

Workspace ONE Mobile Flows Admin Guide

Configure Mobile Flows

Workspace ONE UEM v9.7

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

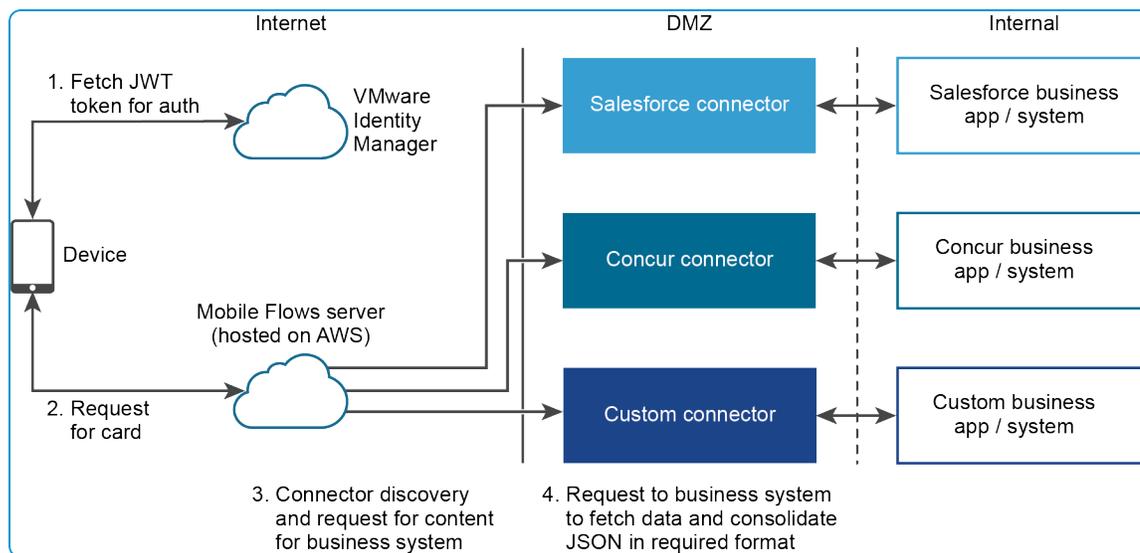
Table of Contents

Chapter 1: Overview	3
Mobile Flows Architecture	3
Requirements	3
Mobile Flows Connectors	4
Chapter 2: Configure Mobile Flows	6
Configure VMware Identity Manager	6
Configure Connectors from Workspace ONE UEM console	7
Create Connectors	8
Chapter 3: Configure Client Applications	9
Configure Mobile Flows with VMware Boxer	9
Chapter 4: Frequently Asked Questions	11

Chapter 1: Overview

Mobile Flows Architecture

The following image provides information about the architecture design and functionality of Mobile Flows.



Requirements

Following are the requirements for configuring Mobile Flows with VMware Boxer:

- AirWatch console v9.3 or later
- VMware Boxer v4.12 or later
- VMware Identity Manager v3.1 or later
- Workspace ONE Enterprise bundle or Workspace ONE Mobile Flows add-on

Hardware Requirements

Number of Devices	Up to 40,000	40,000 - 80,000	80,000 - 120,000	120,000 - 160,000
Number of Servers	2	3	4	5
CPU Cores	4 CPU cores	4 CPU cores each	4 CPU cores each	4 CPU cores each
RAM (GB)	8	8	8	8
Hard Disk Space (GB)	10 GB for Linux Distribution 400 MB for installer 10 GB for log files			

Network Requirements

Source	Destination	Port
Mobile Flows server (https://prod.hero.vmwservices.com)	Mobile Flows Connector	443 (inbound)
Mobile Flows Connector	Backend Business Systems	443
AirWatch Console	Mobile Flows server (https://prod.hero.vmwservices.com)	443

Mobile Flows Connectors

Connectors are services or components that run on the Mobile Flows server. Connectors can be configured to fetch user-specific information that enables Mobile Flows to work on the configured user devices. The connectors fetch user-specific information from the business systems that are behind an organization's internal firewall and send a response back to the user's mobile application. The connectors are specific to each business system. For example, you have to configure and deploy a Salesforce connector to fetch information from a Salesforce business system and respond to Mobile Flows request. For more information on the available connectors and information on configuring the connectors, see [Configure Connectors from Workspace ONE UEM console on page 7](#).

Provision Mobile Flows

- If you are a shared SaaS Workspace ONE UEM user, GEM service enables the Mobile Flows Admin UI in the Workspace ONE UEM console when you purchase the Mobile Flows solution or Workspace ONE Enterprise SKU.
- If you are a dedicated SaaS Workspace ONE UEM user, you can place an order and VMware Deployments or the SaaS Operations team enables the Admin UI on the Workspace ONE UEM console by executing a SQL script in your database.
- If you are an on-premises Workspace ONE UEM user, you can download the SQL script to run on the Workspace ONE UEM Database to enable the Mobile Flows Admin UI. You need the locationgroupID where Mobile Flows admin UI is to be enabled and the flag value to run the SQL script. To download the script and for more information, see [AirWatch Resources](#).

For additional assistance when configuring Mobile Flows, contact MobileFlows@vmware.com.

Chapter 2:

Configure Mobile Flows

Configure VMware Identity Manager

VMware Identity Manager can be used to authenticate the information transfer when using connectors for client applications. If your environment consists of VMware Identity Manager, you can create a VMware Identity Manager template to fetch user specific JWT token for connector authentication. For more information about installing and configuration VMware Identity Manager in your environment, see [Installing and Configuring VMware Identity Manager](#).

Configure Mobile Flows Server Provision

You must install and configure VMware Identity Manager for an uninterrupted Mobile Flows user-experience. When you install and configure VMware Identity Manager for Mobile Flows, VMware Identity Manager creates a tenant in the Mobile Flows server. The tenant is created using API and requires no manual configuration. In case if the tenant is not created using API, you can manually configure a VMware Identity Manager tenant in the Mobile Flows server. For more information about creating VMware Identity Manager tenant, see [Create Your Identity Provider](#) section of the *VMware Identity Manager Connector Installation and Configuration guide*.

Configure VMware Identity Manager Template

1. Log in to the VMware Identity Manager Console and navigate to **Catalog > Settings > Remote App Access > Templates**.
2. Select **Create Template**.
3. Select **Template ID** text box and enter a template name. For example, HeroCard_Template1.
4. Select **Application** text box and enter **Identity Manager**.
5. Select **Scope** text box and enter **ENABLE email, profile, user, openid**.
6. Select **Redirect URL** text box and enter **com.airwatch.herocard://success** as the registered redirect URL.
7. Select **Token Type** and select **Bearer**. This attribute tells the application what type of access token it was given. For VMware Identity Manager, the tokens are bearer tokens.
8. Select **Token Length** and leave the default setting, 32 Bytes.
9. Select **Issue Refresh Token** and select **Enabled** to use refresh tokens.
10. Select **Access Token TTL** and enter **30 days** as the access token time to live length. When the access token expires, the application uses the refresh token to request a new access token.
11. Select **Refresh Token TTL** and enter **365 days** as the refresh token time to live.
12. Select **Add**.

Configure Connectors from Workspace ONE UEM console

The following connectors are provided out of the box that can be configured and deployed to support specific business systems.

Sample Business System Connector Name	Use Case Addressed
Salesforce	Add a contact to an existing account. Show the user existing contact details.
ServiceNow	Approve or reject ServiceNow requests.
JIRA	Comment on an issue, watch an issue, or open an issue in a browser.
Bitbucket Server	Comment on, approve, decline, and merge Bitbucket Server pull requests.
Github	Comment on, approve, reject, request changes, and merge Github pull requests.
Gitlab	Comment on, approve, reject, and merge Gitlab pull requests.
AWS	Approve AWS certificate requests.
AirWatch	Inviting a user to install apps that are missing from the user's device.
Concur	Approve an expense report, reject an expense report, and open an expense report in a browser.

Configure Connectors

Configure the connector details and map them from within the Workspace ONE UEM console for the mobile applications to fetch the required details. Once the mobile application fetches the connector details, the device users are provided with an option to enable or disable the Mobile Flows connectors from within the application.

1. Log in to the UEM Console and navigate to > **Content** > **Mobile Flows**. If Mobile Flows option is not available in the Content page, check with your Account Manager to purchase Workspace ONE Mobile Flows add-on.
2. Select **New** to create a new connector configuration or **Edit** to edit an existing connector configuration. Edit Connector page opens.
3. Select the **Name** text box and enter the name of the connector that you want to be displayed on the Console and the user's device.
4. Select the **Discovery URL** text box and enter the public facing URL for the connector that is deployed within your environment.
5. Select the **Authentication Type** drop-down menu and select the required authentication type. Following are the available authentication types:
 - a. **Basic** - User must enter their username and password credentials when enabling connector on their client application.
 - b. **OAuth 2.0** - The details provided on the console is sent to the client application and the Mobile Flows client

framework adds the information to the request header. You must provide additional key values when selecting **OAuth 2.0** as the authentication type.

- c. **Workspace ONE** - The client application on the device uses the Workspace ONE's SSO token for authentication with backend systems.

6. Select **Save**.

Create Connectors

The Mobile Flows Connectors provided by VMware AirWatch can be customized as per your requirement. You can also create custom connectors to meet a specific use case by using the information provided in this section.

VMware AirWatch Connector Framework

The following approaches can be taken for creating a connector:

- Use the out-of-the-box connectors developed by VMware AirWatch to meet specific use cases.
- Build on the open source out-of-the-box connectors to meet your requirement or address a specific use case.
- Create custom connectors. The connector framework developed by VMware AirWatch can be utilized to build Mobile Flow Connectors to meet any use cases, and to support any backend business systems that utilizes RESTful APIs.

For more information on building and installing custom connectors see, <https://github.com/vmware/connectors-workspace-one>.

Chapter 3:

Configure Client Applications

Configure Mobile Flows with VMware Boxer

VMware Boxer is the email client provided to you by VMware. Apart from numerous email management features, you can configure and deploy custom application configurations to the Boxer app from the Workspace ONE UEM console. Mobile Flows can be configured with Boxer using the application configuration keys provided by VMware AirWatch.

1. Log in to the Workspace ONE UEM console.
2. Navigate to **Apps & Books > Public**.
3. Select the **VMware Boxer** application in the **List View**, select **Assign**, and select **Add Assignment**.
4. Navigate to the **Optional** Application Configuration section of the Add Assignment page and add the following configuration keys for enabling and configuring the Mobile Flows.

Configuration Key	Value Type	Configuration Value	Description
AppMobileFlowsEnabled	Boolean	True - enabled False - disabled	Set to True to enable Mobile Flows for Boxer.
AppMobileFlowsHost	String	Provide https://prod.hero.vmwservices.com as the URL for the Mobile Flows host.	Define the URL for the Mobile Flows host.
AppMobileFlowsvIDM	String	Provide a valid URL for authenticating the device users through VMware Identity Manager. For example, http://acme.vIDM.acme2.com	Defines the URL for the device user to authenticate using the VMware Identity Manager instance.
AppMobileFlowsSyncTimeHours	Integer	Provide a sync value in hours. For example, 24.	Mobile flow cards are not requested for emails sent before the entered value.

Configuration Key	Value Type	Configuration Value	Description
AppMobileFlowsAutoEnableConnectors	Boolean	False - Disabled (default) True - Enabled	If enabled, when turning on Mobile Flows, all connectors are activated in succession. Enable this option only when all connectors are configured with VMware Identity Manager.

5. Select **Add** and then select **Save**.

Chapter 4:

Frequently Asked Questions

What are the components of Workspace ONE Mobile Flows?

- Cloud-hosted mobile flows service
- VMware Identity Manager or other identity provider
- Connectors
- Workspace ONE
- VMware Boxer

Which mobile platforms are supported?

- Android and iOS.

What are the minimum requirements?

- Though the authentication can be configured using any identity provider, to ensure an uninterrupted user-experience you must use VMware Identity Manager to deploy Mobile Flows. Any backend services intended to be used by the Mobile Flows service must also be configured with VMware Identity Manager. The best user-experience is delivered when configured using OAuth2 flows.

Can Mobile Flows be deployed on-premise?

- Mobile Flows is a cloud-only service available to both SaaS and on-premise Workspace ONE customers.

How is Mobile Flows configured?

Customers can leverage Mobile Flows in three ways:

- Pre-configured connectors.
- Configure out-of-the-box connectors to meet a specific requirements.
- Build custom connectors referencing the Mobile Flows framework. For more information about developing custom connectors, see <https://github.com/vmware/connectors-workspace-one/tree/master/connectors> and <https://github.com/vmwamples/card-connectors-guide>.

Is VMware Boxer a requirement to implement Mobile Flows?

- Yes, VMware Boxer is required to take advantage of the Mobile Flows experience.

How do I purchase Workspace ONE Mobile Flows?

- Mobile Flows is part of the new Workspace ONE Enterprise bundle that is provided along with Workspace ONE Intelligence. Mobile Flows is also available in the Workspace ONE Intelligence add-on SKU.