VMware AirWatch Integration with FireEye Mobile Security (Mobile Threat Prevention)

Integrate your application reputation service with AirWatch

Multiple AirWatch versions

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

Revision Table

The following table displays revisions to this guide since the release of Multiple AirWatch versions.

Date	Reason
April 2017	Initial upload.

Table of Contents

Chapter 1:
Overview

Introduction to VMware Workspace ONE UEM Integration With FireEye Mobile Security (Mobile Threat Prevention)

VMware Workspace ONE UEM integrates with FireEye Mobile Security 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 FireEye MTP and VMware Workspace ONE UEM

FireEye Mobile Security (Mobile Threat Prevention, MTP) detects and prevents threats that use mobile devices to attack enterprises. The integration between FireEye MTP and Workspace ONE UEM uses REST APIs over HTTPS to transfer data.

The integration includes these communication interactions.

- Workspace ONE UEM makes APIs available for FireEye MTP to call Workspace ONE UEM endpoints and this availability is why you enable the REST API.

- FireEye MTP APIs use HTTPS, which uses Secure Socket Layer (SSL) to provide communications security.

- FireEye MTP calls to Workspace ONE UEM APIs are synchronous and responses are immediate.

> **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 FireEye MTP. 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. • Enable REST APIs. • To receive scan results, create two app groups, one Android and the other Apple iOS, with the same name .
1. FireEye MTP Actions	1. Enable communication. See FireEye MTP documentation for details on configuring integration in the FireEye MTP Management Portal. **Result** – Workspace ONE UEM sends applications to FireEye MTP.

vmware airwatch

2. FireEye MTP Actions	1. Analyze applications.
	2. Identify offending Android and Apple iOS applications.
	Result – FireEyE MTP sends results to Workspace ONE UEM .
3. Workspace ONE UEM Actions	1. Displays blacklisted applications in the pre-configured app groups.
	2. Configure compliance policies to act on devices with malicious applications.
	Result – Workspace ONE UEM acts as per compliance policies on offending devices.

Supported Components

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 FireEye Mobile Security (Mobile Threat Prevention, MTP) version available as of August 2015.

Supported Operating Systems and Application Types

App Scan Integration is available for the following 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 FireEye MTP and Workspace ONE UEM before you configure the system. Reviewing these components might prevent issues or help solve them.

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.

FireEye MTP Policies

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

Chapter 2:
Pre-Requisite Steps

Custom Admin Role for App Scan Integration

Create a special admin user with restrictive roles to manage the integration so that configurations and changes made for integration 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)

Enable REST API

The App Scan Integration uses REST APIs, and APIs require authentication to integrate with Workspace ONE UEM . Enable the Workspace ONE UEM console to allow REST API authentication using **Basic Authentication**.

Any Workspace ONE UEM architecture can use basic authentication, but it does not integrate with existing corporate users accounts.

Enable API access in the Workspace ONE UEM console using these steps.

1. Ensure that you are in the desired organization group that is a **Customer** type.

2. Navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API**.

3. Select the tab and configure the following setting on the corresponding tab:

Tab	Setting
General	Select **Enable API Access**. This selection automatically generates the API Key for the organization group. Enter this key to the FireEye MTP Management Portal. Do not use an existing API key. Create a unique key for this integration.
Authentication	Select **Basic** as the API authentication method.

4. **Save** your settings.

Create Placeholder App Groups

Create app groups so that Workspace ONE UEM can display FireEye MTP scan results. Make an app group for Android and another for Apple iOS but name the two app groups the same. Enter this single name in the FireEye MTP Management Portal for integration.

Upon scan completion, the system allocates results into the proper app group depending on the platform.

You need at least one application in each group to create the placeholder. However, you can use a made-up application and application ID to create the placeholder app groups.

1. Ensure that you are in the correct organization group.

2. Navigate to **Apps & Books > Applications > Application Settings > App Groups**.

3. Select **Add Group**.

4. Configure the following settings on the **List** tab.

Setting	Description
Type	Select **Blacklist** from the menu.
Platform	Select **Apple** or **Android** from the menu.
Name	Enter a descriptive name for the placeholder group. Use the same name for both the Apple iOS and Android app groups.

5. Select **Add Application** and enter a made-up application name and application ID.

Setting	Description
Application Name	Enter any name because this setting is a placeholder. For example, enter **TestApp**.
Application ID	Enter any string of characters because this setting is a placeholder. For example, enter **test.app.com**.

6. Select **Next** to move to the **Assignment** tab which includes options that you can configure. The configurations are optional and not needed for the placeholder app group to work.

7. Select **Finish** to complete the creation of the placeholder app group.

Chapter 3:
Access Results

Access Results With App Groups

Use Workspace ONE UEM to identify those applications that failed an app scan. Workspace ONE UEM displays them in blacklisted app groups that you created using a placeholder group. 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.

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 **FireEye**. View your FireEye MTP 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 **FireEye**.

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 system blacklisted an application that you need, deactivate FireEye MTP blacklisted app groups.

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:
Manage Results

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 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 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**. 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 Blacklist App(s)** for integration.

   If the engine detects applications listed in 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 the engine performs.

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.