar, drive, groups, groups_enterprise, mobile, rules, user_accounts. Sample Input: `admin, login` To collect all the categories' events in a single instance, enter `all` **Note:** The categories **access_transparency**, **drive**, **rules** and **mobile** are available only for Google Workspace (G Suite) Enterprise and Business accounts.
Start From (In Days)*	Specifies the number of days, prior to the current date, from which log collection should start.
Use Proxy	Select the checkbox 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 an anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using an anonymous proxy).
Source	The IP address that is to be provided to the gsuite plugin instance. (Logs from this event source

Name	Description
Address*	are collected with this device IP.)
Enable Raw JSON Event	Enable if gsuite plugin has to collect logs in JSON format. **Note:** Customers using the NetWitness Platform 11.5 or later must enable Raw JSON Event. If the NetWitness Platform version is before 11.5, customers must uncheck the Enable Raw JSON Event checkbox. In this case, logs will be parsed using cef.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Parameter	Description
Trail By (In Minutes)	Specifies the lag between current time and log collection. The default value is 60 minutes. This can be increased to 300 minutes or reduced to 5 minutes. **Note:** It was observed that some Google Workspace (G Suite) events take a while to be available via the API. If you collect too close to the current time, there is a possibility of missing some events.
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	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	The maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
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 and 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.

Parameter	Description
	This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
SSL Enable	Uncheck this box to disable SSL certificate verification.

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.