# VMware AirWatch Integration with Palo Alto Networks WildFire

Integrate your application reputation service with AirWatch

**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 Palo Alto Networks WildFire

VMware Workspace ONE™ UEM integrates with Palo Alto Networks WildFire 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.

Benefits of integration include consolidating systems in your mobile network and adding a layer of security to unmanaged applications that are used on devices enrolled in Workspace ONE UEM .

## Communication Systems Between Palo Alto Network WildFire and VMware Workspace ONE UEM

Palo Alto Networks WildFire is a firewall that analyzes network traffic, including applications, using the SHA-256 hash calculator. If you use Palo Alto Networks WildFire as a firewall, it integrates with Workspace ONE UEM using scheduled communications with the SHA-256 hash calculator to transfer data.

The integration includes these schedulers and communication interactions.

- Workspace ONE UEM sends application hashes on schedule using the AirWatch Agent for Android on devices and the Workspace ONE UEM Integration Service.
- WildFire responds with three verdicts: malware, grayware, and benign.
- Workspace ONE UEM creates two blacklisted app groups using malware and grayware verdicts. It records benign verdicts and does not resend hashes for benign applications.
- Workspace ONE UEM calls to WildFire are synchronous and responses are immediate.
- Integration uses port 443 for communication.

**Note:** Integrating with other products offers convenience and flexibility to help manage mobile deployments. However, functionality is not guaranteed and it depends upon the proper functioning of third-party solutions.

## App Scan Integration Work Flow

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

Interactions between the systems occur in the listed order.

| | |
|---|---|
| **Workspace ONE UEM Pre-requisites** | Configure an integration admin. |
| **1. Workspace ONE UEM Actions** | 1. Enable communication.<br>2. Sync either automatically with the scheduler or manually.<br>**Result** – Workspace ONE UEM sends applications to WildFire. |
| **2. WildFire Actions** | 1. Analyze application hashes.<br>2. Identify offending Android applications.<br>**Result** – WildFire sends results to Workspace ONE UEM . |
| **3. Workspace ONE UEM Actions** | 1. Creates blacklisted app groups for grayware and malware applications.<br>2. Configure compliance policies to act on devices with malicious applications.<br>**Result** – Workspace ONE UEM acts as per compliance policies on offending devices. |
| **Workspace ONE UEM Troubleshooting Options** | • View console events for integration activity.<br>• Deactivate blacklisted app groups.<br>• Reset integration. |

## Supported Systems

App Scan Integration is available for the listed platforms, application types, and Workspace ONE UEM deployments. Before configuring App Scan Integration, review the supported lists.

Workspace ONE UEM integrates with the Palo Alto Networks WildFire version available as of August 2015.

### Supported Operating Systems, Application Types, and AirWatch Agents

App Scan Integration is available for only **Android unmanaged applications**.

App Scan Integration works using the **AirWatch Agent for Android v5.3+**. Older agent versions do not support integration.

### Supported Deployments

App Scan Integration is available for SaaS and on-premises customers.

## Considerations

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

### Blacklisted Apps Remain Blacklisted

Once an application is blacklisted in the Workspace ONE UEM console using App Scan Integration it remains blacklisted unless unless you take action.

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

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

### Application Hashes, Application Versions, and Application Package Names

Although WildFire works with application hashes, Workspace ONE UEM app groups use the application package ID. The use of different components for analysis and management introduces the possibility to have an application version blacklisted in Workspace ONE UEM while WildFire considers a newer version benign. The new version remains blacklisted in Workspace ONE UEM due to its unchanged application package ID.

### 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.

### 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.

# Chapter 2: 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.<br>For example, enter **<App Scan Vendor> Admin**. |
| **Description** | Enter a description of the custom admin role. |

| Settings | Description |
|---|---|
| **Categories** | Select the following categories so the custom admin can manage the integration for any vendor.<br>• Apps & Books > Application Groups > Application Group Update Active Status (Edit)<br>• Apps & Books > Application Groups > Application Group Add Item (Edit)<br>• Apps & Books > Application Groups > Application Group Edit Item (Edit)<br>• Apps & Books > Application Groups > Application Group View (Read)<br>• Settings > Apps > Catalog > Third-Party App Scanning (Edit)<br>• Settings > Apps > Catalog > App Scan (Read) |

# Chapter 3:
# Enable Integration

Add your Palo Alto Networks WildFire information to the Workspace ONE UEM console so that the two systems can share applications and scan results.

Enable communication 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 WildFire.

| Setting | Description |
|---|---|
| **WildFire API Key** | Enter the key for your WildFire system so Workspace ONE UEM can send application hashes directly to WildFire. |

5. Use the **Test Connection** option to check that Workspace ONE UEM and your service can communicate successfully.

6. Select one of the save options.

| Setting | Description |
|---|---|
| **Save** | Saves configurations and syncs with the App Scan Vendor when the Workspace ONE UEM scheduler task runs. |
| **Sync Now** | Saves configurations and begins a manual sync with the App Scan Vendor without waiting for the scheduler task to run. |

## Using the UI to Troubleshoot

Use the sync messages on the Third Party Integration page for quick answers to these questions.

- When was the last sync between the systems, either successful or unsuccessful?
- When is the next scheduled sync?
- Is a sync currently in progress?

## Sync Options

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 the two systems.

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

### Sync Manually

SaaS and on-premises environments can use the following steps to sync an App Scan Integration system 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 the appropriate system in the **Choose App Scan Vendor** menu.
4. Select **Sync Now** to send applications to the app scanning system. Workspace ONE UEM sends only those applications that have not been scanned before or that have no previous result recorded.

### 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. You can deactivate a group if you know the applications are secure for use.

The system creates app groups by platform. The number of app groups the system creates depends on the vendor and the supported platforms.

## 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 **Palo Alto Networks WildFire**. View your WildFire scan results.

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 **Palo Alto Networks WildFire**.
4. Select the **Name** to view the applications included in the App Group list. This list includes the blacklisted application and its application ID.
5. Select **Edit** from the actions menu to add notes to the **Description** text box on the **Assignment** tab.
6. Select **Finish**.

## Deactivate Blacklisted App Groups

If the systems blacklisted an application that you need, deactivate WildFire Blacklisted App Groups. This action is the only way to revert the blacklisted status without resetting 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

When you deactivate these blacklisted app groups, Workspace ONE UEM takes these actions.

- 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 4:
# 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 perform various actions.

- 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 to perform an action on devices with non-compliant applications.

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

   Add applications from your application reputation scanning system to configure the compliance engine to monitor for their presence on devices.

   If the engine detects applications listed in these unique blacklisted app groups on devices assigned to the compliance rule, the engine performs the actions configured in the rule.
5. Move to the **Actions** tab to set escalating actions for the engine to perform.

| 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.<br>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.<br>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 Resetting Integration

Workspace ONE UEM offers the option to reset the App Scan Integration system. Resetting the system removes configurations, app groups, and compliance policies. Another way to fix application issues is to deactivate blacklisted app groups. This option might fix issues without removing configurations.

To reset the feature results in numerous actions.

- Disables the Third Party App Scan Analysis.
- Removes the App Scan Integration account information from the Workspace ONE UEM console.
- Removes the blacklisted app groups from the UEM console created from third-party vendor scans.
- Removes compliance policies created using the blacklisted app groups.

### Reset Alternative

An alternative to resetting the system is deactivating blacklisted app groups that contain needed applications.

## Reset the System

You might have need to re-configure the integration between Workspace ONE UEM and the App Scan Integration system. If you approve of the results to resetting the integration, use this procedure to remove integration configurations.

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 the application option from the **Choose App Scan Vendor** menu.
4. Select **Reset**.

## 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