

RSA NetWitness Platform

Event Source Log Configuration Guide



VMware Workspace ONE UEM

Last Modified: Tuesday, June 1, 2021

Event Source Product Information:

Vendor: [VMware](#)

Event Source: Workspace ONE UEM

Version: 1904 & above

RSA Product Information:

Supported On: NetWitness Platform 11.0 and later

Event Source Type: vmwareworkspaceone

Collection Method: Syslog

Event Source Class.Subclass: Configuration Management

Introduction

VMware Workspace ONE® is a workspace solution designed by VMware. It is a digital platform that delivers and manages any application on any device by integrating access control, application management, and multi-platform endpoint management.

The platform enables the IT team to deliver a digital workspace that includes the devices and applications of the choice of that particular business, without sacrificing the security and control that IT professionals need.

Workspace ONE UEM distinguishes two types of events:

- **Console events:** Console events are any administrative activity that takes place within the Workspace ONE UEM web console, or any system activity that takes place within servers in the VMware Workspace ONE Cloud. Example: Logging into the console, creation or deletion of admin accounts, and uploading or deleting applications in the console.
- **Device events:** Device events are any activities or interactions between the Workspace ONE Cloud and a managed device. Example: Commands sent to a device to install a configuration profile, a request to wipe data from a device, or a command to install a new managed application.

Note: RSA NetWitness Platform supports Console and Device events collected from Workspace ONE UEM.

Configure VMware Workspace ONE UEM

To configure Syslog collection for the VMware Workspace ONE UEM:

1. Configure syslog settings for VMware Workspace ONE UEM.
2. Configure NetWitness Platform for Syslog Collection.

Configure Syslog Settings for VMware Workspace ONE UEM

1. Log in to Console.
2. Navigate to **Monitor > Reports & Analytics > Events > Syslog**.
The **Syslog** window appears.
3. In the **General** tab, configure the following syslog settings:

Setting	Description	NetWitness Specific Value
Syslog Integration	Enable/Disable	Enable
Host Name	Host Name of Cloud Syslog	IP address or hostname of the RSA NetWitness Log Decoder or Remote Log Collector.
Protocol	UDP, TCP, and Secure TCP	UDP
Port	Port number	514
Syslog Facility	Provides information on the message origin, and help distinguish different classes of messages.	Optional, or as required.
Message Tag	Enter a descriptive tag to identify events from the AirWatch Console in the	AirWatch

	Message Tag field.	
Message Content	Enter the data to include in the transmission in the Message Content field.	As required, currently RSA NetWitness supports below Message Content format in vmwareworkspaceone parser. Event Type: {EventType} Event: {Event} Device: {DeviceFriendlyName} User: {User} Event Source: {EventSource} Event Module: {EventModule} Event Category: {EventCategory} Event Data: {EventData}

- In the **Advanced** tab, configure the following settings.

Setting	Description
Console Events	Select enable or disable to report console events.
Select Console Events to Send to Syslog	For each subheading, select the specific events that you want to trigger a message to syslog.
Device Events	Select enable or disable to report device events.
Select Device Events to Send to Syslog	For each subheading, select the specific events that you want to trigger a message to syslog.

- Select **Save** and use the **Test Connection** button to ensure successful communication between the AirWatch Console and the SIEM tool.

Note: Each syslog message from Workspace ONE UEM is prefaced with a timestamp and the tag AirWatch to easily distinguish it from other systems' messages collected by the syslog server or SIEM. RSA NetWitness supports message tag as AirWatch.

Configure Syslog Event Sources on NetWitness Platform

Perform the following steps in RSA NetWitness Platform-

- Enable the parser.
- Configure Syslog Collection.

Enable the Required Parser

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the Parser for Your Event Source is Enabled



1. In the NetWitness menu, go to **Administration > Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** menu, choose **View > Config**.
3. In the **Service Parsers Configuration** panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is `vmwareworkspaceone`.

Configure Syslog Collection

Note: Configure Syslog collection only for the first time when you set up an event source that uses Syslog to send its output to NetWitness. You must configure either the Log Decoder or the Remote Log Collector for Syslog.

To Configure the Log Decoder for Syslog Collection:

1. In the NetWitness menu, go to **Administration > Services**.
2. In the **Services** grid, select a Log Decoder, and from the **Actions** menu, choose **View > System**.
3. Depending on the icon you see, do one of the following:
 - If you see  **Start Capture**, click the icon to start capturing Syslog.
 - If you see  **Stop Capture**, this Log Decoder is already capturing Syslog.

To Configure the Remote Log Collector for Syslog Collection:

1. In the **NetWitness** menu, select **Administration > Services**.
2. In the **Services** grid, select a Remote Log Collector, and from the **Actions** menu, choose **View > Config > Event Sources**.
3. Select **Syslog / Config** from the drop-down menu. The **Event Categories** panel displays the Syslog 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 either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the **New Type** in the **Event Categories** panel, and click **+** in the **Sources** panel toolbar. The **Add Source** dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary. Click **OK** to confirm the changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. You can continue to add Syslog event sources to your system without any further configuration to NetWitness.

© 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.