VMware AirWatch Integration with Appthority

Integrate your application reputation service with AirWatch

Workspace ONE UEM v9.6

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to VMware Workspace ONE UEM Integration With Appthority

VMware Workspace ONE™ UEM integrates with Appthority so that you can send unmanaged applications from Workspace ONE UEM to your app scanning service. App reputation services scan network data, including applications, for vulnerabilities and threats to prevent and block malicious attacks to enterprise networks.

Integrate to consolidate systems in your mobile network, and secure unmanaged applications that are used on devices enrolled in Workspace ONE UEM .

Updated Integration

If you do not have the SKU for the updated integration with Appthority and you are interested in more information, contact your Professional Services Representative.

Communication Systems Between Appthority and VMware Workspace ONE UEM

Appthority integrates with Workspace ONE UEM using scheduled communications and REST APIs over HTTPS to transfer data. Communications include an extra layer of security with the use of the App Scanning Integration Service.

App Scanning Integration Service

This integration uses the app scanning integration service for security. Systems do not communicate with the enterprise's demilitarized zone (DMZ) unless the communication is secured with a signing certificate. You upload signing certificates from both Workspace ONE UEM and Appthority during the initial setup.

Directions of Communication

Communication, in the form of REST APIs, travels between components over HTTPS. Workspace ONE UEM uses port 443 for communication.

- The Workspace ONE UEM console and the compliance engine send the following to the App Scanning Integration Service.
  - The Workspace ONE UEM compliance engine identifies blacklisted applications.
  - The Workspace ONE UEM console sends applications reported by devices that included identified blacklisted applications.
- The App Scanning Integration Service posts applications reported by devices to the Appthority App Scanning Service.
- The Appthority App Scanning Service posts blacklisted applications back to the App Scanning Integration Service.

App Scan Integration Work Flow

The integration includes alternating actions between Workspace ONE UEM and Appthority. Actions happen in a sequence so that the system reports accurate results and Workspace ONE UEM can act against threats identified by the system.

Note: For help with the integration or with the migration of an existing integration, contact your Professional Services Representative.

Interactions between the systems occur in the listed order. This depiction does not include the app scanning integration service that acts as a secure communication layer between Workspace ONE UEM , Appthority, and the enterprise. Professional Services offers help to admins with these steps.

1. Set the prerequisites to enable the communication between Workspace ONE UEM and Appthority.
   - Admins configure an integration admin in the Workspace ONE UEM console.
   - Admins download the signing certificate from Appthority to upload to the Workspace ONE UEM console.
2. Configure Workspace ONE UEM to send applications to Appthority.
   a. Admins enable communication and upload the Appthority signing certificate.
   b. Admins download the Workspace ONE UEM signing certificate and upload it to Appthority.
   c. Sync either automatically with the Scheduler or manually in the Workspace ONE UEM console.
3. Appthority takes the listed actions and sends analysis results to Workspace ONE UEM .
   a. Appthority analyzes applications sent from Workspace ONE UEM .
   b. Appthority identifies suspicious Android and iOS applications and sends the analysis.
4. Act on blacklisted applications with compliance policies in Workspace ONE UEM .
   a. Workspace ONE UEM creates blacklisted app groups from Appthority's results. It creates an app group for Android and a separate group for iOS.
   b. Admins configure compliance policies that act on the applications in the app groups.

5. Manage the integration in Workspace ONE UEM with events, app groups, and refresh and reconfigure actions.
    - Admins view Console Events for integration activity.
    - Admins can deactivate blacklisted app groups.
    - Admins can refresh and reconfigure integration.

Supported Systems

App scan integration is available for the listed platforms, application types, and Workspace ONE UEM deployments.

Workspace ONE UEM integrates with the Appthority version available as of April 2017.

Supported Operating Systems and Application Types

App scan integration is available for the listed systems and application types.

- Android – Unmanaged applications
- Apple iOS – Unmanaged applications

Supported Deployments

App scan integration is available for SaaS and on-premises customers.

Considerations

Review these specific components that belong to the integration of Appthority and Workspace ONE UEM before you configure the system. Reviewing these components might prevent issues or help solve them.

Blacklisted Status

Once an application is blacklisted in the Workspace ONE UEM console using app scan integration, it remains blacklisted unless you act.

- Deactivate the blacklisted app group that includes the application.
- Reconfigure the integration.

Consider how restrictive your Appthority rules are before performing an app reputation scan and edit rules as necessary.

Customer Type Organization Group

You must configure app scan integration using a **Customer** type organization group. Integration does not work using any other type of organization group.

Appthority Rules

Before enabling integration, ensure that your Appthority rules are configured at the appropriate level to allow necessary applications and to block offending applications.

Android Application Control Profile and Blacklists

The blacklisted app groups created by this integration are not available to use in the Android application control profile.

Sync Times

The systems communicate instantly when you initiate a sync. Depending on the number of applications that need analyzing, sync processes can take some time. If possible, sync the system during off hours. You can, however, manually sync at any time.

Device Types and Privacy Settings in Workspace ONE UEM

The device type and privacy settings in Workspace ONE UEM can affect whether it sends applications to Appthority for analysis.

Challenge

You can configure privacy settings for personal, unmanaged applications to display and collect data, to collect but not display data, or not to collect data.

By default, Workspace ONE UEM displays and collects data for unmanaged applications on corporate devices (both dedicated and shared). However, it does not collect any data for unmanaged applications for employee owned and unassigned devices.

The compliance engine might act on an application on an employee owned device because the application was on a corporate device and Appthority blacklisted it.

Solution

You can deactivate the app group in Workspace ONE UEM that contains the application.

Custom Admin Role for App Scan Integration

To manage the integration, create a special admin user with restrictive roles. Special roles help to separate configurations and changes made for integration, so that they do not affect other areas of your Workspace ONE UEM deployment.

You want this custom admin role to access the **Third-Party Integration** page and to add or make edits to app groups. Give integration admins these abilities by adding a custom admin role with the listed categories, also known as permissions.

If you do not want to create an integration admin, ensure that the appointed admin user has the listed categories.

Configure an Integration Admin

Create an integration admin using these steps.

1. Ensure that you are in the desired organization group that is a **Customer** type.
2. Navigate to **Accounts > Administrators > Roles** and select **Add Role**.
3. Complete the following settings and add the following permissions.

Settings	Description
Name	Enter the **Name** of the role. For example, enter **<App Scan Vendor> Admin**.
Description	Enter a description of the custom admin role.
Categories	Select the following categories so the custom admin can manage the integration for any vendor. • Apps & Books > Application Groups > Application Group Update Active Status (Edit) • Apps & Books > Application Groups > Application Group Add Item (Edit) • Apps & Books > Application Groups > Application Group Edit Item (Edit) • Apps & Books > Application Groups > Application Group View (Read) • Settings > Apps > Catalog > Third-Party App Scanning (Edit) • Settings > Apps > Catalog > App Scan (Read)

Chapter 2:
Enable Integration and Trust

Add Appthority information to the Workspace ONE UEM console and download a certificate to enable secure communications between the two systems. You can use information to track the signing certificate and when the systems last synced.

Retrieve Signing Certificate from Appthority

Go to the Appthority site and download the Appthority certificate so that you can upload it to the Workspace ONE UEM console. When you enable Workspace ONE UEM to communicate with Appthority, you also download a certificate from Workspace ONE UEM to upload to Appthority.

Enable Communication in the Workspace ONE UEM Console

Enable communication between the systems with these steps.

1. Ensure that you are in the desired organization group that is a **Customer** type.
2. Navigate to **Groups & Settings > All Settings > Apps > App Scan > Third-Party Integration**.
3. Configure the settings.

Setting	Description
Enable Third Party App Scan Analysis	Select to enable communication between Workspace ONE UEM and the App Scan Vendor and to display available options on the page.
Choose App Scan Vendor	Select the applicable third-party vendor.

4. Complete the options for Appthority.

Setting	Description
Upload	To retrieve the certificate downloaded from Appthority, select **Upload The Certificate From Appthority**. This certificate and the one you download from Workspace ONE UEM enable secure communication between the Workspace ONE UEM environment and your Appthority environment through the app scanning integration service.
Download Certificate	Download the Workspace ONE UEM certificate to upload to your Appthority environment.
Appthority REST API URL	Enter the URL for your Appthority environment to direct Workspace ONE UEM to the service through the app scanning service.

5. Display and configure the **Application Group Creation** area.

Setting	Description
Enable Email Notification	Displays the **Application Group Creation** area to configure the system to send notifications to admins when analysis creates new app groups in Workspace ONE UEM.
Send Email To	Enter email addresses to receive notifications about new app groups created by analysis. Use a comma to separate addresses.
Message Template	Use **Message Preview** to see the email that the system sends upon the creation of new app groups using the **Vendor Application Group Creation Notification** template.

6. Select **Save** to complete configurations and sync with the vendor when the Workspace ONE UEM scheduler task runs.

For information on the **Sync Now** and **Refresh** options, see Sync Options for Appthority Integrations on page 9. For information on **Reconfigure**, see Results of Reconfiguring Integration on page 13.

Sync Options for Appthority Integrations

You can manually sync the app scan integration system and Workspace ONE UEM at any time, or let the Workspace ONE UEM scheduler task sync integration.

The scheduler task runs every 168 hours. On-premises deployments can edit the recurrence, while SaaS environments cannot. However, you can initiate a manual sync in both environments.

Sync Manually

SaaS and on-premises environments can use the following steps to sync Appthority, the app scanning integration service, and Workspace ONE UEM .

1. Ensure that you are in the correct organization group.
2. Navigate to **Groups & Settings > All Settings > Apps > App Scan > Third Party Integration**.
3. Select Appthority in the **Choose App Scan Vendor** menu.

4. Select one of the options.
    - **Sync Now** - Sends applications to the app scanning system through the app scanning integration service. Workspace ONE UEM sends only those applications that have not been scanned before or that have no previous result recorded.
    - **Refresh** - Wipes application data from Workspace ONE UEM and the app scanning integration service and requests that Appthority wipe application data, too. Then Workspace ONE UEM resends applications for new analysis.

Edit the Scheduler Task

On-premises environments can use the following steps to change the frequency of the **Send Apps to App Scan Vendor** task.

You must have system admin credentials to perform this action.

1. Ensure that you are in the correct organization group.
2. Navigate to **Groups & Settings > All Settings > Admin > Scheduler**.
3. Locate the **Send Apps to App Scan Vendor** task and select **Edit** from the actions menu.
4. Edit the options for **Recurrence Type** and **Range** and then **Save** your edits.

Access Results With App Groups

Use Workspace ONE UEM to identify those applications that failed an app scan. Workspace ONE UEM lists them in blacklisted app groups. The system prevents access to applications in blacklisted app groups for security. Deactivate a group if you know the applications are secure for use.

Representing Appthority Rules

Workspace ONE UEM creates blacklisted app groups by platform. If you have six Appthority rules that identify issues, Workspace ONE UEM displays six blacklisted app groups for Android and six blacklisted app groups for Apple iOS. It displays a total of 12. It is not possible to edit the app group information because Workspace ONE UEM imports the data.

Access Blacklisted App Groups

You can identify your results by the **Created By** column on the **App Groups** page. The column labels blacklisted app groups created by app scan integration as **Appthority**. View your Appthority scan results using the listed procedure.

1. Ensure that you are in the correct organization group.
2. Navigate to **Apps & Books > Applications > Application Settings > App Groups**.
3. Use the **Created By** filter to sort the list by **Appthority**.
4. Select the **Name** and view the applications included in the app group list. This list includes the blacklisted application, its application ID, and the version.

5. Select **Edit** from the actions menu and add notes to the **Description** text box on the **Assignment** tab.
6. Select **Finish** if you added a description.

Deactivate Blacklisted App Groups

If the system blacklisted an application that you need, deactivate Appthority blacklisted app groups in Workspace ONE UEM . Deactivation is the only way to revert the blacklisted status without reconfiguring integration.

1. Ensure that you are in the correct organization group.
2. Navigate to **Apps & Books > Applications > Application Settings > App Groups**.
3. Locate the blacklisted app group with the needed application.
4. Select the drop-down icon from the actions menu and select **Deactivate**.

Results of Deactivation

Deactivation results in the listed Workspace ONE UEM behaviors.

- Workspace ONE UEM does not display them in the list when you build your compliance policy.
- Workspace ONE UEM removes the deactivated group from all compliance policies.

Chapter 3:
Build an Application Compliance Policy

You can create compliance policies that detect when users have blacklisted applications and configure these policies to resolve non-compliance.

Example of Compliance Policy Actions

The compliance engine detects a user with an application blacklisted by an app scan integration vendor. You can configure the compliance engine to take several measures.

- Send a push notification to the user prompting them to remove the application.
- Remove certain features such as Wi-Fi, VPN, or email profiles from the device.
- Send an email notification to the user copying IT, Security, and HR.

Configure Compliance for App Scan

Build an application compliance policy that acts on devices with non-compliant applications:

1. Ensure that you are in the correct organization group.
2. Navigate to **Devices > Compliance Policies > List View**. Select **Add**.
3. Select the platform.
4. Select **Application List** on the **Rules** tab and select **Contains Vendor Blacklisted App(s)** for integration.

   To configure the compliance engine to monitor for applications from your reputation scanning system, add the blacklisted app group to the list.

   If the engine detects blacklisted applications on devices assigned to the compliance rule, the engine acts as configured in the rule.
5. Move to the **Actions** tab to set escalating actions to perform on a user who does not comply with the compliance rule.

Setting	Description
Mark as Not Compliant	Enable the check box to tag devices that violate this rule, but once the device is tagged non-compliant and depending on escalation actions, the system might block the device from accessing resources and might block admins from acting on the device. Disable this option when you do not want to quarantine the device immediately.
Application	Select to remove the managed application.
Command	Select to configure the system to command the device to check in to the console, to perform an enterprise wipe, or to change roaming settings.
Email	Select to block email on the non-compliant device.
Notify	Select to notify the non-compliant device with an email, SMS, or push notification using your default template. You can also send a note to the admin concerning the rule violation.
Profile	Select to use Workspace ONE UEM profiles to restrict functionality on the device.

6. Move to the **Assignment** tab to assign the compliance rule to smart groups.

Setting	Description
Managed By	View or edit the organization group that manages and enforces the rule.
Assigned Groups	Type to add smart groups to which the rule applies.
Exclusions	Select Yes to exclude groups from the rule.
View Device Assignment	Select to view the devices affected by the rule.

7. Move to the **Summary** tab to name the rule and give it a brief description.
8. Select **Finish and Activate** to enforce the newly created rule.

Results of Reconfiguring Integration

Workspace ONE UEM offers the option to reconfigure the integration with Appthority. Reconfiguring the system removes configurations, app groups, and compliance policies.

Reconfiguring Appthority integration results in numerous actions.

- Disables the Third-Party App Scan Analysis feature.
- Removes the Appthority signing certificates from the Workspace ONE UEM console.
- Removes the Appthority URL information from the Workspace ONE UEM console.
- Removes the blacklisted app groups from the Workspace ONE UEM console created from the integration.
- Removes compliance policies created using the blacklisted app groups.
- Wipes all data from the app scanning integration service.
- Requests Appthority to remove certificates and data from the integration.

Reconfigure Alternative

Another way to fix application issues is to deactivate blacklisted app groups. This option might fix issues without removing configurations.

Reconfigure the System

Reconfigure your integration only if you approve of the actions the system takes. The system removes all data and certificates and you must reconfigure all settings.

1. Ensure that you are in the correct organization group.
2. Navigate to **Groups & Settings > All Settings > Apps > App Scan > Third-Party Integration**.
3. Select **Reconfigure**.

Monitor Integration With Console Events

Workspace ONE UEM lists events so that you can troubleshoot issues or find general information about systems configured in the console. Review console events to get information on app scans, blacklisted app groups, and errors with the integration process.

Console events specific to the **App Scan Integration** report about various components of the system.

- Scanning modifies applicable blacklisted app groups.
- The vendor adds applications to blacklisted app groups.
- Vendors begin scanning applications.
- The system identifies an error in the process.
- The scanning system resets or is reconfigured.

Access Console Events

Access console events using the following steps.

1. Navigate to **Hub > Reports & Analytics > Events > Console Events**.
2. Select a **Date Range** from the menu.
3. Select **Applications** from the **Category** menu.
4. Find the applicable **Events**.
    - App Scan Vendor Application Group Modified
    - Application Added To App Scan Vendor Application Group
    - Third Party Application Scanning Started

- Error occurred while Third Party Application Scanning
- Reset Perform for Third Party Application Scanning Vendor

Manage Certificates

Certificates enable a secure communication between Workspace ONE UEM and Appthority through the app scanning integration service, so retrieve certificates from both Appthority and Workspace ONE UEM .

Keep these certificates current on the **Groups & Settings > All Settings > Apps > App Scan > Third-Party Integration** page.

Available Options for Management

Setting	Description
Upload	Retrieves the Appthority certificate with **Upload The Certificate From Appthority**.
Change	Updates the Appthority by selecting this option. The system displays this option after you upload the initial certificate.
Clear	Removes a certificate. The system displays this option after you upload the initial certificate.
Download Certificate	Download the Workspace ONE UEM certificate to upload to Appthority.