

RSA NetWitness Platform

Event Source Log Configuration Guide



VMware AppDefense

Last Modified: Friday, April 13, 2018

Event Source Product Information:

Vendor: [VMware](#)

Event Source: AppDefense

Versions: API v1.0

RSA Product Information:

Supported On: Security Analytics 10.6.2 and later

Event Source Log Parser: cef

Note: The CEF parser parses this event source as `device.type=vmwareappdefense`.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

To configure VMware AppDefense, you must complete these tasks:

- I. Getting Started with NetWitness Platform and VMware AppDefense
- II. Configure the VMware AppDefense event source
- III. Set Up VMware AppDefense Event Source in RSA NetWitness

Getting Started with NetWitness Platform and VMware AppDefense

VMware AppDefense is a data center security tool that enables Application Control, Detection, and Response. It is meant to provide foundation elements of Cloud Workload Protection, such as System Integrity, Application Control, and Memory Monitoring.

AppDefense is a multi-tenant web application. When a customer subscribes to AppDefense, an organization is provisioned for them, with an organization ID (**orgId**) that separates their data from other customers' data. To make this separation clear, all URLs for the AppDefense API are prefixed with the customer's **orgId**. VMware AppDefense provides a RESTful HTTP API for reading and modifying data via the cloud management console.

Configure the VMware AppDefense Event Source

Perform the following tasks to configure the event source:

- I. Deploy the AppDefense appliance
- II. Setup API Key – Access Token

Deploy the AppDefense appliance

Environment setup

Setup VMWare AppDefense appliance on-premise as per your organization infrastructure. Refer to the *AppDefense Installation Guide* for prerequisites and recommended setup.

Provision AppDefense Org

VMWare will setup your organization and username within the AppDefense Cloud Manager. The organization Id (**orgId**) that is created in this step is required later for RSA NetWitness plugin configuration.

Configure AppDefense Appliance

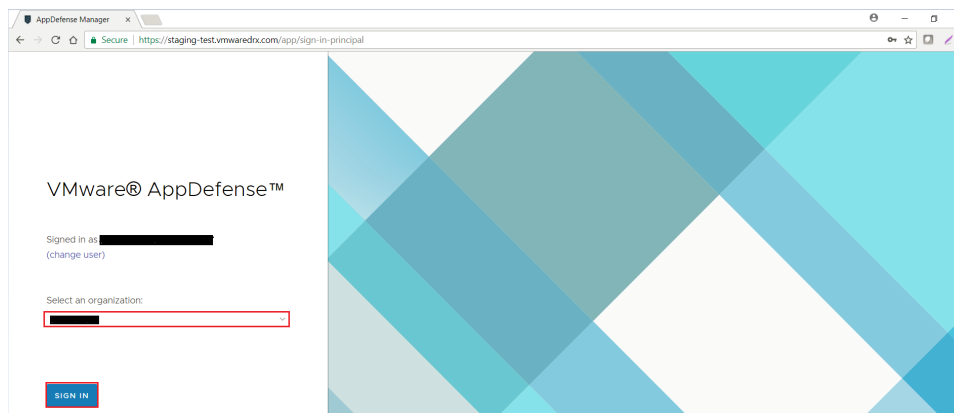
Refer the the *AppDefense Installation Guide* for details on how to download the AppDefense appliance ova file, deploy the OVF file, configure appliance with AppDefense Cloud manager, and Configure Host and Guest Module.

Setup API Key – Access Token

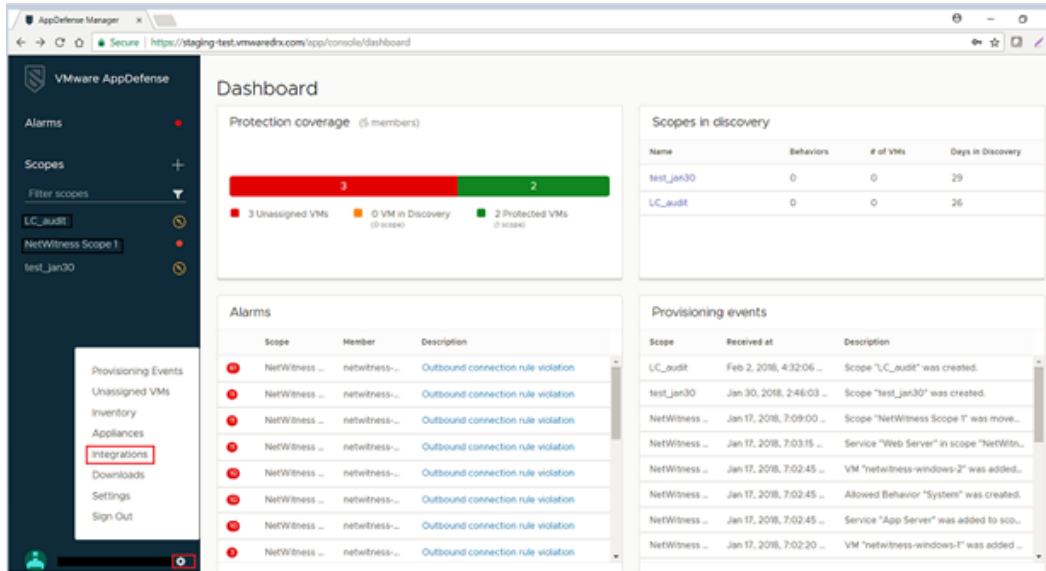
Note: For support resources from VMware, see <https://www.vmware.com/in/products/appdefense.html>.

To set up the API Key:

1. Log into your AppDefense account by visiting one of the following URLs:
 - Production Login URL: <https://appdefense.vmware.com>
 - Staging Login URL: <https://staging-test.vmwaredrx.com>
2. Select your organization and click on **SIGN-IN**.



3. Click on the settings cog at the bottom left of AppDefense console, and select **Integrations**.



4. Click on **Provision New API Key** at the upper right of the screen.
5. Fill in the **Integration Name**, and select **NetWitness** from the Integration Type drop down menu.

The 'New Integration' form shows the following fields:

- Integration Name:
- Integration Type:
- PROVISION button

6. Click **Provision**. The API key will be generated and displayed in the popup window.

The 'New Integration Created' popup window displays the following information:

- Endpoint URL:
- API Key:
- Warning: Once you close this notice the API key will no longer be recoverable. Be sure to save this information!
- OK button

7. Make sure to note and copy the value of the API Key, but *do not* copy the keyword "Bearer" along with the key. The API key is stored secretly and cannot be retrieved from AppDefense once the dialog is closed.
8. **Copy this key!** You will need the API key later, when you configure the Access Token value in RSA NetWitness.

Set Up the VMware AppDefense Event Source in NetWitness Platform

In RSA NetWitness Platform, perform the following tasks:

- I. Deploy the VMware AppDefense files from Live
- II. Configure the event source.

Deploy VMware Appware Defense Files from Live

VMware AppDefense 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 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 VMware AppDefense package. Browse Live for VMware AppDefense content, typing "VMware AppDefense" into the Keywords text box, then click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy it to the appropriate Log Collectors, using the Deployment Wizard.

Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.

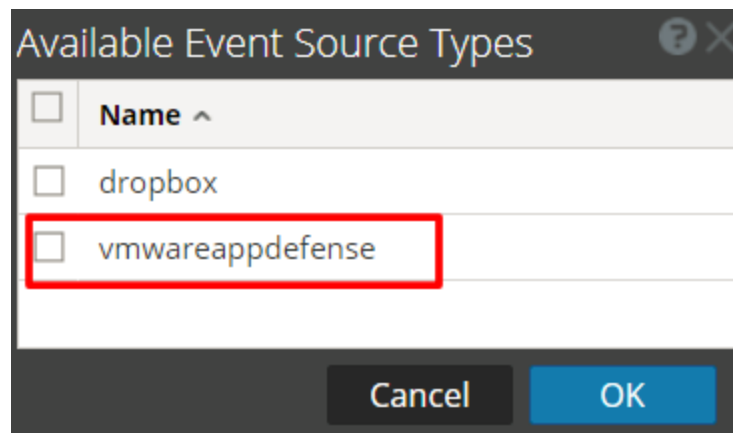
For more details, see the [Add or Update Supported Event Source Log Parsers](#) topic, or the [Live Services Management Guide](#).

Configure the Event Source

To configure the VMware AppDefense 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.

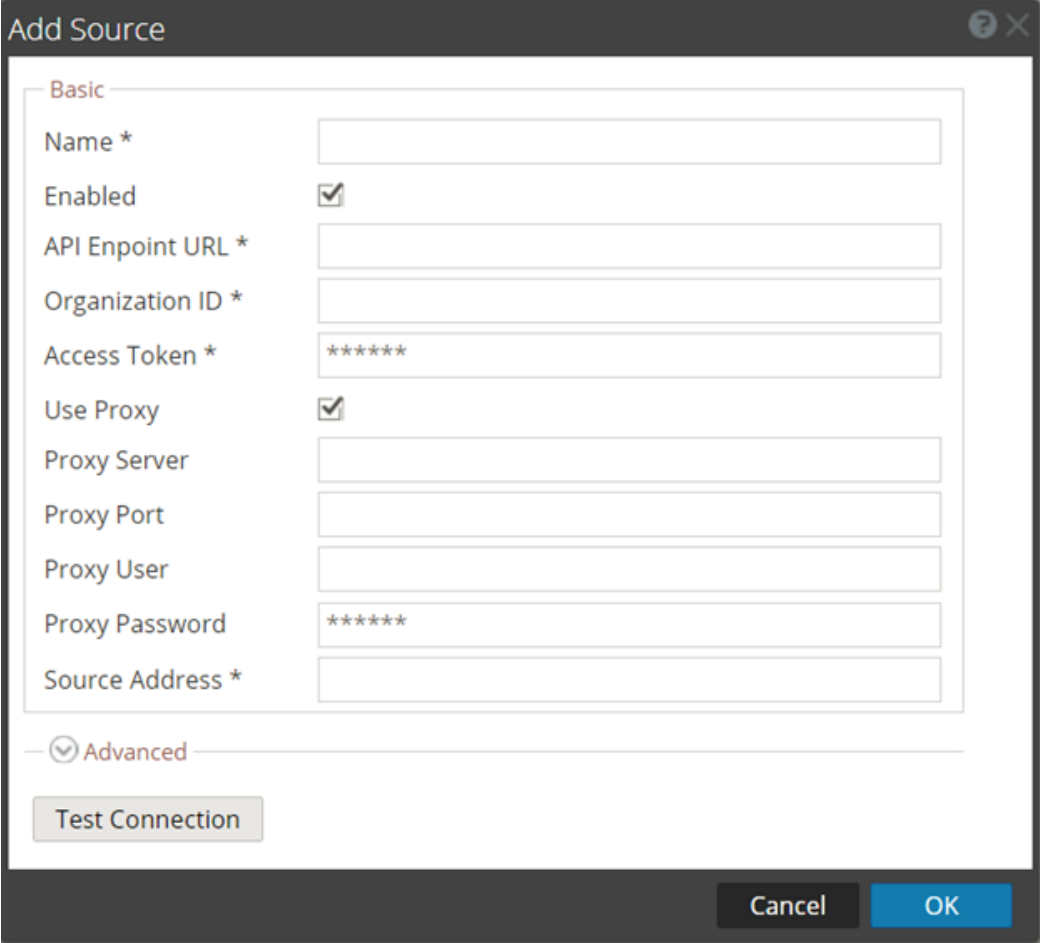


5. Select **vmwareappdefense** from the list, and click **OK**.

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 [VMware AppDefense 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.

VMware AppDefense Collection Configuration Parameters

The following tables describe the configuration parameters for the VMware AppDefense 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 *	Use one of the following URLs: <ul style="list-style-type: none"> Production Login URL: https://appdefense.vmware.com Staging Login URL: https://staging-test.vmware.com <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>Note: This staging API may be taken down temporarily or permanently without notice.</p> </div>
Organization ID *	Once you subscribe to AppDefense, an organization is provisioned for you, along with an organization ID (orgId).
Access Token *	An API key generated from VMware AppDefense management console. This is the key generated during the procedure describe in the Configure AppDefense Appliance section.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.

Advanced Parameters

Click  next to **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Polling Interval	<p>Interval (amount of time in seconds) between each poll. The default value is 180.</p> <p>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, the collector waits for that cycle to finish. 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.</p>
Max Duration Poll	<p>Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.</p>
Max Events Poll	<p>The maximum number of events per polling cycle (how many events collected per polling cycle).</p>
Max Idle Time Poll	<p>Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.</p>
Command Args	<p>Optional arguments to be added to the script invocation.</p>
Debug	<div data-bbox="464 1125 1385 1297" style="border: 1px solid yellow; 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> <div data-bbox="464 1318 1385 1409" style="border: 1px solid yellow; padding: 5px;"> <p>Caution: Enables or disables debug logging for the event source. Valid values are:</p> </div> <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>

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

Trademarks

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