NetWitness® Platform

Cisco Advanced Malware Protection for Endpoints Event Source Log Configuration Guide

NETWITNESS
Platform

Cisco Advanced Malware Protection for Endpoints

Last Modified: Thursday, July 25, 2024

Event Source Product Information:

Vendor: Cisco

Event Source: Cisco AMP

Versions: All

NetWitness Product Information:

Supported On: NetWitness Platform 12.2 and later

Event Source Log Parser: cef

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

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

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.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

July 2024

Contents

To configure Cisco Advanced Malware Protection (AMP) for Endpoints, you must complete these tasks:

I. Configure the Cisco AMP event source

II. Set Up Cisco AMP Event Source in NetWitness

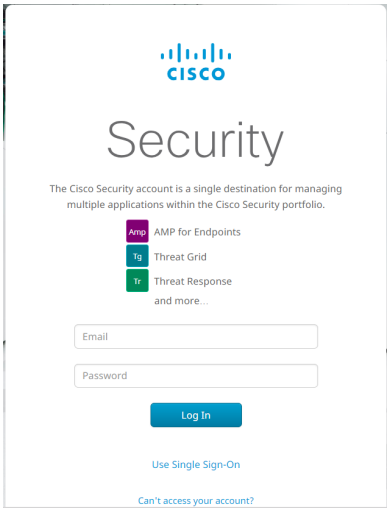
Configure the Cisco AMP Source

Cisco Advanced Malware Protection (AMP) for Endpoints prevents threats at point of entry, then continuously tracks every file it lets onto your endpoints. AMP can uncover advanced threats, including file-less malware and ransomware. The NetWitness Cisco AMP plugin collects the events generated in the amp endpoints (Audit, Domain Controller, IP Blocking Group, Protect, Server and Triage groups). For more information, see Cisco AMP for Endpoints.

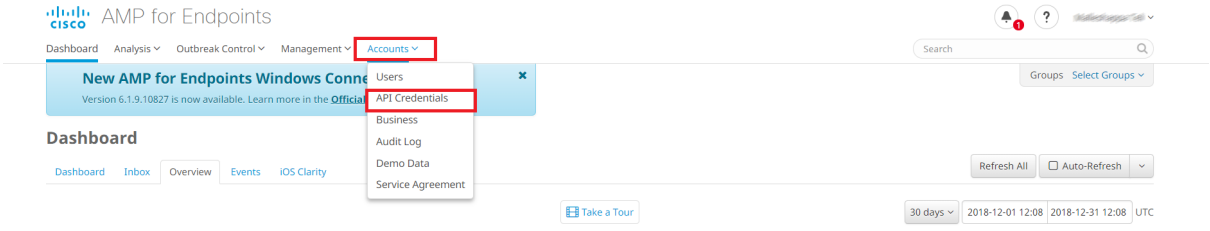
Enable Cisco Amp Log Management

To enable Cisco AMP:

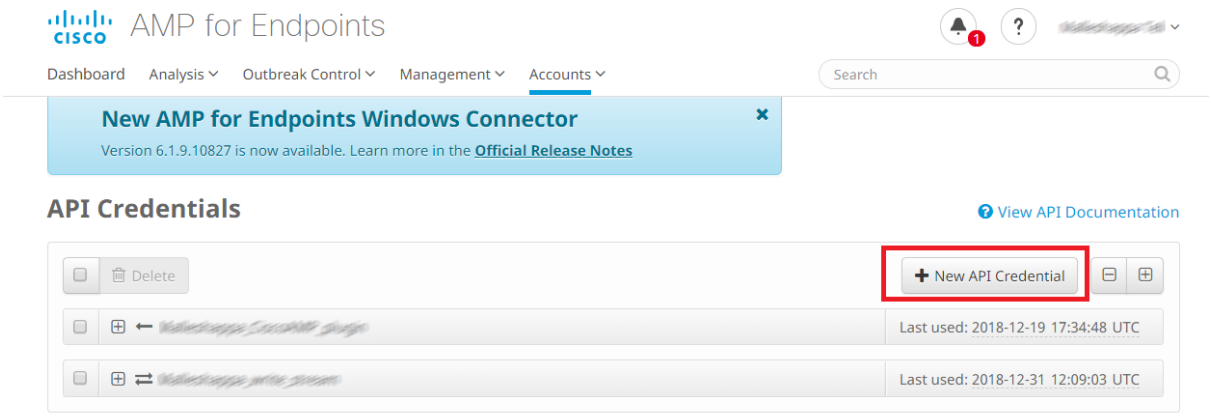
1. Log onto your Cisco AMP account.



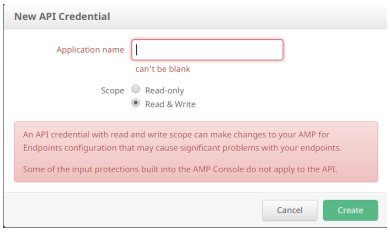
2. After you log in, click **Accounts > API Credentials**.



3. Click the **New API Credential** button.



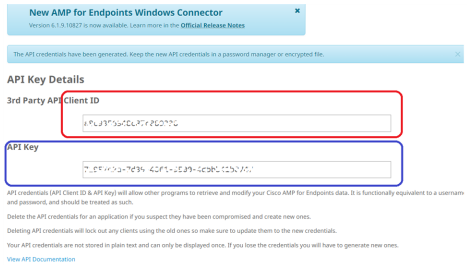
A new window is displayed:



4. Enter an **Application name**, ensure **Read & Write** is selected, and click **Create**.

   This generates your client ID and API key.

5. Copy both the client ID and API Key: you need them when you create an event stream.



Create an Event Stream

Cisco AMP pushes events to event streams (**event_streams**). Event streams contain the **event_stream_queue**, to where the events are queued. One organization can create a maximum of 5 **event_streams**.

To create an event_stream:

1. Log onto a NetWitness Log Collector, and navigate to the plugin directory using the following command:

   ```
   cd /etc/netwitness/ng/logcollection/content/collection/cmdscript/ciscoamp
   ```

2. Run the python script and respond to the prompts.

a. Run the command:

```
python3.9 create_event_stream.py
```

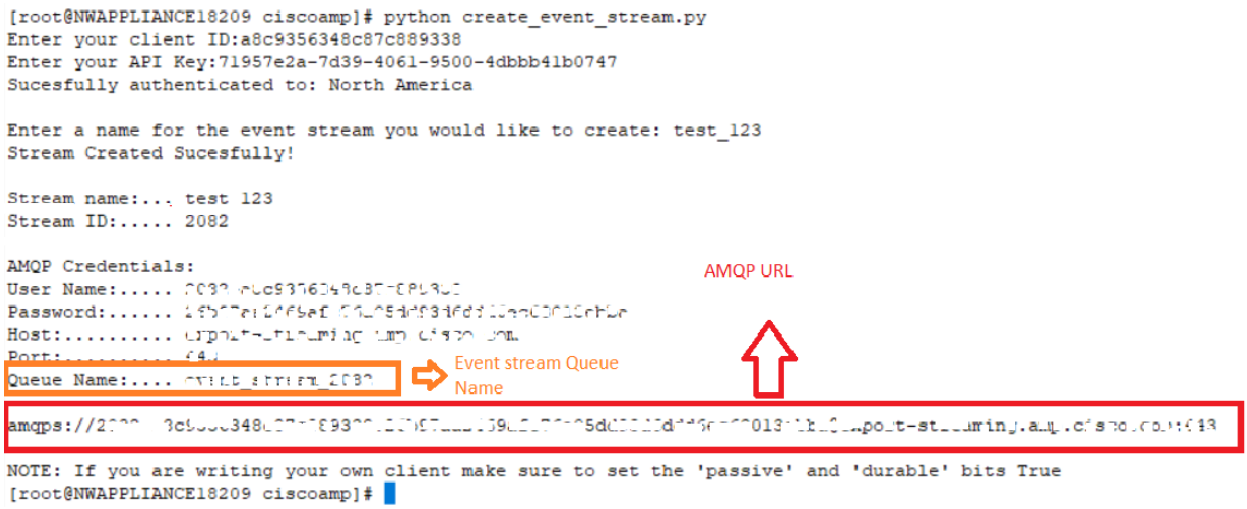
b. The script prompts you for your client ID: type it in and click **Enter**.

c. The script prompts you for your API key: type it in and click **Enter**.

If your client ID and API key values are correct, the script displays a message that you have successfully authenticated to your region.

d. The script prompts you to enter a name for the new event stream. Type in a name, and click **Enter**.

The event stream is created, and details are displayed, such as stream name, stream Id, AMQP credentials and AMQP URL. For example:



Note: Make sure to copy the AMQP URL and the Queue Name, as you need them when you configure the event source in NetWitness.

Set Up the Cisco AMP Event Source in NetWitness Platform

In NetWitness , perform the following tasks:

I. Deploy the **ciscoamp** package and CEF parser from Live

II. Configure the event source.

Deploy Cisco AMP Files from Live

Cisco AMP requires resources available in Live to collect logs.

To deploy the cef parser from Live:

1. In the 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 Cisco AMP package. Browse Live for Cisco AMP content, typing "Cisco Amp" into the Keywords text box, then click **Search**.
5. Select the package and click **Deploy** to deploy it to the appropriate Log Collectors.

   Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.
6. 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 NetWitness . In addition to the procedure, the Cisco AMP Collection Configuration Parameters are described, as well as how to collect Cisco AMP events in NetWitness Platform.

To configure the Cisco AMP Event Source:

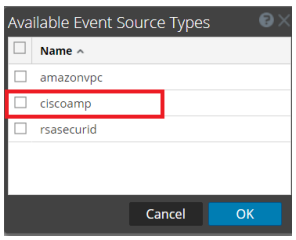
1. In the NetWitness Platform menu, select **ADMIN > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View > Config**.

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.

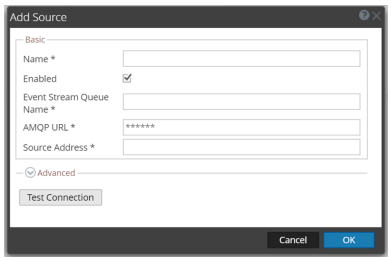


5. Select **ciscoamp** from the list, and click **OK**.

   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 in Cisco AMP 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 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 AMP Collection Configuration Parameters

The following tables describe the configuration parameters for the Cisco AMP integration with NetWitness . 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.
Event Stream Queue Name *	Enter the Event Stream Queue Name. This was displayed when you created the event stream earlier.
AMPQ URL*	Enter the AMPQ URL. This was displayed when you created the event stream earlier.
Source Address	A custom value chosen to represent the IP address for the Cisco AMP Logs 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.

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 idle time in seconds, of a polling cycle. Zero (0) indicates no limit, and 300 is the maximum value allowed.

Parameter	Description
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 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.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See the documentation for Logstash JDBC input plugin here: https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.