Setting up VMware Workspace ONE App on Devices

VMware Identity Manager

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-001950-02

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2016 VMware, Inc. All rights reserved. Copyright and trademark information.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Workspace ONE App Documentation

Setting up the VMware Workspace ONE App on Devices provides information about deploying and accessing the VMware Workspace ONE app.

Intended Audience

This information is intended for administrators who manage the availability of the VMware Workspace ONE app in AirWatch for VMware Identity Manager users.

Catalog Integration with AirWatch from VMware Identity Manager 1

Before you deploy VMware Workspace ONE™, configure VMware Identity Manager with your AirWatch instance to enable a unified catalog. When the unified catalog is enabled, native applications that are internally developed or publically available in app stores can be made available to your end users from Workspace ONE.

When AirWatch is integrated with the unified catalog, end users are able to see all apps that they are entitled to from both VMware Identity Manager and AirWatch. To see the apps entitled from AirWatch, end users must enroll their device into AirWatch management.

When AirWatch is not integrated with the unified catalog, end users see only the apps that they are entitled to from VMware Identity Manager. Native apps that your company can develop for internal use and apps that are available on a public store are not available when the catalog is not integrated with AirWatch, even when the device is enrolled in management with AirWatch.

This chapter includes the following topics:

Setting up AirWatch for Integration with VMware Identity Manager

You configure settings in the AirWatch admin console to communicate with VMware Identity Manager before you configure AirWatch settings in the VMware Identity Manager admin console.

When you configure AirWatch for integration, you should perform all the AirWatch configurations at the same organization group level. It is highly recommended that you select the global > customer level organization group from which to set up your AirWatch integration.

The following are set up in the AirWatch admin console.

- REST admin API key for communication with the VMware Identity Manager service
- API Admin account for VMware Identity Manager and the admin auth certificate that is exported from AirWatch and added to the AirWatch settings in VMware Identity Manager
- REST enrolled user API key

Create REST Admin API Key

REST Admin API access must be enabled in the AirWatch admin console to integrate VMware Identity Manager with AirWatch. When you enable Admin API access, an API key is generated.

Procedure

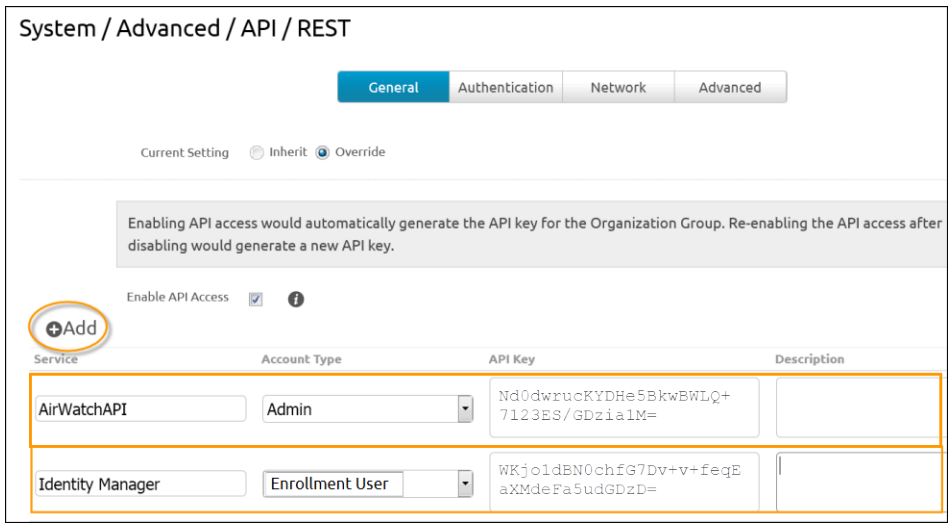
1 In the AirWatch admin console, select the Global > Customer-level organization group and navigate to **Groups & Settings > All Settings > System > Advanced > API > Rest API**.

2 In the General tab, click **Add** to generate the API key to use in the VMware Identity Manager service. The account type should be Admin.

Add a description, such as **`admin API key for VMware Identity Manager`**.

3 Copy the API key and save it to a file.

You add this key when you set up AirWatch in the VMware Identity Manager admin console.



What to do next

In the AirWatch admin console, add an Enrolled User Rest API key and create an admin account and export the admin client certificate.

Create Admin Account and Certificate in AirWatch

After the admin API key is created, you add an admin account and set up certificate authentication in the AirWatch admin console.

For REST API certificate-based authentication, a user level certificate is generated from the AirWatch admin console. The certificate used is a self-signed AirWatch certificate generated from the AirWatch admin root cert.

Prerequisites

The AirWatch REST admin API key is created.

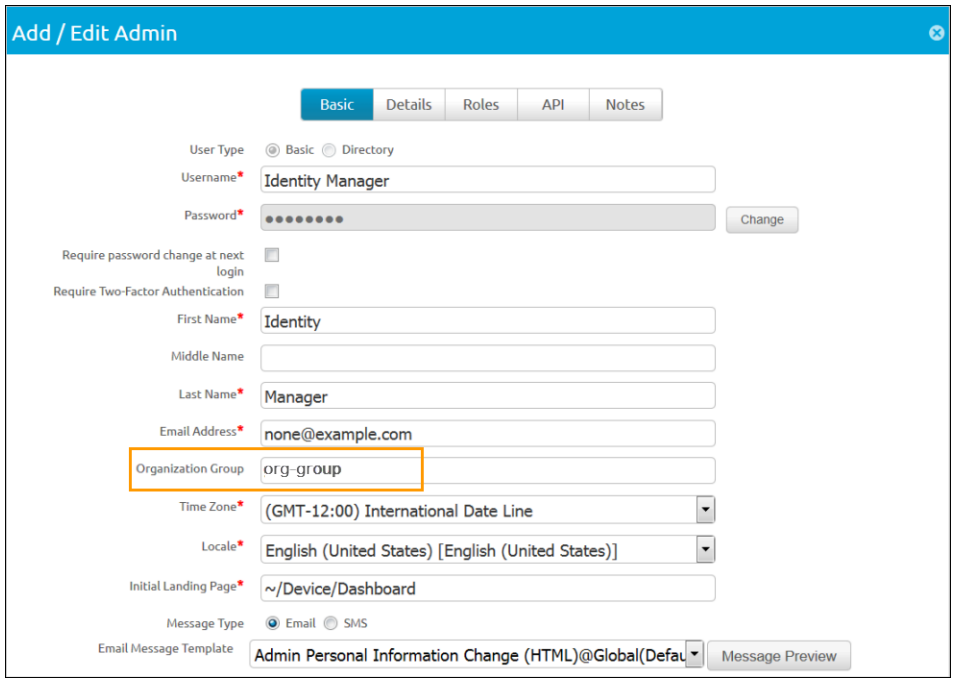
Procedure

1 In the AirWatch admin console, select the Global > Customer-level organization group and navigate to **Accounts > Administrators > List View**.

2 Click **Add > Admin**.

3 In the Basic tab, enter the certificate admin user name and password in the required fields.

Important Make sure the Organization Group shown in the form is the same organization group that the Rest API key was created in.



4 Select the API tab and in the Authentication field, select **Certificates**.

5 Enter the certificate password. The password is the same password entered for the admin on the Basic tab.

6 Click **Generate Client Certificate**.

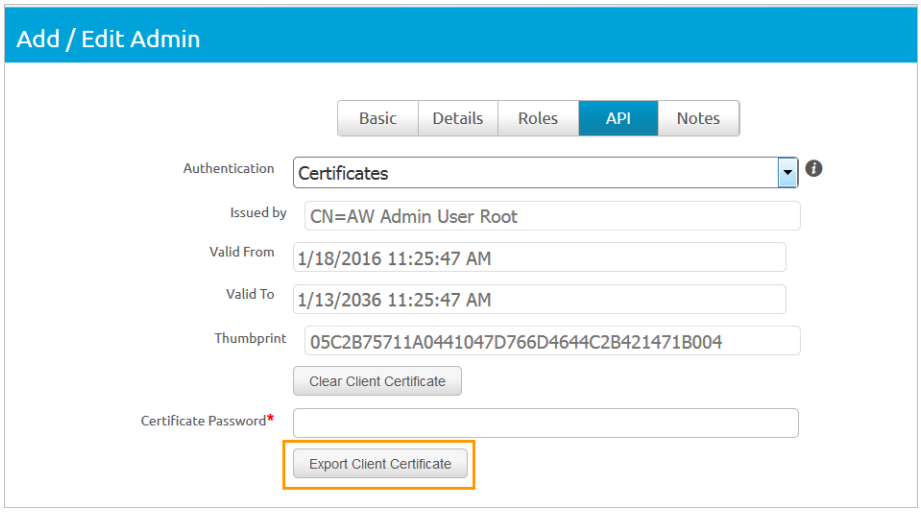
7 Click **Save**.

The new admin account and the client certificate are created.

8 Select the API tab again and in the Authentication drop-down menu, select **Certificates**.

The certificates page displays information about the certificate.

9 Click **Export Client Certificate** and save the file.



The client certificate is saved as a .p12 file type.

What to do next

Configure your AirWatch URL settings in the VMware Identity Manager admin console.

Create REST Enrolled User API Key

REST enrolled user API access must be enabled in the AirWatch admin console.

Procedure

1 In the AirWatch admin console, select the Global >Customer-level organization group and navigate to **Groups & Settings > All Settings > System > Advanced > API > Rest API**.

2 In the General tab, click **Add** to generate the API key to use in the VMware Identity Manager service.

3 In the Account Type drop-down menu, select **Enrolled User**.

Add a description, such as **`enrolled user API key for VMware Identity Manager`**.

4 Copy the API key and save it to a file.

You add this key when you set up AirWatch in the VMware Identity Manager admin console.

Add AirWatch Settings to VMware Identity Manager

Configure AirWatch settings in VMware Identity Manager to integrate AirWatch with VMware Identity Manager and enable the AirWatch feature integration options. The AirWatch API key and the certificate are added for VMware Identity Manager authorization with AirWatch.

Prerequisites

- AirWatch server URL that the admin uses to log in to the AirWatch admin console.
- AirWatch admin API key that is used to make API requests from VMware Identity Manager to the AirWatch server to setup integration.
- AirWatch certificate file used to make API calls and the certificate password. The certificate file must be in the .p12 file format.

- AirWatch enrolled user API key.
- AirWatch group ID for your tenant, which is the tenant identifier in AirWatch.

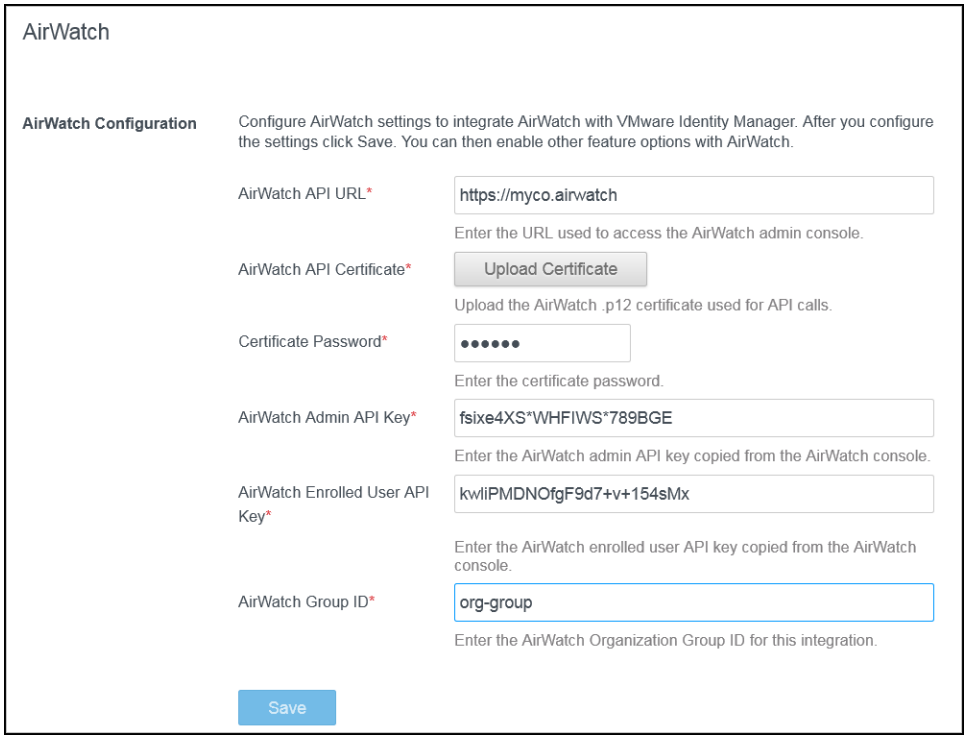
Procedure

1 In the VMware Identity Manager administration console, Identity & Access Management tab, click **Setup > AirWatch**.

2 Enter the AirWatch integration settings in the following fields.

Field	Description
AirWatch URL	Enter the AirWatch URL. For example, `https://myco.airwatch.com`
AirWatch Certificate	Upload the certificate file used to make API calls.
Certificate Password	Enter the certificate password.
AirWatch API Key	Enter the admin API key value. Example of an API key value `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
AirWatch User API Key	Enter the enrolled user API key value.
AirWatch Group ID.	Enter the AirWatch group ID for the organization group that the API key and admin account were created in.

3 Click **Save**.



What to do next

- Enable the AirWatch feature option for a unified catalog to merge applications setup in the AirWatch catalog to the unified catalog.
- Create a directory that syncs to the AirWatch directory and enable and configure AirWatch Cloud Connector for password authentication to AirWatch. .
- Configure Kerberos authentication for AirWatch-managed iOS 9 devices and enable compliance checking.

Enable Unified Catalog for AirWatch

When you configure VMware Identity Manger with your AirWatch instance, you can enable the unified catalog which lets end users see all apps that they are entitled to from both VMware Identity Manager and AirWatch.

When AirWatch is not integrated with the unified catalog, end users see only the apps that they are entitled to from the VMware Identity Manager service.

Prerequisites

AirWatch configured in VMware Identity Manager.

Procedure

1 In the administration console, Identity & Access Management tab, click **Setup > AirWatch**

2 In the Unified Catalog section on this page, select **Enable**.

3 Click **Save**.

What to do next

Notify AirWatch end users about how to access the unified catalog and view their app portal through VMware Identity Manager.

Deploying VMware Workspace ONE 2

When the VMware Workspace ONE app is installed on users' mobile devices, they can access the resources that you have authorized them to use.

Users can launch their entitled application using single sign-on functionality when their identities are managed with VMware Identity Manager. They also have access to an app catalog where they can add more apps they have not yet activated.

The Workspace ONE app interface offers a similar experience and options on any smart phone, tablet, or desktop computer.

If you use AirWatch for mobile device management (MDM), you have the option to push Workspace ONE as a public app.

This chapter includes the following topics:

Supported Platforms

Users can download the Workspace ONE app on any unmanaged or managed device.

The VMware Workspace ONE app works on the following platforms.

- Android 4.1 and later
- Apple iOS 8.0 and later
- Windows 10 desktop and later

Getting and Distributing the VMware Workspace ONE App

Users can either download the VMware Workspace ONE application from their device app store or administrators can configure AirWatch to push the application as a public app to devices that are under mobile device management (MDM) with AirWatch.

For devices that are not managed by AirWatch, users can download and install Workspace ONE from their device app store. After they sign into Workspace ONE they can access Web and SaaS apps that are entitled to them.

For managed devices, you can deploy Workspace ONE from the AirWatch admin console to specific groups and users within your organization. The following steps are to push Workspace ONE as a public app using the AirWatch admin console.

Note For detailed information on configuring public apps in AirWatch, see the AirWatch Mobile Application Management (MAM) Guide, available from the Resources Portal at https://resources.air-watch.com.

Prerequisites

If you are planning to push Workspace ONE from the AirWatch admin console, prepare Smart Groups of end users that are entitled to Workspace ONE.

Procedure

1 In the AirWatch admin console, navigate to **Apps & Books > Applications** > **List View > Public**, and select **Add Application**.

2 Select the platform, either iOS, Android, or Windows.

3 Select **Search App Store**, and in the **Name** field enter `Workspace ONE` as the key word to find VMware Workspace ONE in the App Store.

4 Choose **Next**, and use **Select** to upload the VMware Workspace ONE app from the App Store Result page.

5 Configure the assignment and deployment options for Workspace ONE users in the following tab settings.

Tab	Description
Info	Enter and view information concerning supported device models, ratings, and categories.
Assignment	Assign Workspace ONE to smart groups of end-users that can use the Workspace ONE app on their device.
Deployment	Configure availability and advanced enterprise mobility management (EMM) features, if applicable. To automatically configure managed applications, enable **Send Application Configuration** and enter the App Configuration for Enterprise (ACE) key value pairs. See "AirWatch App Configuration for Enterprise Key Value Pairs," on page 14.
Terms of Use	Enable Terms of Use to require users to accept the terms of use before using Workspace ONE.

6 Select **Save & Publish** to make the application available to users.

Complete these steps for each supported platform.

AirWatch App Configuration for Enterprise Key Value Pairs

When deploying the Workspace ONE app as a public application in AirWatch and you enable Send Application Configurations when you push the Workspace ONE app from the AirWatch catalog, you can preconfigure Workspace ONE settings that are applied when users deploy Workspace ONE from the catalog.

When the Workspace ONE app is uploaded to the AirWatch admin console as a managed mobile application, you can automatically configure the VMware Workspace ONE Server URL, the device UID value, and requirement for certificate authentication in Android devices.

Table 2-1. Workspace ONE Managed Device Configurations Options in AirWatch Admin Console

Platform	Configuration Key	Value Type	Configuration Value	Explanation
All	`AppServiceHost`	String	**<VMware Workspace ONE Server URL>**	Configures the server URL for VMware Workspace ONE on devices.
All	`deviceUDID`	String	**{DeviceUid}** Enter the device UID value. Do not use the Insert Lookup Value function.	Tracks the devices used to authenticate to the VMware Identity Manager environment.
Android	`RequireCertAuth`	Boolean	**True**	Requires VMware Workspace ONE to use certificates for authentication when integrated with Android for Work
Android	`ManagedAppCertAlias` (Dependent on RequireCertAuth set to True)	String	**<Android app certificate alias value>** Note: This value is the UUID for the credentials profile you configured for your Android for Work integration	Identifies the certificate VMware Workspace ONE uses when using certificates to authenticate when integrated with Android for Work.

Note For detailed information integrating VMware Identity Manager, AirWatch, and Android for Work, see the article Mobile SSO with AirWatch and VMware Identity Manager, available from the AirWatch Knowledge Base at https://support.air-watch.com/home.

Session Authentication Setting

The VMware Identity Manager service includes a default access policy that controls user access to their VMware Identity Manager resources.

The authentication session length configured in the policy rules determine the maximum amount of time users have since their last authentication event to access their apps launcher page or to launch a specific Web application. The default is eight hours. After users authenticate, they have eight hours to launch a Web application unless they initiate another authentication event that extends the time.

You can edit the default policy to change the session length from the VMware Identity Manager administration console, Identity & Access Management tab, Manage > Policies. See the VMware Identity Manager Administration guide, Managing Access Policies.

Customize Branding for the User Portal

You can add a logo, change the background colors and add images to customize the end user's Web view from the browser and from their mobile and tablet devices.

Procedure

1 In the VMware Identity Manager administration console Catalogs tab, select **Settings > User Portal Branding**.

2 Edit the settings in the form as appropriate.

Note Some settings on the User Portal Branding page are no longer used. If a setting is not listed in this table, that setting is not used and cannot be customized.

Form Item	Description
Logo	Add a logo to be the banner image at the top of the admin console and user's app portal Web pages. The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG or GIF.
	Portal (Web View)
Background Color	The color that displays for the background of the Web portal screen. Enter a new six-digit hexadecimal color code over the existing one to change the background color. The background color changes in the app portal preview screen when you type in a new color code. However, if an image is added, the background color might not be visible in the preview. Select **Background Highlight** to accent the background color. If this is enabled, browsers that support multiple background images show the overlay in the launcher and catalog pages. Select **Background Pattern** to set the predesigned triangle pattern in the background color.
Name and Icon Color	You can select the text color for names listed under the icons on the app portal pages. Enter a hexadecimal color code over the existing one to change the font color.
Lettering effect	Select the type of lettering to use for the text on the user's portal screens.
Image (Optional)	To add an image to the background on the app portal screen instead of a color, upload an image.
	Portal (Mobile and Tablet Views)
Title bar color	This is the background color of the banner. Enter a six-digit hexadecimal color code over the existing one to change the title bar color viewed from the user's app portal or mobile device. Select **Title Bar pattern** to set the predesigned triangle pattern in the title bar color.
Title color	Enter a six-decimal hexadecimal color code over the existing one to change the text color used in the title bar heading.
Use the same values for both the Launcher and the Catalog	If you want to use the same branding design for the App Center screen view as used for the user's portal screen view on mobile devices, check this box. If you want to design the App Center screen differently, leave this box unchecked and configure the background, title bar color and title color for the App Center screen.
	First-Time User Tour
First-Time User Tour	The first time user tour is not available.

3 Click **Save**.

Custom branding updates are refreshed every 24 hours for the user portal. To push the changes sooner, as the administrator, open a new tab and enter this URL, substituting your domain name for myco.example.com. `https://<myco.example>.com/catalog-portal/services/api/branding?refreshCache=true`.

What to do next

Check the appearance of the branding changes in the various interfaces.

Using VMware Workspace ONE

Users download the Workspace ONE app from an app store to their mobile device. To sign in to the Workspace ONE app, users must authenticate to VMware Identity Manager.

Users must know your company's VMware Workspace ONE URL, the VMware Identity Manager domain name, and their VMware Identity Manager sign-in credentials. Typically, the administrator sends a welcome email with this information.

The Workspace ONE app icon appears on their device.

The **Select your domain** dialog box appears with the domain menu. Users select their domain and on the next dialog box enter their user name and password.

Users stay signed in to Workspace ONE until they sign out or until their session times out.

Setting Passcodes for the Workspace ONE App

The first time the Workspace ONE app is launched, users are required to create a passcode. This passcode is entered whenever users access Workspace ONE from their device.

When the Workspace ONE app is installed, users are prompted to set up a four-digit passcode to access the Workspace ONE app. Where the passcode is set depends on the platform. For Android devices, the passcode is set at the app level. For iOS devices and Window desktop devices, the passcode is set at the device level.

Workspace ONE can detect possible security issues on devices. If users remove the passcode requirement from the device, the next time they access the Workspace ONE app they are prompted to set the passcode before they can access Workspace ONE.

If other types of security issues are detected, an error message directing users to contact their admin is displayed. This functionality helps to secure the mobile network and the enterprise's mobile assets.

Working in VMware Workspace ONE 3

When the VMware Workspace ONE app is installed on devices, users can sign into Workspace ONE to securely access a catalog of applications that your organization enabled for them. They do not need to reenter their sign-in credentials when they launch the apps.

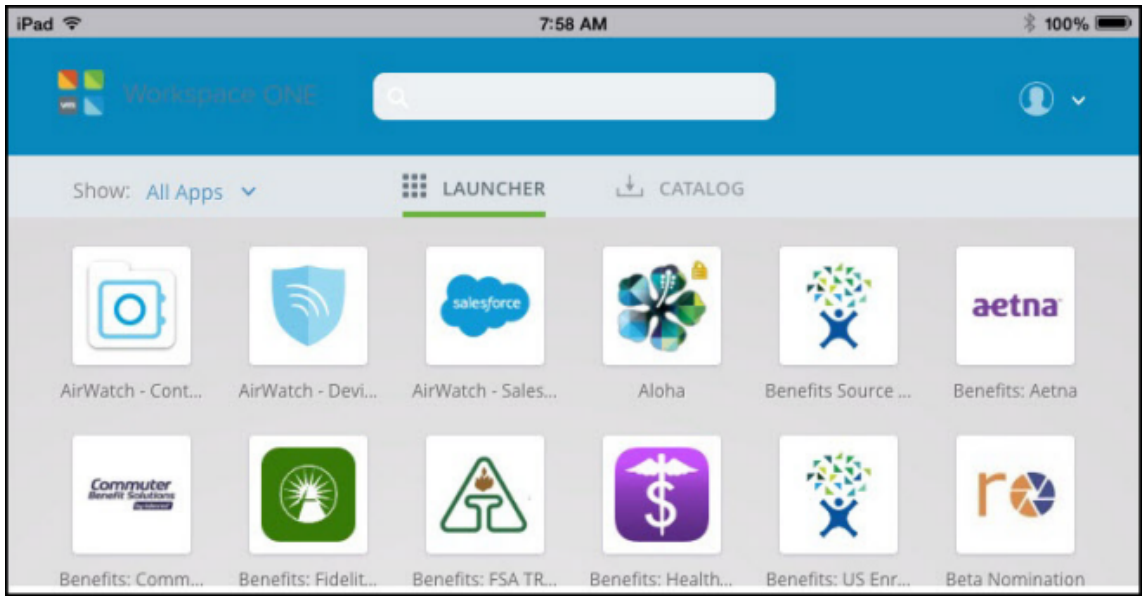
The Workspace ONE user interface works similarly on phones, tablets, and desktops. Workspace ONE opens to a Launcher page that displays resources that have been pushed to Workspace ONE. Users can tap or click to search, add, and update apps; right-click on an app to remove it from the page, and go to the Catalog page to add entitled resources.

This chapter includes the following topics:

Working with Web Apps in Workspace ONE

When users sign in to Workspace ONE, the first page that appears is the Launcher page. The Launcher page displays the Web apps that are ready to access and use from Workspace ONE.

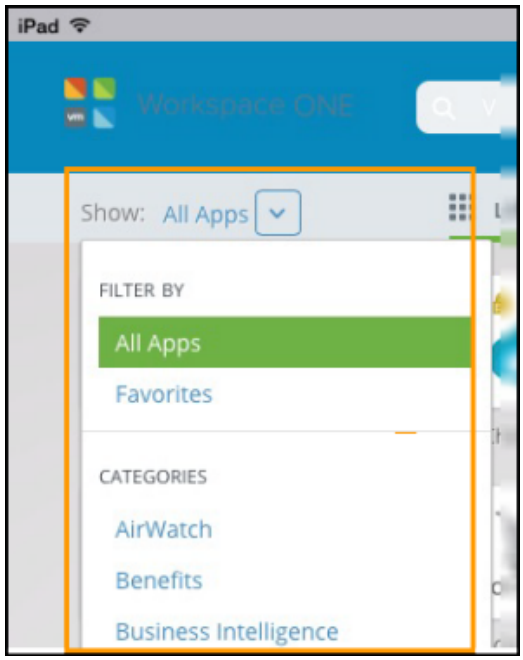
Figure 3-1. Workspace ONE App Launcher Page



Users can long press on an app icon to see more information about the app and to mark the app as a favorite.

The **Show** drop-down menu lets users select the category of apps that display on the Launcher page, including the apps that are favorites in the Favorites category.

Figure 3-2. Select Apps by Category



Applications that are available to users are displayed in the Catalog page. Users tap Add on an app icon to add the app to the Launcher page. They can long press the app icon for information about the app, the categories to which the app applies, and the app version.

When native apps are added to the device, they are added directly to the device's home screen. They do not appear in the Workspace ONE Launcher page.

Users tap a Web app icon on the Launcher page to open it in the browser.

Adding Native Applications on Managed Devices

Native applications are app programs that are developed for a specific mobile device. Users can see their AirWatch-entitled native applications from the Workspace ONE Catalog page. For example, if a user is viewing the catalog from an iOS device, only iOS applications entitled to the user are shown.

In the Catalog page, users tap Install to install the app on their device. Upon tapping Install, a pop-up appears to let users know what is happening next. The information displayed is based on the app type and platform.

Index