

# RSA NetWitness Platform

## Event Source Log Configuration Guide



## Cisco Umbrella

Last Modified: Wednesday, December 8, 2021

### Event Source Product Information:

**Vendor:** [Cisco](#)

**Event Source:** Cisco Umbrella

**Versions:** Schema Version 4

### RSA Product Information:

**Supported On:** NetWitness Platform 11.2.1 and later

**Event Source Log Parser:** cisco\_umbrella

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

**Collection Method:** Plugin Framework

**Event Source Class.Subclass:** Host.Cloud

**Note:** `ciscoumbrella` plugin will be deprecated soon. Customers can use `ciscoumbrella2` plugin to collect Cisco Umbrella logs.

To configure Cisco Umbrella, you must complete these tasks:

- I. Configure the Cisco Umbrella event source
- II. Set Up Cisco Umbrella Event Source in RSA NetWitness

## Configure the Cisco Umbrella Event Source

---

Cisco Umbrella uses the infrastructure of the Internet to block malicious destinations before a connection is established. Cisco Umbrella delivers security from the cloud, by observing your internet traffic, and blocking malicious destinations, then logs the activities. The RSA NetWitness Cisco Umbrella plugin is meant to collect these logs and send them to a SIEM, helping security analysts to analyze the different kinds of attacks, security breaches and so on.

For more information about Cisco Umbrella, see <https://umbrella.cisco.com>.

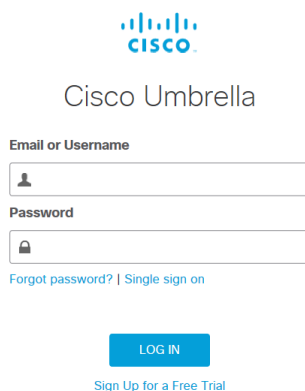
**Note:** The Cisco Umbrella plugin is meant for collecting the Cisco Umbrella DNS, Proxy and IP logs generated in your internet traffic. Cisco Umbrella logs are sent to S3 bucket and stored in comma separated gzip files.


## Enable Cisco Umbrella Log Management

In the Cisco Umbrella User Interface, you select the method of log management to use.

### To enable Cisco Umbrella:

1. Log onto your Cisco Umbrella account.



  
Cisco Umbrella

Email or Username

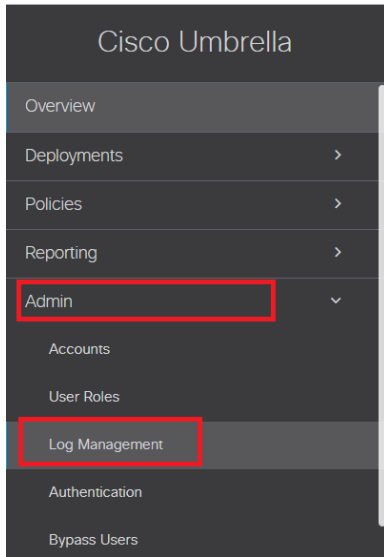
Password

[Forgot password?](#) | [Single sign on](#)

[LOG IN](#)

[Sign Up for a Free Trial](#)

2. After you log in, click **Admin > Log Management**.



3. Cisco Umbrella Log exports the logs to an AWS S3 bucket. Cisco Umbrella provides two options to configure the S3 bucket, and you can select either of the following options:

- Use your company-managed Amazon S3 bucket, or
- Use Cisco-managed Amazon S3 storage

Amazon S3

Status: Not Configured | Last Sync: Never

Use your company-managed Amazon S3 bucket

Cisco will write your logs to an Amazon S3 bucket provided and managed by your company. For setup instructions [view our guide](#).

We have recently updated our logs to include Proxy and IP logs, and made minor label and identity changes. For more information on these changes view the [log management export format document](#).

**Amazon S3 bucket**

Amazon S3 bucket name  [VERIFY](#)

Use Cisco-managed Amazon S3 storage

The setup for those options is described below.

## Configure a Self-Managed S3 Bucket

The following sections describe the required procedures:

- Create AWS User and Attach S3 Service Policies
- Configure S3 Bucket and Policy

### Create AWS User and Attach S3 Service Policies

If you do not have a user or role in your AWS environment, you must create one: RSA requires an AWS user or role to create an S3 bucket. The bucket is used to collect Cisco Umbrella logs: these logs are then read from the bucket.

For details on how to create users and roles, see [IAM Users](#) in the *Amazon AWS Identity and Access Management User Guide*. You must attach both read and write policies to the user or role.

**Note:** When you create the user or role, you receive a secret key and access key: these values are required when you configure Cisco Umbrella in RSA NetWitness Platform.

If you already have an S3 bucket and you want to read the logs from it, you need to attach S3 read access policy to the user or role. See [Adding and Removing IAM Identity Permissions](#) in the *Amazon AWS Identity and Access Management User Guide* for details of embedding an inline policy for a user or role.


## Configure S3 Bucket and Policy

You can use a self-managed bucket, where you own the bucket in Amazon and set up the configuration for it. To configure a self-managed bucket, follow the steps in the following Cisco support topic: [Setting up a self-managed Amazon bucket in S3](#).

After you configure your S3 bucket, you can view the details for it:

Amazon S3	Status	Last Sync
	● Active	Never

---

 We're sending data to your S3 storage.

<b>Data Path</b>	s3: <code>arn:aws:s3:::us-east-1-logs-umbrella-logs</code>
<b>Last Sync</b>	Never
<b>Schema Version</b>	v3   <a href="#">View Details</a>

Cisco will write your logs to an Amazon S3 bucket provided and managed by your company. For setup instructions [view our guide](#).

We have recently updated our logs to include Proxy and IP logs, and made minor label and identity changes. For more information on these changes view the [log management export format document](#).

[STOP LOGGING](#)

Cisco Umbrella will now begin sending logs to your S3 Bucket.

**Note:** Save the data path, your AWS account's secret key, and access details. You need to provide that information when you configure the plugin.

## Configure a Cisco-Managed S3 Bucket

You can use a Cisco-managed bucket, where Cisco owns the bucket. To configure a Cisco-managed bucket, follow the steps in the following Cisco support topic: [Cisco-managed Buckets in Amazon S3 for Log Management](#).

Once you configure your Cisco-managed bucket, an “Activation Complete” dialog box is displayed.

## Activation Complete!



Your keys are ready. Please keep them in a safe place. If you need to regenerate keys, *old keys will immediately and permanently lose access.*

**Data Path** s3: [redacted] 

**Access Key** [redacted] 

**Secret Key** [redacted] 

Got it!

**CONTINUE**

**Note:** Save the Data Path, Access Key and Secret Key, because you need to provide that information when you configure the plugin.

Click **Continue** to complete the configuration. Your logs will be exported to this bucket.

# Set Up the Cisco Umbrella Event Source in NetWitness Platform

---

In RSA NetWitness Platform, perform the following tasks:

- I. Deploy the **ciscoumbrella** package and **cisco\_umbrella** parser from Live
- II. Configure the event source.

## Deploy Cisco Umbrella Files from Live

Cisco Umbrella requires resources available in Live in order to collect logs.

### To deploy the Cisco Umbrella content from Live:

1. In the RSA NetWitness Platform menu, select **Live**. To browse Live for Cisco Umbrella plugin, type **ciscoumbrella** in the Keywords text box and click **Search**.

**Note:** Type **ciscoumbrella2** in the keywords text box and click **Search** to browse Live Cisco Umbrella content for the latest version.

2. Select the item returned from the Search.
3. Click **Deploy** to deploy the Cisco Umbrella content to the appropriate Log Collectors, using the Deployment Wizard.
4. Log Parser **cisco\_umbrella** have been added as required resources of Cisco Umbrella Plugin in RSA Live. Deploy the parser to appropriate Log Decoders when you deploy plugin log collection file.

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. In addition to the procedure, the Cisco Umbrella Collection Configuration Parameters are described, as well as how to collect Cisco Umbrella Events in NetWitness Platform.

### To configure the Cisco Umbrella Event Source:

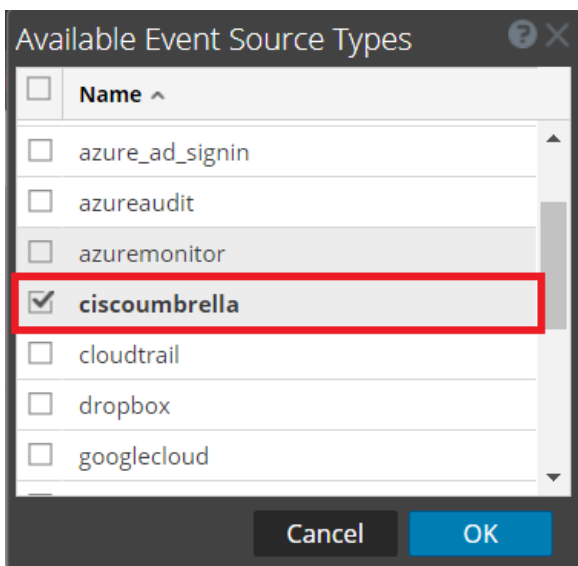
1. In the RSA NetWitness Platform menu, select **ADMIN > Services**.
2. In the **Services** grid, select a Log Collector service, and from the **Actions** menu, choose **View > Config**.

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

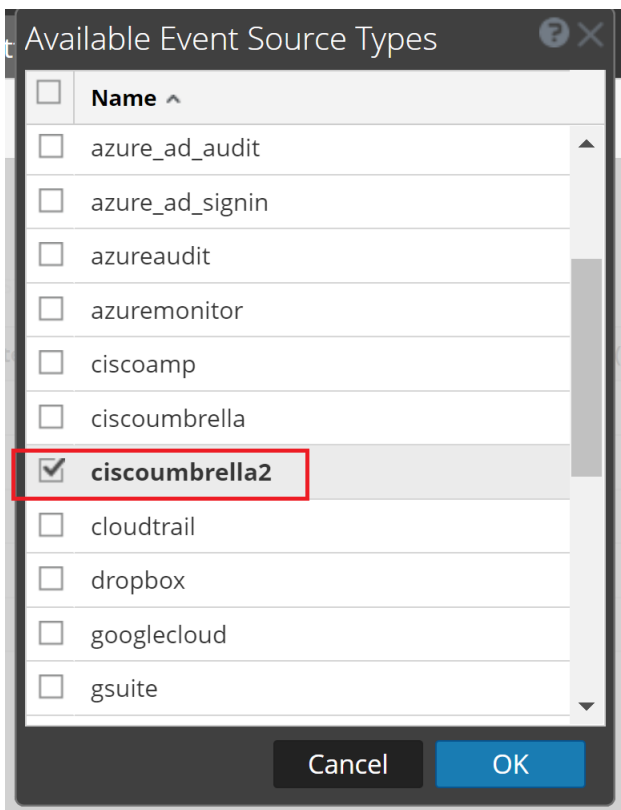
The **Event Categories** panel displays the File event sources that are configured, if any.

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

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



#### Cisco Umbrella v2 Plugin



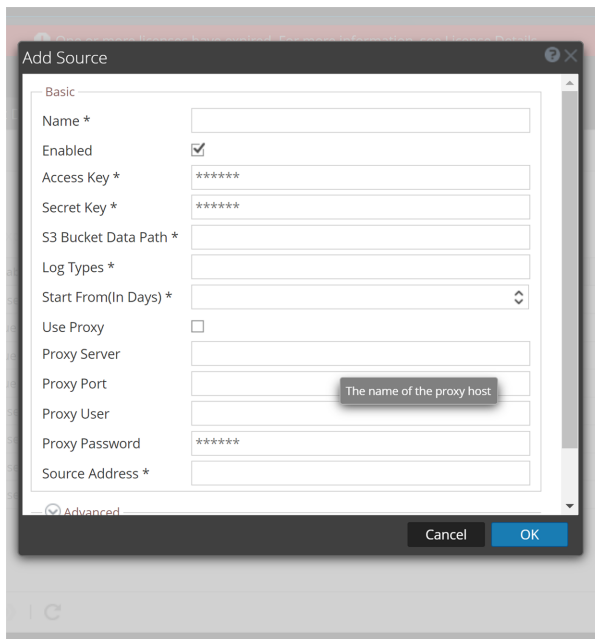
5. Select **ciscoumbrella** from the list, and click **OK**. To add the new version of the plugin, select **ciscoumbrella2** from the list.



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 in [Cisco Umbrella Collection Configuration 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.

# Cisco Umbrella Collection Configuration Parameters

The following tables describe the configuration parameters for the Cisco Umbrella 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.
Access Key *	Access key for the AWS account.
Secret Key *	Secret key for the AWS account.
S3 Bucket Data Path *	Data path where the Cisco Umbrella logs are being sent. To get your data path, navigate to <b>Admin &gt; Log Management</b> and the data path is displayed. <ul style="list-style-type: none"><li>For Cisco-managed buckets, the data path is always in the following format: <code>s3://&lt;cisco_managed_bucket_name&gt;/&lt;path&gt;</code></li><li>For self-managed buckets, the data path is always in the following format: <code>s3://&lt;your_bucket_name&gt;</code></li></ul> <div style="border: 1px solid green; padding: 5px;"><b>Note:</b> Remember to add <code>s3://</code> before your data path. Also, do not edit the S3 Bucket Data Path in the running event source instance. You should create a separate event source instance for a new S3 bucket Data Path.</div>
Start From (In Days)*	Specifies the number of days prior to the current time, from which log collection should start. <b>Maximum allowed value is 30.</b>
Log Type	Type of logs to be collected. For Example: dnslogs, proxylogs, and iplogs. <div style="border: 1px solid green; padding: 5px;"><b>Note:</b> Log Type is the new parameter for <b>ciscoumbrella2</b> plugin.</div>
Use Proxy	Check to enable proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.

Name	Description
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 Cisco Umbrella Event Source in the customer environment. The value of this parameter is captured by the <b>device.ip</b> 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
<b>Polling Interval</b>	Interval (amount of time in seconds) between each poll. The default value is <b>180</b> . For example, if you specify <b>180</b> , 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.
<b>Max Duration Poll</b>	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
<b>Max Events Poll</b>	The maximum number of events per polling cycle (how many events collected per polling cycle).
<b>Max Idle Time Poll</b>	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
<b>Command Args</b>	Optional arguments to be added to the script invocation.

Parameter	Description
<b>Debug</b>	<p><b>Caution:</b> 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> <p>Enables or disables debug logging for the event source. Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>Off</b> = (default) disabled</li> <li>• <b>On</b> = enabled</li> <li>• <b>Verbose</b> = enabled in verbose mode - adds thread information and source context information to the messages.</li> </ul> <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>
<b>SSL Enabled</b>	<p>The check box is selected by default.</p> <p>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.