Setting up VMware Workspace ONE Application 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-002264-00

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

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

Contents

About VMware Workspace ONE Application Documentation

Setting up the VMware Workspace ONE Application on Devices provides information about deploying and accessing the VMware Workspace® ONE® application.

Intended Audience

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

Workspace ONE Version 2.1, released September 2016

Catalog Integration with AirWatch from VMware Identity Manager 1

Before you deploy the VMware Workspace® ONE™ mobile application, 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 the Workspace ONE portal.

When AirWatch is integrated with the unified catalog, end users can see all apps that they are entitled to from both VMware Identity Manager and AirWatch. Applications that display with a locked icon require users to enable Workspace services before the application can be installed and used.

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.

To integrate AirWatch and VMware Identity Manager, the following is required.

- The organization group in AirWatch for which you are configuring VMware Identity Manager is **Customer**.
- A REST API admin key for communication with the VMware Identity Manager service and a REST enrolled user API key for AirWatch Cloud Connector password authentication are created at the same organization group where VMware Identity Manager is configured.
- API Admin account settings and the admin auth certificate from AirWatch added to the AirWatch settings in the VMware Identity Manager admin console.
- Active Directory user accounts set up at the same organization group where VMware Identity Manager is configured.
- If end users are placed into a child organization group from where VMware Identity Manager is configured after registration and enrollment, User Group mapping in the AirWatch enrollment configuration must be used to filter users and their respective devices to the appropriate organization group.

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 used for AirWatch Cloud Connector password authentication

Create REST API Keys in AirWatch

REST Admin API access and enrolled users access must be enabled in the AirWatch admin console to integrate VMware Identity Manager with AirWatch. When you enable 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.

Provide a unique service name. Add a description, such as **`AirWatchAPI for IDM`**.

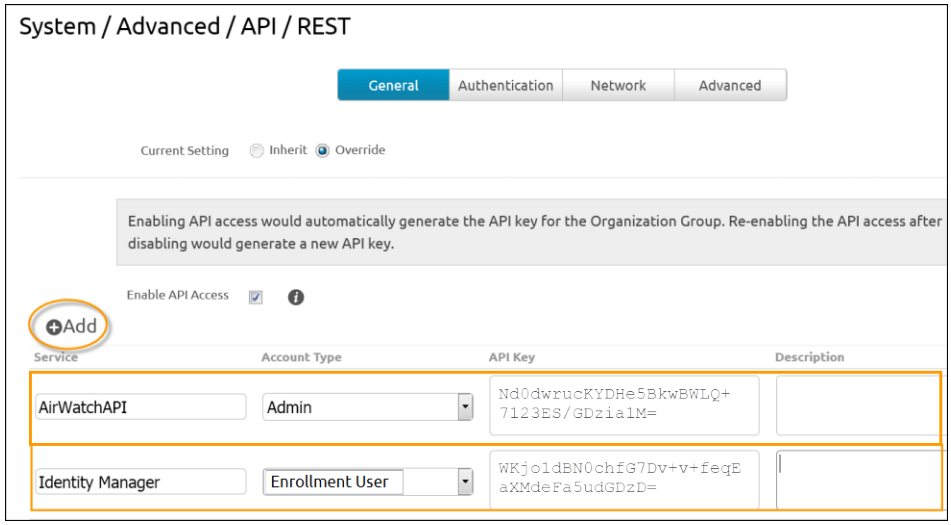
3 To generate the enrollment user API key, click **Add** again.

4 In the Account Type drop-down menu, select **Enrollment User**.

Provide a unique service name. Add a description such as **`UserAPI for IDM`**.

5 Copy the two API keys and save the keys to a file.

You add these keys when you set up AirWatch in the VMware Identity Manager admin console.



6 Click **Save**.

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

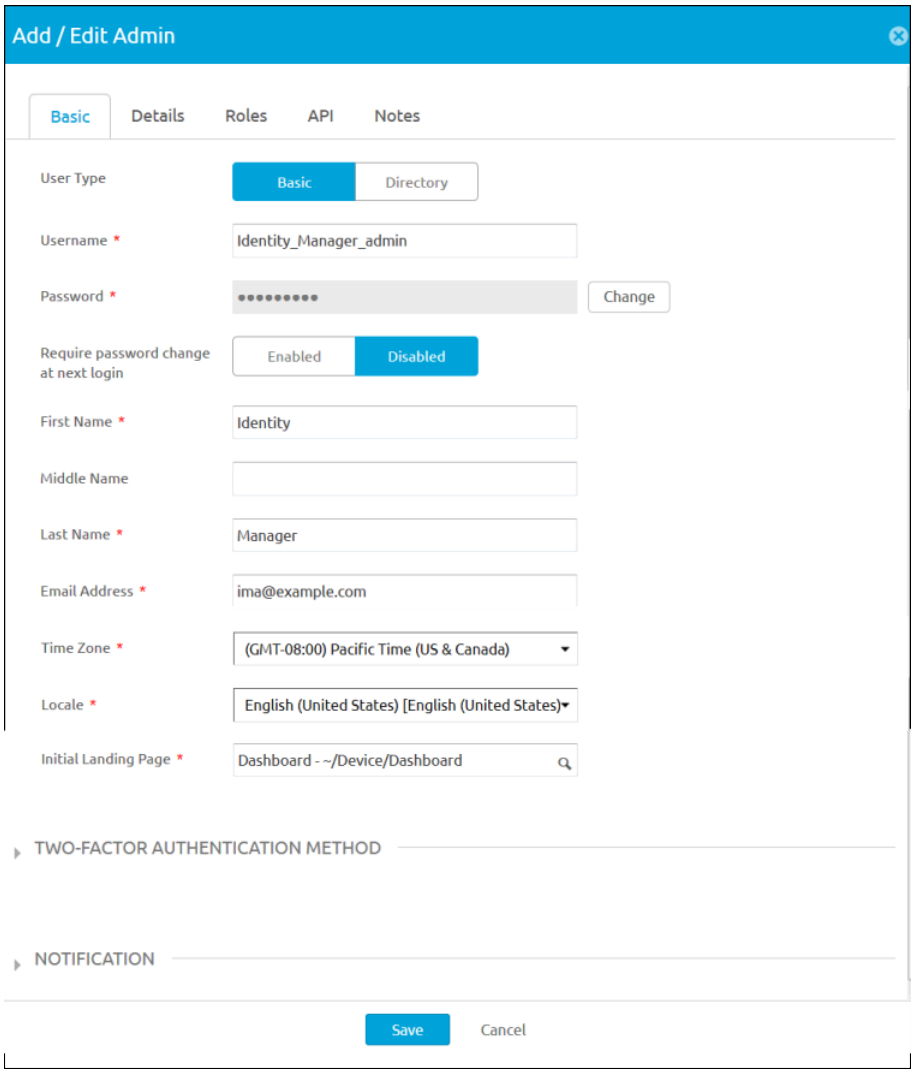
The AirWatch REST admin API key is created.

Procedure

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

2 Click **Add > Add Admin**.

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



4 Select the Roles tab; choose the current organization group and in the drop-down menu, select **AirWatch Administrator**.

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

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

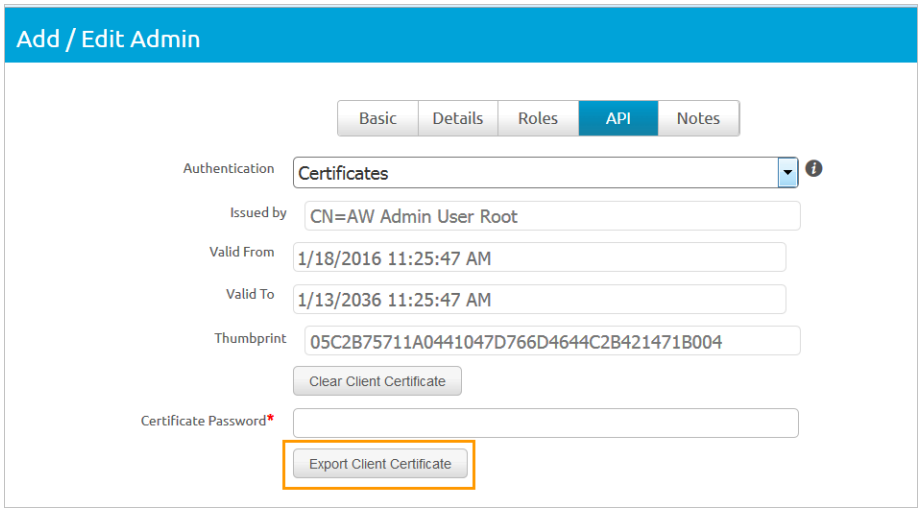
7 Click **Save**.

The new admin account and the client certificate are created.

8 In the List View page, select the admin you created and open the API tab again.

The certificates page displays information about the certificate.

9 Enter the password you set in the Certificate Password field, 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 **Enrollment User**.

Provide a unique service name. 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.

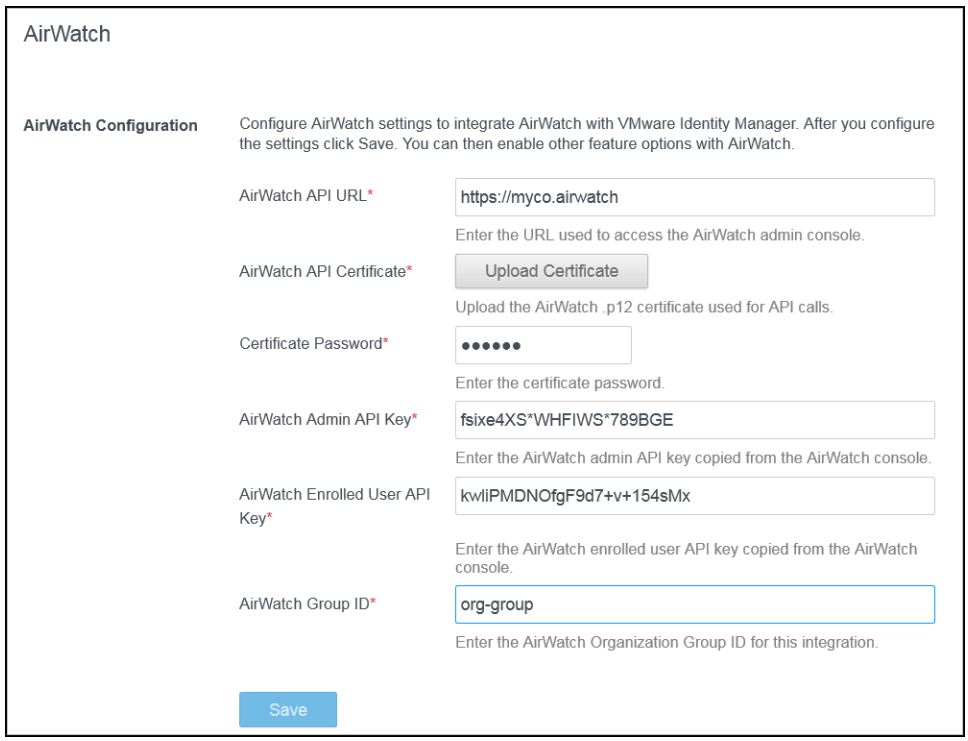
Procedure

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 API URL	Enter the AirWatch URL. For example, `https://myco.airwatch.com`
AirWatch API Certificate	Upload the certificate file used to make API calls.
Certificate Password	Enter the certificate password.
AirWatch Admin API Key	Enter the admin API key value. Example of an API key value `FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=`
AirWatch Enrolled 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 feature option Unified Catalog to merge apps set up in the AirWatch catalog to the unified catalog.
- Enable Compliance check to verify that AirWatch managed devices adhere to AirWatch compliance policies.

See "Enable Compliance Checking for AirWatch Managed Devices," on page 18.

Enable Unified Catalog for AirWatch

When you configure VMware Identity Manager 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 Workspace ONE portal through VMware Identity Manager.

Deploying the VMware Workspace ONE Mobile Application 2

When the VMware Workspace ONE application is installed on mobile devices, users can access the resources that you authorized for their use.

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

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

If the device is enrolled in mobile device management (MDM), you can push the Workspace ONE application as a public application.

This chapter includes the following topics:

Supported Platforms

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

The VMware Workspace ONE application works on the following platforms.

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

Managing Access to Applications

Internal and public applications can be deployed as either managed or unmanaged when using AirWatch for native application delivery. This adaptive management approach protects data inside applications without requiring devices to be managed.

Adaptive management is available on the following devices.

- Apple iOS
- Android for Work
- Windows 10

When applications are managed, users must enable Workspace services to install and use the managed applications. When you upload an application in the AirWatch admin console, you can enable the **Device must be MDM managed to install** option to require the device be managed before the application can be installed.

Applications that require management display a lock icon when viewed in an unmanaged state in the catalog. Users must choose to enable Workspace services through the adaptive management process to use the application. When users attempt to download an application that displays a lock icon, they are prompted with a message that reads `Installation of this app requires enablement of Workspace Services`. Users can click the Learn More link to see the privacy impact for their personal information if they choose to continue with the adaptive management process. The privacy notice automatically pulls settings from the AirWatch environment they are about to enroll into. After reviewing the privacy setting information, users can either proceed to enable Workspace services or back out and continue to use the Workspace ONE application unmanaged on their device. When users enable Workspace services, the lock icon is removed from all the managed applications.

See the VMware AirWatch Mobile Application Management Guide for detailed information about uploading and configuring applications to be managed. See the VMware AirWatch Bring Your Own Device (BYOD) Guide for information about the AirWatch provided ready-made BYOD environment.

Disabling Workspace One Services on Managed Devices

Users can disable the Workspace ONE app on their managed device from the Workspace ONE About page. Administrators can perform an enterprise wipe from the Air Watch admin console to disable Workspace ONE services.

Disabling Workspace ONE on managed devices revokes access granted through the Workspace ONE application and disables the account in AirWatch. Apps that required management are removed from the device and access to AirWatch productivity apps such as Boxer, Browser, and Content Locker, is revoked.

Getting and Distributing the Workspace ONE Application

Users can either download the VMware Workspace ONE application from their device app store or administrators can configure AirWatch to push the Workspace ONE application as a public application to devices.

You deploy the Workspace ONE application from the AirWatch admin console to specific groups and users within your organization. After users sign into the Workspace ONE application on their devices, they can access Web and SaaS apps that are entitled to them.

The following steps are to push the Workspace ONE mobile application as a public application from the AirWatch admin console.

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

Prerequisites

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

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** text box 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 application 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 the Workspace ONE mobile application to smart groups of end users who can use the application 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 15.
Terms of Use	(Optional) 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.

Registering Email Domains for Auto Discovery

You can register your email domain in the auto discovery service in VMware Identity Manager to make it easier for end users to access their apps portal through the Workspace ONE application. End users enter their email address instead of the organization's URL.

When auto discovery is not used, the first time that end users open the Workspace One application, they must provide the complete organization URL. For example, they enter **myco.vmwareidentity.com**.

When the email domain of the organization is registered for auto discovery, end users enter only their email address in the sign-in page to access their apps portal. For example, they enter **username@myco.com**.

Set up Auto Discovery in VMware Identity Manager

To register a domain, you enter your email domain and email address in the VMware Identity Manager admin console Auto Discovery page.

An email message with an activation-token is sent to your email address on the domain. To activate the domain registration, you enter the token in the Auto Discovery page and verify that the domain you registered is your domain.

Note To set up auto discovery for VMware Identity Manager on-premises deployments, you must log in to the admin console as the local admin. You enter the AirWatch ID and password that you created in the AirWatch Web site, https://secure.air-watch.com/register.

Procedure

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

2 (On-premises deployments only). Configure the AirWatch auto discovery URL.

Option	Description
Auto Discovery URL	Enter the URL as https://discovery.awmdm.com.
AirWatch ID	Enter the email address you registered with AirWatch to log in to their Web site.
Password	Enter the password associated with the AirWatch account.

3 In the **Email Domain** text box, enter your organizations email domain to register.

4 In the **Confirmation Email Address** text box, enter an email address on that email domain to receive the verification token.

5 Click **OK**.

The status of this email domain registration is marked Pending. You can have only one pending email domain at a time.

6 Navigate to the email and copy the activation token that is in the message.

7 Return to the **Identity & Access Management > Auto Discovery** page and paste the token in the Activation Token text box

8 Click **Verify** to register the domain.

The email domain is registered and is added to the list of registered email domains on the Auto Discovery page.

End users can now enter their email address in the Workspace ONE application to access their app portal.

What to do next

If you have more than one email domain, add another email domain to register.

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.

Enable Compliance Checking for AirWatch Managed Devices

When users enroll their devices through the AirWatch Agent application, samples containing data used to evaluate compliance are sent on a scheduled basis. The evaluation of this sample data ensures that the device meets the compliance rules set by the administrator in the AirWatch console. If the device goes out of compliance, corresponding actions configured in the AirWatch console are taken.

VMware Identity Manager includes an access policy option that can be configured to check the AirWatch server for device compliance status when users sign in from the device. The compliance check ensures that users are blocked from signing in to an application or using single sign-in to the VMware Identity Manager portal if the device goes out-of-compliance. When the device is compliant again, the ability to sign in is restored.

The Workspace ONE application automatically signs out and blocks access to the applications if the device is compromised. If the device was enrolled through adaptive management, an enterprise wipe command issued through the AirWatch console un-enrolls the device and removes the managed applications from the device. Unmanaged applications are not removed.

For more information about AirWatch compliance policies, see the VMware AirWatch Mobile Device Management Guide, available on the AirWatch Resources Web site.

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.

Form Item	Description
Logo	Add a masthead logo to be the banner at the top of the admin console and user's Workspace ONE portal Web pages. The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG or GIF.
	Portal
Masthead Background Color	Enter a new six-digit hexadecimal color code over the existing one to change the background color of the masthead. The background color changes in the app portal preview screen when you type in a new color code.
Masthead Text Color	Enter a new six-digit hexadecimal color code over the existing one to change the color of the text that displays in the masthead.
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. 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.

Form Item	Description
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.

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 the Workspace ONE Mobile Application

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

The Workspace ONE application icon appears on their device.

Users must know the 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.

Note When auto discovery is configured with your registered email domain, users enter their email address instead of the URL to access the Workspace ONE application. The next screen asks for their sign-in credentials.

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 Application

Users must have the lock out passcode feature enabled on their devices. If it is not enabled, the first time the Workspace ONE application is launched, users are asked to create a passcode. This passcode is entered whenever users access Workspace ONE from their device.

If the passcode feature is not used, users are prompted to set up a passcode before they can access the Workspace ONE application. 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.

Note iOS devices also support the Touch ID fingerprint sensing functionality.

Workspace ONE can detect possible security issues on devices. If users disable the passcode on the device, the next time they access the Workspace ONE application, they are prompted to set a passcode before they can access Workspace ONE.

Working in the Workspace ONE Mobile Application 3

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

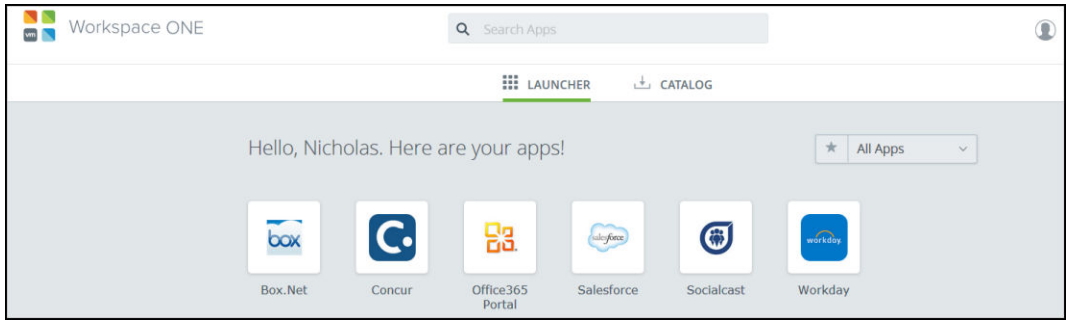
The Workspace ONE user interface works similarly on phones, tablets, and desktops. Workspace ONE opens to a Launcher page that displays resources that have been pushed to Workspace ONE. Users can tap or click to search, add, and update apps; right-click on an app to remove it from the page, and go to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

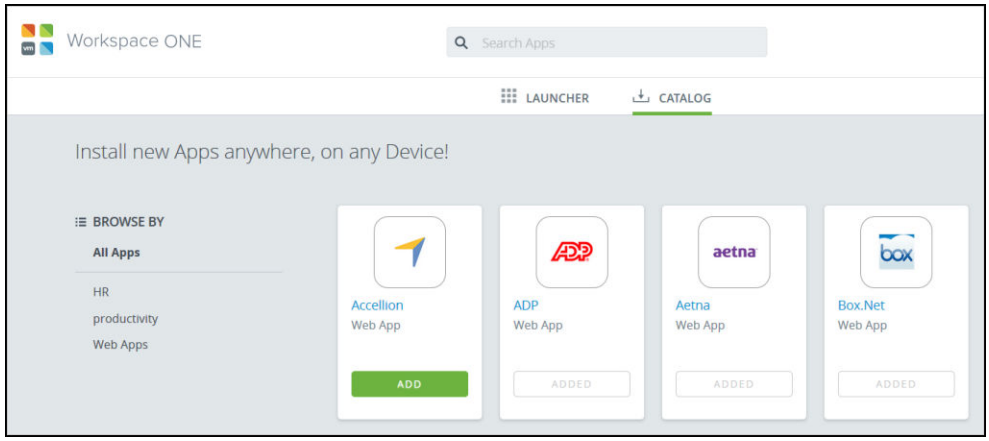
Figure 3-1. Workspace ONE App Launcher Page



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

The Catalog page displays all the apps that the user can download. Users can browse for apps by categories.

Figure 3-2. Workspace ONE Catalog Page



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

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. Applications that display a lock icon require that the device be managed by AirWatch. When an end user attempts to download an app with a lock icon, they are prompted with a message that reads `Installation of this app requires enablement of Workspace Services`.

Index