

# Guide to Deploying VMware Workspace ONE

MAY 2018

VMware AirWatch 9.3

VMware Identity Manager 3.2



vmware®

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

<https://docs.vmware.com/>

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

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2017–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

About Deploying VMware Workspace ONE	5
<b>1 Introduction to Workspace ONE</b>	<b>6</b>
Workspace ONE Architecture Overview	6
Requirements	7
Workspace ONE Feature Details	7
Getting Started with the Workspace ONE Wizard	8
<b>2 Integrating AirWatch With VMware Identity Manager</b>	<b>10</b>
Set Up Integration from AirWatch Admin Console	10
Setting up an AirWatch Instance in VMware Identity Manager	13
Enable Workspace ONE Catalog for AirWatch	16
Enabling Compliance Checking for AirWatch Managed Devices	16
Enable User Password Authentication through AirWatch	17
Configure Access Policy Rule	17
Updating VMware Identity Manager After Upgrading AirWatch	19
Implementing Authentication with AirWatch Cloud Connector	20
<b>3 Implementing Mobile Single Sign-in Authentication for AirWatch -Managed iOS Devices</b>	<b>24</b>
Implementation Overview to Configure Mobile SSO for iOS	24
Configure Active Directory Certificate Authority in AirWatch	25
Using AirWatch Certificate Authority for Kerberos Authentication	28
Using a Key Distribution Center for Authentication from iOS Devices	29
Configure Mobile SSO for iOS Authentication	30
Configure Built-in Identity Provider for Mobile SSO iOS Authentication	32
Configure Apple iOS Profile in AirWatch Using Active Directory Certificate Authority and Certificate Template	32
Configure Apple iOS Profile in AirWatch Using AirWatch Certificate Authority	34
Assign an AirWatch Device Profile	36
<b>4 Implementing Mobile Single Sign-On Authentication for AirWatch -Managed Android Devices</b>	<b>37</b>
Configure Single-Sign-on for Android Device from AirWatch Admin Console	38
Configure VMware Tunnel VPN Access Settings from AirWatch Admin Console	39
Configure Per App Tunnel Profile for Android	41
Enable Per-App VPN for Android Apps	41
Configure Traffic Rules in AirWatch	42

	Configure Mobile SSO for Android Authentication in the Built-in Identity Provider	44
<b>5</b>	<b>Direct Enrollment in AirWatch Using Workspace ONE</b>	<b>47</b>
	Enable Workspace ONE for Direct Enrollment	47
	User Experience When Directly Enrolling into AirWatch with Workspace ONE	50
<b>6</b>	<b>Leveraging Workspace ONE to Support Apple Device Enrollment Program Integration</b>	<b>58</b>
<b>7</b>	<b>Enabling the Out of Box Experience for Workspace ONE on Dell Windows 10 Devices</b>	<b>60</b>
	Enable External Access Token in AirWatch	60
	Activate External Access Token as an Authentication Method	61
	Associate External Access Token Authentication Method to the Built-in Identity Provider	62
	Create Access Policy for Workspace ONE Out-of-Box Experience Process	63
	Workspace ONE for Windows 10 Custom Out-of-Box Branding	64
<b>8</b>	<b>Deploying the VMware Workspace ONE Mobile Application</b>	<b>66</b>
	Device Management Options in AirWatch for Public and Internal Apps for Workspace ONE	66
	Managing Access to Applications	68
	Requiring Terms of Use to Access the Workspace ONE Catalog	69
	Getting and Distributing the Workspace ONE Application	70
	Registering Email Domains for Auto Discovery	73
	Session Authentication Setting	74
	Deployment Strategies for Setting Up Multiple AirWatch Organization Groups	75
<b>9</b>	<b>Working in the Workspace ONE Portal</b>	<b>79</b>
	Working with Applications in Workspace ONE	79
	Setting Passcodes for the Workspace ONE Application	83
	Adding Native Applications	83
	Using VMware Verify for User Authentication	84
	Send Alerts to Workspace ONE Users	84
	Working with Workspace ONE for Android Devices	84
<b>10</b>	<b>Using the Workspace ONE Catalog</b>	<b>87</b>
	Managing Resources in the Catalog	87
<b>11</b>	<b>Custom Branding for VMware Identity Manager Services</b>	<b>90</b>
	Customize Branding in VMware Identity Manager Service	90
	Customize Branding for the User Portal	91
<b>12</b>	<b>Accessing Other Documents</b>	<b>93</b>

# About Deploying VMware Workspace ONE

The Guide to Deploying VMware Workspace™ ONE™ provides information about integrating VMware Identity Manager™ and VMware AirWatch® to provide single sign-on to Workspace ONE, device management in AirWatch, and VMware Workspace ONE as a catalog of applications.

When AirWatch and VMware Identity Manager are integrated, users with AirWatch enrolled devices can log in to their enabled applications securely without entering multiple passwords.

## Intended Audience

This information is intended for administrators who are familiar with both AirWatch and VMware Identity Manager services.

# Introduction to Workspace ONE

VMware Workspace® ONE® is a secure enterprise platform that delivers and manages applications on iOS, Android, and Windows 10 devices. Identity, application, and enterprise mobility management are integrated into the Workspace ONE platform.

VMware AirWatch® and VMware Identity Manager™ are integrated to give you the Workspace ONE catalog of applications and mobile access management services.

VMware Identity Manager services provide the identity-related components, including authentication for users who single sign-on to their resources. You create a set of policies that relate to networking and authentication to control access to these resources.

AirWatch services provide device enrollment, application distribution, and compliance checking tools to ensure that remote access devices meet corporate security standards. Users from AirWatch enrolled devices can log in to their enabled applications securely without entering multiple passwords.

This chapter includes the following topics:

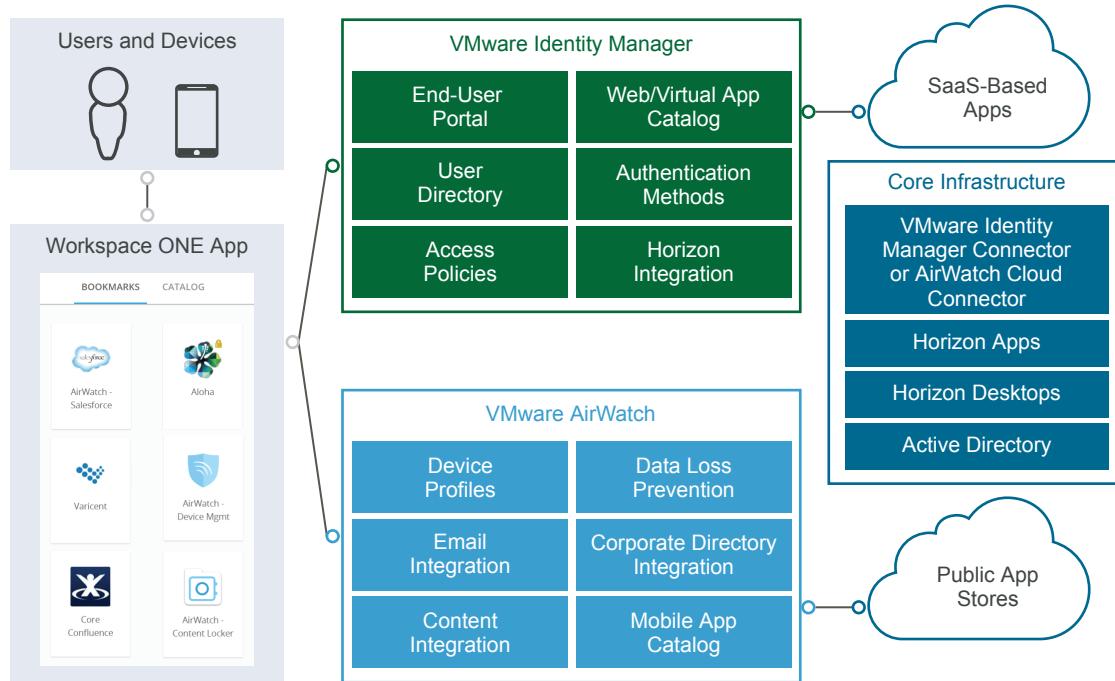
- [Workspace ONE Architecture Overview](#)
- [Requirements](#)
- [Workspace ONE Feature Details](#)
- [Getting Started with the Workspace ONE Wizard](#)

## Workspace ONE Architecture Overview

Workspace ONE provides users secure access to cloud, mobile, and Windows applications managed from a unified catalog. For device access, the Workspace ONE native application is available for iOS, Android, and Windows 10 devices.

When Workspace ONE is deployed, the following VMware Identity Manager and AirWatch services must be implemented.

- VMware Enterprise Systems Connector installed and configured. You can either configure the VMware Identity Manager Connector component or the AirWatch Cloud Connector (ACC) component.
- Integration of your company's Active Directory with VMware Identity Manager or with AirWatch Cloud Connector to sync users and groups from Active Directory to the Workspace ONE service.
- Configure VMware Identity Manager with AirWatch API keys and the administrator root certificate and enable the unified catalog, compliance check, and user password authentication through AirWatch.

**Figure 1-1. Workspace ONE Architecture Overview**

## Requirements

The Workspace ONE system requirements are listed below.

**Table 1-1. Workspace ONE System Requirements**

Workspace ONE Requirements	Details
Active Directory	Windows Server 2008 and 2008 R2 Windows Server 2012 and 2012 R2
Web browser to access VMware Identity Manager and AirWatch admin console	Internet Explorer 11 for Windows Google Chrome 4.0 and later Mozilla Firefox 40 and later Safari 6.2.8 and later
VMware Enterprise Connector, with either the VMware Identity Manager Connector or AirWatch Cloud Connector or installed.	Windows Server 2008 R2 Windows Server 2012 or 2012 R2 .NET framework 4.6.2 See the VMware Enterprise Systems Connector Installation and Configuration guide to deploy the connectors.

## Workspace ONE Feature Details

The major features in Workspace ONE are described below.

## Native Mobile Workspace ONE Applications

Users can install the Workspace ONE application on a mobile device and use corporate credentials for single sign-on (SSO) access to corporate, cloud, and mobile applications.

## Self-service App Catalog for Web, Horizon, and Citrix Resources

Workspace ONE provides users access to cloud, mobile, and Windows applications using a unified catalog. The catalog contains applications published to VMware Identity Manager and VMware AirWatch. Supported application types include internal web, SaaS, native mobile, internally developed mobile, legacy and modern Windows, Horizon 7, VMware Horizon Cloud Service™, Citrix published, and ThinApp packages. The application store also contains virtualized desktops.

## Launch Web and Virtual Apps with Single Sign-on

Workspace ONE provides mobile single sign-on (SSO), a one-touch login implementation to mobile applications. Mobile SSO is available for Android, iOS, and Windows 10 devices.

## Conditional Access with Device Compliance

With Workspace ONE, you can enforce conditional access based on the network range, platform, and application-specific criteria for authentication. A device must prove compliance with security rules before authorizing access to an application. 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.

## Multi Factor Authentication

Workspace ONE provides multi factor authentication through the VMware Verify application. When a user attempts to access the Workspace ONE catalog or any application requiring strong authentication, VMware Verify sends a notification to the user's phone. To verify attempted access to Workspace ONE, the user must swipe Accept to access the application.

## Adaptive Management

For applications that require only a basic level of security, users are not required to enroll their device into AirWatch Mobile Device Management™. Users can download the Workspace ONE mobile application and select the applications they want to install. For applications that require a higher level of security, users can enroll their device into AirWatch directly from the Workspace ONE mobile application.

## Getting Started with the Workspace ONE Wizard

You can use the Workspace ONE Getting Started wizard to guide you through many of the configuration steps to integrate AirWatch and VMware Identity Manager services to create the Workspace ONE environment.



The Getting Started wizard does not replace the ability to configure or edit any individual setting, but significantly automates the initial setup for most customers.

The Workspace ONE Getting Started wizard can be used to set up the following.

- **Enterprise Connector & Directory.** The wizard walks you through the steps to set up the VMware Enterprise System Connector and configure the Active Directory connection from the AirWatch Cloud Connector to import users and groups from your company's directory. See the VMware Workspace ONE Quick Configuration Guide to help you set up the Enterprise Connector.
- **Auto Discovery.** Run the wizard to register your email domain in the auto discovery service to make it easier for end users to access their apps portal through the Workspace ONE application. End users then enter their email address instead of the organization's URL.
- **Workspace ONE Catalog.** The Workspace ONE Catalog wizard walks you through the steps to set up the Workspace ONE catalog. You can also use the Workspace ONE custom branding step to add your company's brand information to the Workspace ONE catalog and application. See the VMware Workspace ONE Quick Configuration Guide to help you set up the Workspace ONE Catalog.
- **Adaptive Management.** Set up adaptive management to restrict certain applications by requiring a profile to be installed on the user's devices. The profile ensures that corporate applications and data can be removed if required. You can also choose to require public applications to be managed or used independently by manually downloading them from the app store.

The Getting Started wizard can alert you if existing potentially conflicting configurations are already enabled in AirWatch or the VMware Identity Manager services. If this occurs, or the getting started wizard only partially completes the steps, features can be configured manually. Use this guide to configure the AirWatch and VMware Identity Manager services manually for Workspace ONE.

# Integrating AirWatch With VMware Identity Manager

## 2

To set up AirWatch mobile management services for devices with VMware Identity Manager services for single sign-on and identity management for users, you must integrate the services.

When AirWatch and VMware Identity Manager are integrated, users from AirWatch enrolled devices can log in to Workspace ONE to access their enabled applications securely without entering multiple passwords.

The Workspace ONE Getting Started wizard can guide you through many of the configuration steps to integrate AirWatch and VMware Identity Manager. See the VMware Workspace ONE Quick Configuration Guide to run the Workspace ONE wizards.

This chapter includes the following topics:

- [Set Up Integration from AirWatch Admin Console](#)
- [Setting up an AirWatch Instance in VMware Identity Manager](#)
- [Enable Workspace ONE Catalog for AirWatch](#)
- [Enabling Compliance Checking for AirWatch Managed Devices](#)
- [Enable User Password Authentication through AirWatch](#)
- [Configure Access Policy Rule](#)
- [Updating VMware Identity Manager After Upgrading AirWatch](#)
- [Implementing Authentication with AirWatch Cloud Connector](#)

## Set Up Integration from AirWatch Admin Console

To integrate with VMware Identity Manager services, configure these settings in the AirWatch admin console.

- Rest API admin key for communication with the VMware Identity Manager service
- REST enrolled user API key for AirWatch Cloud Connector password authentication created in the same organization group where VMware Identity Manager is configured.
- API Admin account for VMware Identity Manager and the admin auth certificate that is exported from AirWatch and added to the AirWatch settings in the VMware Identity Manager admin console.

## 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.

System > Advanced > API > REST API

General Authentication Advanced

Current Setting ☐ Inherit ☒ Override

Enable API Access Enabled Disabled ⓘ

+Add

Service	Account Type	API Key	Description
AirWatchAPI	Admin	130HA4AAAAG5A7AADQA	
UserAPI	Enrollment User	DrhD17luOMyah1Rya5qkcTfEs+ZV8NTd ujoEvdDyVyl=	

- 6 Click **Save**.

## Export VMware AirWatch Administrator Root Certificate

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 text boxes.

The screenshot shows the 'Add / Edit Admin' form with the following fields and values:

- User Type:** Basic (selected), Directory
- Username \*:** Identity Manager
- Password \*:** [Masked with dots], Change button
- Require password change at next login:** Disabled (selected), Enabled
- First Name \*:** Identity
- Middle Name:** [Empty]
- Last Name \*:** Manager
- Email Address \*:** mgr@example.com
- Time Zone \*:** (GMT-08:00) Pacific Time (US & Canada)
- Locale \*:** English (United States) [English (United States)]
- Initial Landing Page \*:** Dashboard - ~/Device/Dashboard

Buttons at the bottom: Save, Cancel.

- 4 Select the Roles tab and choose the current organization group and click the second text box and select **AirWatch Administrator**.
- 5 Select the API tab and in the Authentication text box, 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 text box, click **Export Client Certificate** and save the file.

The screenshot shows the 'Add / Edit Admin' interface with the 'API' tab selected. Under the 'Authentication' section, a dropdown menu is set to 'Certificates'. Below this, there are fields for 'Issued by' (CN=AW Admin User Root), 'Valid From' (1/18/2016 11:25:47 AM), 'Valid To' (1/13/2036 11:25:47 AM), and 'Thumbprint' (05C2B75711A0441047D766D4644C2B421471B004). There is a 'Clear Client Certificate' button and a 'Certificate Password' field with a red asterisk. The 'Export Client Certificate' button is highlighted with an orange box.

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.

## Setting up an AirWatch Instance in VMware Identity Manager

After you configure the settings in the AirWatch admin console, in the VMware Identity Manager admin console Identity & Access Management page, you enter the AirWatch URL; the API key values, and the certificate. After AirWatch settings are configured, you can enable feature options available for Workspace ONE.

## Add AirWatch Settings in VMware Identity Manager Admin Console

Configure the AirWatch settings in the VMware Identity Manager admin console to integrate AirWatch with VMware Identity Manager.

You can link domains configured in VMware Identity Manager to specific organization groups in AirWatch to facilitate device registration in AirWatch. See Mapping VMware Identity Manager Domains to Multiple Organization Groups.

### 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 set up 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
<b>AirWatch API URL</b>	Enter the AirWatch API URL. For example <b>https://api91.example.com</b>
<b>AirWatch API Certificate</b>	Upload the certificate file used to make API calls.
<b>Certificate Password</b>	Enter the certificate password.
<b>AirWatch Admin API Key</b>	Enter the admin API key value. Example of an API key value FPseqCSataGcnJf8/Rvahzn/4jwkZENGkZzyc+jveeYs=
<b>AirWatch Enrolled User API Key</b>	Enter the enrolled user API key value.
<b>AirWatch Group ID.</b>	Enter the AirWatch group ID for the organization group that the API key and admin account were created in.

- 3 To map domains to multiple organization groups, select the **Map Domains to Multiple Organization Groups** check box.
  - a Select the domain to map from the drop-down menu and enter the organization group ID and the admin API key for that group in the text boxes.
  - b Click **+** to map additional organization groups to the domain.
  - c To map another domain, click **+** next to the drop-down menu.

#### 4 Click **Save**.

**AirWatch Configuration**

Configure AirWatch settings to integrate AirWatch with VMware Identity Manager. After you configure the settings click Save. You can then enable other feature options with AirWatch.

AirWatch API URL\*

Enter the AirWatch API URL.

AirWatch API Certificate\*

Upload Certificate

Upload the AirWatch .p12 certificate used for API calls.

Certificate Password\*

Enter the certificate password.

API Key\*

Enter the AirWatch admin API key copied from the AirWatch console.

AirWatch Enrolled User API Key\*

Enter the AirWatch enrolled user API key copied from the AirWatch console.

AirWatch Group ID\*

Enter the AirWatch Organization Group ID for this integration.

Map Domains to Multiple Organization Groups
☒

Map AirWatch Organization Groups (OG) to the user's domain in identity manager to register the user's device to the OG.

Select a Domain

+

×

Organization Group	API Key	<div>+</div>	<div>×</div>
Organization Group	API Key	<div>+</div>	<div>×</div>

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.

## Mapping VMware Identity Manager Domains to Multiple Organization Groups in AirWatch

When setting up users and devices in AirWatch, AirWatch uses organization groups (OG) to organize and group users and to establish permissions. When AirWatch is integrated with VMware Identity Manager, the admin and enrollment user REST API keys can only be configured at the AirWatch organization group of type Customer.

In AirWatch environments configured for multi-tenancy, many organization groups are created for users and devices. Devices become registered or enrolled into an organization group. Organization groups can be set up in unique configurations in a multi-tenancy environment. For example, organization groups by separate geographies, departments, or use cases.

You can link domains configured in VMware Identity Manager to specific organization groups in AirWatch to manage device registration through Workspace ONE. When users log in to Workspace ONE, a device registration event is triggered within VMware Identity Manager. During the device registration, a request is sent to AirWatch to pull any applications that the user and device combination is entitled to.

The device organization groups must be identified when AirWatch is integrated with VMware Identity Manager so that identity manager can locate the user and successfully register the device into the appropriate organization group.

When you configure the AirWatch settings in the VMware Identity Manager service, you can enter device organization group IDs and the API keys to map multiple OG to a domain. When users sign in to Workspace ONE from their devices, the user records are verified and the device is registered to the appropriate organization group in AirWatch.

To learn more about how to configure multiple organization groups, see [Deployment Strategies for Setting Up Multiple AirWatch Organization Groups](#).

---

**Note** When AirWatch is integrated with VMware Identity Manager and multiple AirWatch organization groups are configured, the Active Directory Global Catalog option cannot be configured for use with the VMware Identity Manager service.

---

## Enable Workspace ONE Catalog for AirWatch

When you configure VMware Identity Manager with your AirWatch instance, you can enable the Workspace ONE catalog. End users see all applications that they are entitled to from their Workspace ONE portal.

### 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.

## Enabling Compliance Checking for AirWatch Managed Devices

When users enroll their devices, 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.



The VMware Identity Manager service 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 Workspace ONE 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 unenrolls 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 website.

## Enable User Password Authentication through AirWatch

To implement authentication with the AirWatch Cloud Connector, you must enable the Password Authentication through AirWatch feature.

### Prerequisites

- AirWatch configured in VMware Identity Manager.
- AirWatch Cloud Connector installed and activated.
- AirWatch directory services integrated with Active Directory.

### Procedure

- 1 In the administration console, Identity & Access Management tab, click **Setup > AirWatch**
- 2 In the User Password Authentication through AirWatch section, select **Enable**.
- 3 Click **Save**.

### What to do next

See [Implementing Authentication with AirWatch Cloud Connector](#) to use AirWatch Cloud Connector authentication.

## Configure Access Policy Rule

To provide secure access to the users' Workspace ONE portal and to launch Web and desktop applications, you configure access policies. Access policies include rules that specify criteria that must be met to sign in and to use their resources.

You must edit the default policy rules to select the authentication methods you configured. A policy rule can be configured to authenticate users based on conditions such as network, device type, AirWatch device enrollment and compliant status, or application being accessed. A policy rule can also be configured to deny access to users by network range and device type. You can add groups to a policy to manage authentication for specific groups.

When Compliance Check is enabled, you create an access policy rule that requires authentication and device compliance verification for devices managed by AirWatch.

The compliance checking policy rule works in an authentication chain with Mobile SSO for iOS, Mobile SSO for Android, and Certificate cloud deployment. The authentication method to use must precede the device compliance option in the policy rule configuration.

### Prerequisites

Authentication methods configured and associated to a built-in identity provider.

Compliance checking enabled in the VMware Identity Manager AirWatch page.

### Procedure

- 1 In the administration console Identity & Access Management tab, select **Manage > Policies**.
- 2 Click **Edit Default Policy**.
- 3 Click **Next**.
- 4 Click **Add Policy Rule** to add a rule, or select a rule to edit.

The Add a Policy Rule page appears.

- a Select the network range to apply to this rule.
- b In the **and user accessing content from** drop-down menu, select the mobile device type.
- c In the **then the user may authenticate using** drop-down menu, select the authentication method to use.
- d Click **+** to select **Device Compliance (with AirWatch)**
- e Click **Save**.

## 5 Click **Save**.

The screenshot shows the 'Add Policy Rule' configuration window. It has a left sidebar with a '< Configuration' link. The main area contains the following configuration:

- Conditions:**
  - \* If a user's network range is: All Ranges (dropdown)
  - \* and user accessing content from: IOS (dropdown)
  - and user belongs to group(s): Q Select Groups... (search box)
  - Rule applies to all users if no group(s) selected.
- Actions:**
  - Then perform this action: Authenticate using... (dropdown)
  - \* then the user may authenticate using: Mobile SSO (for IOS) (dropdown)
  - and: Device Compliance (with AirWatch) (dropdown)
  - If the preceding method fails or is not applicable, then: Select fallback method... (dropdown)
  - + Add fallback method (button)
  - \* Re-authenticate after: 8 (input) Hours (dropdown)

At the bottom right, there are 'Cancel' and 'Save' buttons.

## Updating VMware Identity Manager After Upgrading AirWatch

When you upgrade AirWatch to a new version, you must update the Unified Catalog and User Password Authentication options the AirWatch configuration page in the VMware Identity Manager admin console.

When you save these options after you upgrade AirWatch, the AirWatch settings in the VMware Identity Manager service are updated with the new version of AirWatch.

### Procedure

- 1 After you upgrade AirWatch, sign in to the VMware Identity Manager admin console.
- 2 In the Identity & Access Management tab, click **Setup > AirWatch**.
- 3 Scroll down the page to the **Unified Catalog** section and click **Save**.
- 4 Scroll down to the **User Password Authentication through AirWatch** section and click **Save**.

The AirWatch configuration is updated with the new version in the VMware Identity Manager service.

## Implementing Authentication with AirWatch Cloud Connector

The AirWatch Cloud Connector (ACC) component of VMware Enterprise Systems Connector is integrated with VMware Identity Manager for user password authentication in Workspace ONE.

---

**Note** You install ACC and configure the ACC component in AirWatch. See the VMware Enterprise Systems Connector Installation and Configuration guide for information about installing and configuring the AirWatch Cloud Connector. After the ACC is installed and configured, you integrate the AirWatch directory services with Active Directory. See the VMware AirWatch Directory Services Guide for information about enabling the directory services.

---

To implement AirWatch Cloud Connector authentication for Workspace ONE, in the VMware Identity Manager admin console, the Password (AirWatch Connector) authentication method is associated to a built-in identity provider.

You can enable just-in-time support in AirWatch to add new users to the VMware Identity Manager directory when users sign in for the first time. When just-in-time support is enabled, users do not need to wait for the next scheduled sync from the AirWatch server to access Workspace ONE. Instead, new users sign in to their Workspace ONE portal, either from an iOS or Android device or from their desktop computer and enter their Active Directory user name and password. The VMware Identity Manager service authenticates the Active Directory credentials through the AirWatch Cloud Connector and adds the user profile to the directory.

After you associate the authentication methods in the built-in identity provider, you create access policies to apply to this authentication method.

---

**Note** User name and password authentication are integrated into the AirWatch Cloud Connector deployment. To authenticate users using other VMware Identity Manager -supported authentication methods, the VMware Identity Manager connector must be configured.

---

## Managing User Attributes Mapping

You can configure the user attribute mapping between the AirWatch directory and the VMware Identity Manager directory.

The User Attributes page in the VMware Identity Manager, Identity & Access Management tab lists the default directory attributes that are mapped to AirWatch Directory attributes. Attributes that are required are marked with an asterisk. Users missing a required attribute in their profile are not synced to the VMware Identity Manager service.

**Table 2-1. Default AirWatch Directory Attributes Mapping**

VMware Identity Manager User Attribute Name	Default Mapping to AirWatch User Attribute
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName

**Table 2-1. Default AirWatch Directory Attributes Mapping (Continued)**

VMware Identity Manager User Attribute Name	Default Mapping to AirWatch User Attribute
employeeID	employeeID
domain	Domain
disabled (external user disabled)	disabled
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Email*
userName	username*

## Sync Users and Groups from AirWatch Directory to VMware Identity Directory

You configure the VMware Identity Manager settings in the AirWatch admin console to establish a connection between your organization group instance of the AirWatch Directory and VMware Identity Manager. This connection is used to sync users and groups to a directory created in the VMware Identity Manager service.

Users and groups initially sync to the VMware Identity Manager directory manually. The AirWatch sync schedule determines when users and groups sync with the VMware Identity Manager directory.

When a user or a group is added or deleted on the AirWatch server, the change is reflected on the VMware Identity Manager service immediately.

### Prerequisites

- VMware Identity Manager local admin name and password.
- Identify attribute values to map from the AirWatch directory. See [Managing User Attributes Mapping](#).

### Procedure

- 1 In the AirWatch admin console, Groups & Settings, All Settings page, select the Global > Customer-level organization group and navigate to **System > Enterprise Integration > VMware Identity Manager**.
- 2 In the Server section, click **Configure**.

**Note** The configuration button is only available when the Directory Service is also configured for the same organization group. If the Configure button is not visible, you are not in the correct organization group. You can change the organization group in the Global drop-down menu.

### 3 Enter the VMware Identity Manager settings.

Option	Description
URL	Enter your tenant VMware URL. For example, <code>https://myco.identitymanager.com</code> .
Admin Username	Enter the VMware Identity Manager local admin user name.
Admin Password	Enter the VMware Identity Manager local admin user's password.

### 4 Click **Next**.

### 5 Enable custom mapping to configure the user attributes mapping from AirWatch to the VMware Identity Manager service.

### 6 Click **Test Connection** to verify that the settings are correct.

### 7 Click **Sync Now** to manually sync all users and groups to VMware Identity Manager service.

---

**Note** To control the system load, manual sync can only be performed four hours after a previous sync.

---

An AirWatch directory is created in the VMware Identity Manager service and the users and groups are synced to a directory in VMware Identity Manager.

#### What to do next

Review the Users and Groups tab in the VMware Identity Manager admin console to verify that the user and group names are synced.

## Managing Configuration of Password Authentication to AirWatch

You can review and manage the Password (AirWatch Connector) configuration that was set up when you installed AirWatch and added the VMware Identity Manager service.

The Password (AirWatch Connector) authentication method is managed from the Identity & Access Management > Authentication Methods page and is associated to the built-in identity provider in the Identity Providers page.

---

**Important** When the AirWatch Cloud Connector software is upgraded, make sure that you update the VMware Identity Manager AirWatch configuration in the VMware Identity Manager admin console AirWatch page.

---

#### Procedure

- 1 To review and manage the configuration, in the Identity & Access Management tab, select **Authentication Methods**.
- 2 In the **Password (AirWatch Connector)** Configure column, click the pencil icon.

### 3 Review the configuration.

Option	Description
<b>Enable AirWatch Password Authentication</b>	This check box enables AirWatch password authentication.
<b>AirWatch Admin Console URL</b>	Pre-populated with the AirWatch URL.
<b>AirWatch API Key</b>	Pre-populated with the AirWatch Admin API key.
<b>Certificate Used for Authentication</b>	Pre-populated with the AirWatch Cloud Connector certificate.
<b>Password for Certificate</b>	Pre-populated with the password for the AirWatch Cloud Connector certificate.
<b>AirWatch Group ID</b>	Pre-populated with the organization group ID.
<b>Number of authentication attempts allowed</b>	The maximum number of failed login attempts when using AirWatch password authentication. No more log ins are allowed after the failed login attempts reach this number. The VMware Identity Manager service tries to use the fallback authentication method if it is configured. The default is five attempts.
<b>JIT Enabled</b>	If JIT is not enabled, select this check box to enable just-in-time provisioning of users in the VMware Identity Manager service dynamically when they log in the first time.

### 4 Click **Save**.

## Configure Built-in Identity Providers

You can configure multiple built-in identity providers and associate authentication methods that have been configured in the Identity & Access Management Manage > Auth Methods page.

### Procedure

- 1 In the Identity & Access Management tab, go to **Manage > Identity Providers**.
- 2 Click **Add Identity Provider**, and select **Create Built-in IDP**.

Option	Description
<b>Identity Provider Name</b>	Enter the name for this built-in identity provider instance.
<b>Users</b>	Select which users to authentication. The configured directories are listed.
<b>Network</b>	The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication.
<b>Authentication Methods</b>	<p>The authentication methods that are configured on the service are displayed. Select the check box for the authentication methods to associate to this built-in identity provider.</p> <p>For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page.</p>

### 3 Click **Add**.

### What to do next

Configure the default access policy rule to add the authentication policy to the rule. See [Configure Access Policy Rule](#)

# Implementing Mobile Single Sign-in Authentication for AirWatch -Managed iOS Devices

## 3

For iOS device authentication, VMware Identity Manager uses an identity provider that is built in to the VMware Identity Manager service to provide access to mobile SSO authentication.

This authentication method for iOS devices uses a Key Distribution Center (KDC) without the use of a connector or a third-party system. Kerberos authentication provides users, who are successfully signed in to their domain, access to their Workspace ONE apps portal without additional credential prompts.

This chapter includes the following topics:

- [Implementation Overview to Configure Mobile SSO for iOS](#)
- [Configure Active Directory Certificate Authority in AirWatch](#)
- [Using AirWatch Certificate Authority for Kerberos Authentication](#)
- [Using a Key Distribution Center for Authentication from iOS Devices](#)
- [Configure Mobile SSO for iOS Authentication](#)
- [Configure Built-in Identity Provider for Mobile SSO iOS Authentication](#)
- [Configure Apple iOS Profile in AirWatch Using Active Directory Certificate Authority and Certificate Template](#)
- [Configure Apple iOS Profile in AirWatch Using AirWatch Certificate Authority](#)
- [Assign an AirWatch Device Profile](#)

## Implementation Overview to Configure Mobile SSO for iOS

Implementing Mobile SSO authentication for AirWatch-managed iOS 9 or later devices requires the following configuration steps.

- Download the issuer certificate to configure Mobile SSO for iOS
  - If you are using Active Directory Certificate Services, configure a certificate authority template for Kerberos certificate distribution in the Active Directory Certificate Services. Then configure AirWatch to use Active Directory Certificate Authority. Add the Certificate template in the AirWatch admin console. Download the issuer certificate to configure Mobile SSO for iOS.



- If you are using AirWatch Certificate Authority, enable Certificates in the VMware Identity Manager Integrations page. Download the issuer certificate to configure Mobile SSO for iOS.
- Establish the Key Distribution Center (KDC) to use.
- Configure the iOS device profile and enable single sign-in from the AirWatch admin console.
- Configure the Mobile SSO (iOS) authentication method
- Configure the built-in identity provider and associate the Mobile SSO for iOS authentication in the VMware Identity Manager administration console.

## Configure Active Directory Certificate Authority in AirWatch

To set up single sign-on authentication to AirWatch managed iOS 9 mobile devices, you can set up a trust relationship between Active Directory and AirWatch and enable the Mobile SSO for iOS authentication method in VMware Identity Manager.

After you configured the certificate authority and certificate template for Kerberos certificate distribution in the Active Directory Certificate Services, you enable AirWatch to request the certificate used for authentication and add the certificate authority to the AirWatch admin console.

### Procedure

- 1 In the AirWatch admin console main menu, navigate to **Devices > Certificates > Certificate Authorities**.
- 2 Click **Add**.
- 3 Configure the following in the Certificate Authority page.

**Note** Make sure that Microsoft AD CS is selected as the Authority Type before you start to complete this form.

Option	Description
<b>Name</b>	Enter a name for the new Certificate Authority.
<b>Authority Type</b>	Make sure that <b>Microsoft AD CS</b> is selected.
<b>Protocol</b>	Select <b>AD CS</b> as the protocol.
<b>Server Hostname</b>	<p>Enter the URL of the server. Enter the hostname in this format <code>https://{servername.com}/certsrv.adcs/</code>. The site can be http or https depending on how the site is set up. The URL must include the trailing <code>/</code>.</p> <p><b>Note</b> If the connection fails when you test the URL, remove the <code>http://</code> or <code>https://</code> from the address and test the connection again.</p>
<b>Authority Name</b>	Enter the name of the certificate authority that the AD CS end point is connected to. This name can be found by launching the Certification Authority application on the certificate authority server.

Option	Description
<b>Authentication</b>	Make sure that <b>Service Account</b> is selected.
<b>Username and Password</b>	Enter the user name and password of the AD CS admin account with sufficient access to allow AirWatch to request and issue certificates.

4 Click **Save**.

#### What to do next

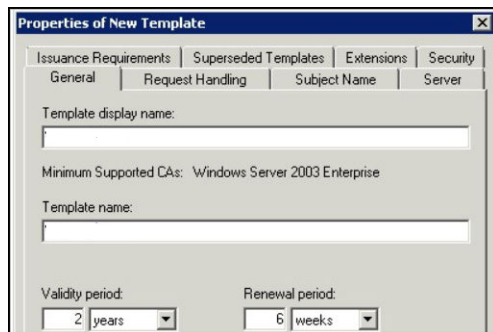
Configure the Certificate Template in AirWatch.

## Configuring AirWatch to use Active Directory Certificate Authority

Your certificate authority template must be properly configured for Kerberos certificate distribution. In the Active Directory Certificate Services (AD CS), you can duplicate the existing Kerberos Authentication template to configure a new certificate authority template for the iOS Kerberos authentication.

When you duplicate the Kerberos Authentication template from AD CS, you must configure the following information in the Properties of New Template dialog box.

**Figure 3-1. Active Directory Certificate Services Properties of New Template Dialog Box**



- **General** tab. Enter the Template display name and the Template name. For example iOSKerberos. This is the display name that is shown in the Certificate Templates snap-in, Certificates snap-in, and Certification Authority snap-in.
- **Request Handling** tab. Enable **Allow private key to be exported**.
- **Subject Name** tab. Select **Supply in the request** radio button. The subject name is supplied by AirWatch when AirWatch requests the certificate.
- **Extensions** tab. Define the application policies.
  - Select Applications Policies and click Edit to add a new application policy. Name this policy Kerberos Client Authentication.
  - Add the object identifier (OID) as follows: 1.3.6.1.5.2.3.4. Do not change.
  - In the Description of Application Policies list delete all policies listed except for the Kerberos Client Authentication policy and the Smart Card Authentication policy.

- **Security** tab. Add the AirWatch account to the list of users that can use the certificate. Set the permissions for the account. Set Full Control to allow the security principal to modify all attributes of a certificate template, including the permissions for the certificate template. Otherwise, set the permissions according to your organization's requirements.

Save the changes. Add the template to the list of templates used by the Active Directory Certificate Authority.

In AirWatch configure the Certificate Authority and add the Certificate Template.

## Add Certificate Template in AirWatch

You add the certificate template that associates the certificate authority used to generate the user's certificate.

### Prerequisites

Configure the Certificate Authority in AirWatch.

### Procedure

- 1 In the AirWatch admin console, navigate to **System > Enterprise Integration > Certificate Authorities**.
- 2 Select the **Request Template** tab and click **Add**.
- 3 Configure the following in the certificate template page.

Option	Description
<b>Name</b>	Enter the name for the new request template in AirWatch.
<b>Certificate Authority</b>	In the drop-down menu, select the certificate authority that was created.
<b>Issuing Template</b>	Enter the Microsoft CA certificate template name exactly as you created in AD CS. For example, <b>iOSKerberos</b> .
<b>Subject Name</b>	After <b>CN=</b> , enter <b>{EnrollmentUser}</b> , where the {} text box is the AirWatch lookup value. The text entered here is the Subject of the certificate, which can be used to determine who received the certificate.
<b>Private Key Length</b>	This private key length matches the setting on the certificate template that is being used by AD CS. It is usually 2048.
<b>Private Key Type</b>	Select the check box for <b>Signing and Encryption</b> .
<b>San Type</b>	For the Subject Alternate Name, select <b>User Principal Name</b> . The value must be <b>{EnrollmentUser}</b> . If device compliance check is configured with Kerberos authentication, you must set a second SAN type to include the UDID. Select the San type <b>DNS</b> . The value must be <b>UDID={DeviceUid}</b> .
<b>Automatic Certificate Renewal</b>	Select the check box to have certificates using this template automatically renewed before their expiration date.
<b>Auto Renewal Period (days)</b>	Specify the auto renewal in days.
<b>Enable Certificate Revocation</b>	Select the check box to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.

Option	Description
<b>Publish Private Key</b>	Select this check box to publish the private key.
<b>Private Key Destination</b>	Either Directory Service or Custom Web Service

#### 4 Click **Save**.

**Certificate Template - Add / Edit**

Name\* withDeviceUDID

Description

Certificate Authority\* HSO\_CA

Issuing Template certificatetemplate:CloudKDC

Subject Name\* CN={EnrollmentUser}

Private Key Length\* 2048

Private Key Type\* Signing ☒ Encryption ☒

San Type

User Principal Name {EnrollmentUser}

DNS Name UDID={DeviceUid}

Automatic Certificate Renewal ☒

Auto Renewal Period (days)\* 5

Enable Certificate Revocation ☐

Publish Private Key ☐

ECU Attributes Add

Force Key Generation On Device ☐

Save Save and Add Another Template Cancel

#### What to do next

In the Identity Provider admin console, configure the built-in identity provider with the Mobile SSO for iOS authentication method.

## Using AirWatch Certificate Authority for Kerberos Authentication

You can use the AirWatch Certificate Authority instead of the Active Directory Certificate Authority to set up single sign-on with built-in Kerberos authentication to AirWatch managed iOS 9 mobile devices. You can enable AirWatch Certificate Authority in the AirWatch admin console and export the CA issuer certificate for use in the VMware Identity Manager service.

The AirWatch Certificate Authority is designed to follow Simple Certificate Enrollment Protocol (SCEP) and is used with AirWatch managed devices that support SCEP. VMware Identity Manager integration with AirWatch uses the AirWatch Certificate Authority to issue certificates to iOS 9 mobile devices as part of the profile.

The AirWatch Certificate Authority issuer root certificate is also the OCSP signing certificate.

## Enable and Export the AirWatch Certificate Authority

When VMware Identity Manager is enabled in AirWatch, you can generate the AirWatch issuer root certificate and export the certificate for use with the Mobile SSO for iOS authentication on managed iOS 9 mobile devices.

### Procedure

- 1 In the AirWatch admin console, navigate to **System > Enterprise Integration > VMware Identity Manager**.
- 2 To enable AirWatch Certificate Authority, the organization group type must be Customer.



**Tip** To view or change the group type, navigate to Groups & Settings, **Groups > Organization Groups > Organization Group Details**.

- 3 In the CERTIFICATE section, click **Enable**.  
The page displays the issuer root certificate details.
- 4 Click **Export** and save the file.

### What to do next

In the VMware Identity Manager admin console, configure Kerberos Authentication in the built-in identity provider and add the certificate authority issuer certificate.

## Using a Key Distribution Center for Authentication from iOS Devices

For iOS device, you integrate the service with Kerberos. Kerberos authentication provides users, who are successfully signed in to their domain, access to their application portal without additional credential prompts. This authentication method for iOS devices uses a Key Distribution Center (KDC) without the use of a connector or a third-party system.

VMware Identity Manager Cloud tenants do not need to manage or configure the KDC.

For on premises deployments, two KDC service options are available.

- Built-in KDC. The built-in KDC requires initializing KDC on the appliance and creating public DNS entries to allow the Kerberos clients to find the KDC. For more information about enabling the built-in KDC, see the VMware Identity Manager Administration guide.
- KDC as a VMware Identity Manager cloud hosted service. Using KDC in the cloud requires selecting the appropriate realm name in the iOS authentication adapter page.

**Note** When the VMware Identity Manager is installed and configured with AirWatch in a Windows environment, the iOS Mobile authentication method must be configured to use the VMware Identity Manager cloud hosted KDC service.

## Using the Cloud Hosted KDC Service

To support using Kerberos authentication for Mobile SSO for iOS, VMware Identity Manager provides a cloud hosted KDC service.

The KDC service hosted in the cloud must be used when the VMware Identity Manager service is deployed with AirWatch in a Windows environment.

To use the KDC managed in the VMware Identity Manager appliance, see the Preparing to Use Kerberos Authentication on iOS devices in the VMware Identity Manager Installation and Configuration Guide.

When you configure Mobile SSO for iOS authentication, you configure the realm name for the cloud hosted KDC service. The realm is the name of the administrative entity that maintains authentication data. When you click Save, the VMware Identity Manager service is registered with the cloud hosted KDC service. The data that is stored in the KDC service is based on your configuration of the Mobile SSO for iOS authentication method, which includes the CA certificate, the OCSP signing certificate, and the OCSP request configuration details. No other user-specific information is stored in the cloud service.

The logging records are stored in the cloud service. The Personally Identifiable Information (PII) in the logging records include the Kerberos principal name from the user's profile, the subject DN and UPN and EMAIL SAN values, the device ID from the user's certificate, and the FQDN of the IDM service that the user is accessing.

To use the cloud hosted KDC service, VMware Identity Manager must be configured as follows.

- The FQDN of the VMware Identity Manager service must be reachable from the Internet. The SSL/TLS certificate used by VMware Identity Manager must be publicly signed.
- An outbound request/response port 88 (UDP) and port 443 (HTTPS/TCP) must be accessible from the VMware Identity Manager service.
- If you enable OCSP, the OCSP responder must be reachable from the Internet.

## Configure Mobile SSO for iOS Authentication

You configure the Mobile SSO for iOS authentication method from the Auth Methods page in the administration console. Select the Mobile SSO (for iOS) authentication method to use in the built-in identity provider.

### Prerequisites

- Certificate authority PEM or DER file used to issue certificates to users in the AirWatch tenant.
- For revocation checking, the OCSP responder's signing certificate.
- For the KDC service select, the realm name of the KDC service. If using the built-in KDC service, the KDC should be initialized. See the Installing and Configuring VMware Identity Manager for the built-in KDC details.

### Procedure

- 1 In the Identity & Access Management tab, go to **Manage > Auth Methods**.

- 2 In the **Mobile SSO (for iOS)** Configure column, click the icon.
- 3 Configure the Kerberos authentication method.

Option	Description
<b>Enable KDC Authentication</b>	Select this check box to enable users to sign in using iOS devices that support Kerberos authentication.
<b>Realm</b>	<p>If you are using the cloud hosted KDC, enter the pre-defined supported realm name that is supplied to you. The text in this parameter must be entered in all caps. For example, OP.VMWAREIDENTITY.COM</p> <p>If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays.</p> <p>The realm value is read-only. The realm entered here is the identity manager realm name for your tenant.</p>
<b>Root and Intermediate CA Certificate</b>	Upload the certificate authority issuer certificate file. The file format can be either PEM or DER.
<b>Uploaded CA Certificate Subject DNs</b>	The content of the uploaded certificate file is displayed here. More than one file can be uploaded and whatever certificates that are included are added to the list.
<b>Enable OCSP</b>	Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
<b>Send OCSP Nonce</b>	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
<b>OCSP Responder's Signing Certificate</b>	<p>Upload the OCSP certificate for the responder.</p> <p>When you are using the AirWatch Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the AirWatch certificate here as well.</p>
<b>OCSP Responder's Signing Certificate Subject DN</b>	The uploaded OCSP certificate file is listed here.
<b>Cancel Message</b>	Create a custom sign-in message that displays when authentication is taking too long. If you do not create a custom message, the default message is <code>Attempting to authenticate your credentials.</code>
<b>Enable Cancel Link</b>	<p>When authentication is taking too long, give users the ability to click Cancel to stop the authentication attempt and cancel the sign-in.</p> <p>When the Cancel link is enabled. Cancel appears at the end of the authentication error message that displays.</p>
<b>Enterprise Device Management Server URL</b>	Enter the Mobile Device Management (MDM) server URL to redirect users when access is denied because the device is not enrolled into AirWatch for MDM management. This URL displays in the auth failure error message. If you do not enter a URL here, the generic Access Denied message displays.

- 4 Click **Save**.

#### What to do next

- Associate the Mobile SSO (for iOS) authentication method in the built-in identity provider.
- Configure the default access policy rule for Kerberos authentication for iOS devices. Make sure that this authentication method is the first method set up in the rule.
- Go to the AirWatch admin console and configure the iOS device profile in AirWatch and add the KDC server certificate issuer certificate from VMware Identity Manager.

## Configure Built-in Identity Provider for Mobile SSO iOS Authentication

You configure the built-in identity provider and associate the Mobile SSO for iOS authentication method that has been configured in the Identity & Access Management **Manage > Auth Methods** page.

### Prerequisites

Mobile SSO (for iOS) authentication configured in the Authentication Methods page.

### Procedure

- 1 In the Identity & Access Management tab, go to **Manage > Identity Providers**.
- 2 Click **Add Identity Provider**, and select **Create Built-in IDP**.

Option	Description
<b>Identity Provider Name</b>	Enter the name for this built-in identity provider instance.
<b>Users</b>	Select which users to authentication. The configured directories are listed.
<b>Network</b>	The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication.
<b>Authentication Methods</b>	<p>The authentication methods that are configured on the service are displayed. Select the check box for the iOS authentication method to associate to this built-in identity provider. Add any other authentication methods.</p> <p>For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page.</p>

- 3 In the KDC Certificate Export section, click **Download Certificate**. Save this certificate to a file that can be access from the AirWatch admin console.

You upload this certificate when you configure the iOS device profile in AirWatch.

- 4 Click **Add**.

### What to do next

- Configure the default access policy rule for Kerberos authentication for iOS devices. Make sure that this authentication method is the first method set up in the rule.
- Go to the AirWatch admin console and configure the iOS device profile in AirWatch and add the KDC server certificate issuer certificate from VMware Identity Manager.

## Configure Apple iOS Profile in AirWatch Using Active Directory Certificate Authority and Certificate Template

Create and deploy the Apple iOS device profile in AirWatch to push the Identity Provider settings to the device. This profile contains the information necessary for the device to connect to the VMware Identity Provider and the certificate that the device used to authenticate. Enable single sign-on to allow seamless access without requiring authentication into each app.



## Prerequisites

- Mobile SSO for iOS is configured in VMware Identity Manager.
- iOS Kerberos certificate authority file saved to a computer that can be accessed from the AirWatch admin console.
- Your Certificate Authority and Certificate Template is properly configured in AirWatch.
- List of URLs and application bundle IDs that use Mobile SSO for iOS authentication on iOS devices.

## Procedure

- 1 In the AirWatch admin console, navigate to **Devices > Profiles & Resources > Profiles**.
- 2 Select **Add > Add Profile** and select **Apple iOS**.
- 3 Enter the name as **iOSKerberos** and configure the **General** settings.
- 4 In the left navigation pane, select **Credentials > Configure** to configure the credential.

Option	Description
<b>Credential Source</b>	Select <b>Defined Certificate Authority</b> from the drop-down menu.
<b>Certificate Authority</b>	Select the certificate authority from the list in the drop-down menu.
<b>Certificate Template</b>	Select the request template that references the certificate authority from the drop-down menu. This is the certificate template created in Adding the Certificate Template in AirWatch.

- 5 Click **+** in the lower right corner of the page again and create a second credential.
- 6 In the **Credential Source** drop-down menu, select **Upload**.
- 7 Enter a credential name.
- 8 Click **Upload** to upload the KDC server root certificate that is downloaded from the Identity & Access Management > Manage > Identity Providers > Built-in Identity provider page.
- 9 In the left navigation pane, select **Single Sign-On** and click **Configure**.
- 10 Enter the connection information.

Option	Description
<b>Account Name</b>	Enter <b>Kerberos</b> .
<b>Kerberos Principal Name</b>	Click <b>+</b> and select <b>{EnrollmentUser}</b> .
<b>Realm</b>	Enter the Identity Manager realm name for your tenant. The text in this parameter must be capitalized. Realm name choices are <b>VMWAREIDENTITY.COM</b> , <b>VMWAREIDENTITY.EU</b> , and <b>VMWAREIDENTITY.ASIA</b> . Enter the realm name you used when you initialized KDC in the VMware Identity Manager appliance. For example, <b>EXAMPLE.COM</b>
<b>Renewal Certificate</b>	Select <b>Certificate #1</b> from the drop-down menu. This is the Active Directory CA cert that was configured first under credentials.

Option	Description
<b>URL Prefixes</b>	<p>Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP.</p> <p>Enter the VMware Identity Manager server URL as <code>https://myco.example.com</code>.</p> <p>Enter the VMware Identity Manager server URL as <code>https://&lt;tenant&gt;.vmwareidentity.&lt;region&gt;</code>.</p>
<b>Applications</b>	<p>Enter the list of application identities that are allowed to use this sign-on. To perform single sign-on using iOS built-in Safari browser, enter the first application bundle ID as <code>com.apple.mobilesafari</code>. Continue to enter application bundle IDs. The applications listed must support SAML authentication</p>

## 11 Click **Save & Publish**.

### What to do next

Assign the device profile to a smart group. Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision.

## Configure Apple iOS Profile in AirWatch Using AirWatch Certificate Authority

Create and deploy the Apple iOS device profile in AirWatch to push the Identity Provider settings to the device. This profile contains the information necessary for the device to connect to the VMware Identity Provider and the certificate that the device uses to authenticate.

### Prerequisites

- Built-in Kerberos configured in VMware Identity Manager.
- VMware Identity Manager KDC server root certificate file saved to a computer that can be accessed from the AirWatch admin console.
- Certificate enabled and downloaded from the AirWatch admin console System > Enterprise Integration > VMware Identity Manager page.
- List of URLs and application bundle IDs that use Built-in Kerberos authentication on iOS devices.

### Procedure

- 1 In the AirWatch admin console, navigate to **Devices > Profiles & Resources > Profile > Add Profile** and select **Apple IOS**.
- 2 Configure the profile's **General** settings and enter the name of the device as **iOSKerberos**.

- 3 In the left navigation pane, select **SCEP > Configure** to configure the credential.

Option	Description
<b>Credential Source</b>	Select <b>AirWatch Certificate Authority</b> from the drop-down menu.
<b>Certificate Authority</b>	Select the <b>AirWatch Certificate Authority</b> from the drop-down menu.
<b>Certificate Template</b>	Select <b>Single Sign On</b> to set the type of certificate that is issued by the AirWatch Certificate Authority.

- 4 Click **Credentials > Configure** and create a second credential.
- 5 In the **Credential Source** drop-down menu, select **Upload**.
- 6 Enter the iOS Kerberos credential name.
- 7 Click **Upload** to upload the VMware Identity Manager KDC server root certificate that is downloaded from the Identity & Access Management > Manage > Identity Providers > Built-in Identity provider page.
- 8 In the left navigation pane, select **Single Sign-On**.
- 9 Enter the Connection information.

Option	Description
<b>Account Name</b>	Enter <b>Kerberos</b> .
<b>Kerberos Principal Name</b>	Click + and select <b>{EnrollmentUser}</b> .
<b>Realm</b>	Enter the Identity Manager realm name for your tenant. The text in this parameter must be capitalized. Realm name choices are <b>VMWAREIDENTITY.COM</b> , <b>VMWAREIDENTITY.EU</b> , and <b>VMWAREIDENTITY.ASIA</b> . Enter the realm name you used when you initialized KDC in the VMware Identity Manager appliance. For example, <b>EXAMPLE.COM</b> .
<b>Renewal Certificate</b>	On iOS 8 and later devices, select the certificate used to reauthenticate the user automatically without any need for user interaction when the user's single sign-on session expires.
<b>URL Prefixes</b>	Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. Enter the VMware Identity Manager server URL as <b>https://myco.example.com</b> . Enter the VMware Identity Manager server URL as <b>https://&lt;tenant&gt;.vmwareidentity.&lt;region&gt;</b> .
<b>Applications</b>	Enter the list of application identities that are allowed to use this sign-in. To perform single sign-on using iOS built-in Safari browser, enter the first application bundle ID as <b>com.apple.mobilesafari</b> . Continue to enter application bundle IDs. The applications listed must support SAML authentication.

- 10 Click **Save & Publish**.

When the iOS profile is successfully pushed to users' devices, users can sign in to VMware Identity Manager using the Built-in Kerberos authentication method without entering their credentials.

### What to do next

Assign the device profile to a smart group. Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision.

## Assign an AirWatch Device Profile

After you create a device profile, you assign the profile to a smart group.

Smart groups are customizable groups that determine which platforms devices, and users receive an assigned application, compliance policy, device profile, or provision. See the AirWatch Mobile Device Management Guide.

### Procedure

- 1 In the AirWatch admin console, navigate to **Devices > Profiles & ResourcesProfiles**
- 2 Select the device profile that you want to assign to the smart group.
- 3 In the General tab, click the **Assigned Groups** text box and select **Create Assignment Group**.
- 4 In the Create New Smart Group page, enter the name for the smart group.
- 5 Select **Platform and Operating System** and select the correct operating system and version from the drop down menus.
- 6 Click **Save & Publish**.

After you assign a smart group to the device option, users can sign in to Workspace ONE and access applications from the catalog.

# Implementing Mobile Single Sign-On Authentication for AirWatch -Managed Android Devices

## 4

Mobile SSO for Android is an implementation of the certificate authentication method for AirWatch-managed Android devices.

The VMware Tunnel mobile application is installed on the Android device. The VMware Tunnel client is configured to access the VMware Identity Manager service for authentication. The tunnel client uses the client certificate to establish a mutually authenticated SSL session and the VMware Identity Manager service retrieves the client certificate for authentication.

---

**Note** Mobile SSO authentication for Android is supported for Android devices 4.4 and later.

---

## Mobile Single Sign-on Without VPN Access

Mobile single sign-on authentication for Android devices can be configured to bypass the Tunnel server when VPN access is not required. Implementing Mobile SSO for Android authentication without using a VPN uses the same configuration pages as used for configuring the VMware Tunnel. Because you are not installing the Tunnel server, you do not enter the VMware Tunnel server host name and port. You still set up a profile using the VMware Tunnel profile form, but traffic is not directed to the Tunnel server. The Tunnel client is used only for single sign-on.

In the AirWatch admin console, you configure the following settings.

- Per App Tunnel component in the VMware Tunnel. This configuration allows Android devices access to internal and managed public apps through the VMware Tunnel mobile app client.
- Per App Tunnel Profile. This profile is used to enable the per app tunneling capabilities for Android.
- In the Network Traffic Rules page, because the Tunnel server is not configured, you select Bypass so that no traffic is directed towards a Tunnel server.

## Mobile Single Sign-on with VPN Access

When the application configured for single sign-on also is used to access intranet resources behind the firewall, configure VPN access and set up the Tunnel server. When single sign-on is configured with VPN, the Tunnel client can optionally route application traffic and login requests through the Tunnel server. Instead of the default configuration used for the Tunnel client in the console in the single sign-on mode, the configuration should point to the Tunnel server.

Implementing Mobile SSO for Android authentication for AirWatch managed Android devices requires configuring the VMware Tunnel in the AirWatch admin console and installing the VMware Tunnel server before you configure Mobile SSO for Android in the VMware Identity Manager administration console. The VMware Tunnel service provides per app VPN access to AirWatch managed apps. VMware Tunnel also provides the ability to proxy traffic from a mobile application to VMware Identity Manager for single sign-on.

In the AirWatch admin console, you configure the following settings.

- Per App Tunnel component in the VMware Tunnel. This configuration allows Android devices access to internal and managed public applications through the VMware Tunnel mobile app client.

After the Tunnel settings are configured in the admin console, you download the VMware Tunnel installer and proceed with the installation of the VMware Tunnel server.

- Android VPN profile. This profile is used to enable the per app tunneling capabilities for Android.
- Enable VPN for each app that uses the application tunnel functionality from the admin console.
- Create device traffic rules with a list of all the applications that are configured for per app VPN, the proxy server details, and the VMware Identity Manager URL.

For detailed information about installing and configuring the VMware Tunnel, see the VMware Tunnel Guide on the AirWatch Resources website.

This chapter includes the following topics:

- [Configure Single-Sign-on for Android Device from AirWatch Admin Console](#)
- [Configure VMware Tunnel VPN Access Settings from AirWatch Admin Console](#)
- [Configure Per App Tunnel Profile for Android](#)
- [Enable Per-App VPN for Android Apps](#)
- [Configure Traffic Rules in AirWatch](#)
- [Configure Mobile SSO for Android Authentication in the Built-in Identity Provider](#)

## Configure Single-Sign-on for Android Device from AirWatch Admin Console

Configure single sign-on for Android devices to allow users to sign in securely to enterprise apps, without entering their password.

To configure single-sign-on for Android devices, you do not need to configure the VMware Tunnel, but you configure single sign-on using many of the same fields

### Prerequisites

- Android 4.4 or later
- Applications must support SAML or another supported federation standard

## Procedure

- 1 In the AirWatch admin console, navigate to **System > Enterprise Integration > VMware Tunnel**.
- 2 The first time you configure VMware Tunnel, select **Configure** and follow the configuration wizard. Otherwise, select **Override** and select the **Enable VMware Tunnel** check box. Then click **Configure**.
- 3 In the Configuration Type page, enable **Per-App Tunnel (Linux Only)**. Click **Next**.  
Leave **Basic** as the deployment model.
- 4 In the Details page, enter a dummy value in the text box, as this field is not required for the single sign-on configuration. Click **Next**.
- 5 In the SSL page, configure the Per-App Tunneling SSL Certificate. To use a public SSL, select the **Use Public SSL Certificate** check box. Click **Next**.

The Tunnel Device Root Certificate is automatically generated.

---

**Note** SAN certificates are not supported. Make sure that your cert is issued for the corresponding server host name or is a valid wildcard certificate for the corresponding domain.

---

- 6 In the Authentication page, select the certificate authentication type to use. Click **Next**.

Option	Description
<b>Default</b>	Select Default to use the AirWatch issued certificates.
<b>Enterprise CA</b>	A drop-down menu listing the certificate authority and certificate template that you configured in AirWatch is displayed. You can also upload the root certificate of your CA.

If you select Enterprise CA, make sure that the CA template contains the subject name **CN=UDID**. You can download the CA certificates from the VMware Tunnel configuration page.

- 7 Click **Next**.
- 8 In the Profile Association page, associate an existing or create a new VMware Tunnel VPN profile for Android.  
  
If you create the profile in this step, you still must publish the profile. See [Configure Android Profile in AirWatch](#).
- 9 Review the summary of your configuration and click **Save**.  
  
You are directed to the system settings configuration page.

## Configure VMware Tunnel VPN Access Settings from AirWatch Admin Console

You enable the Per App Tunnel component in the VMware Tunnel settings to set up per app tunneling functionality for Android devices. Per app tunneling allows your internal and managed public applications to access your corporate resources on an app-by-app basis.

The VPN can automatically connect when a specified app is launched.

## Procedure

- 1 In the AirWatch admin console, navigate to **System > Enterprise Integration > VMware Tunnel**.
- 2 The first time you configure VMware Tunnel, select **Configuration** and follow the configuration wizard. Otherwise, select **Override** and select **Enable** . Then click **Configure**.
- 3 In the Configuration Type page, enable **Per-App Tunnel (Linux Only)**. Click **Next**.

Leave **Basic** as the deployment model.

- 4 In the Details page, for the Per-App Tunneling Configuration enter the VMware Tunnel server host name and port. For example, enter as `tunnel.example.com`. Click **Next**.
- 5 In the SSL page, configure the Per-App Tunneling SSL Certificate. To use a public SSL, select the **Use Public SSL Certificate** check box. Click **Next**.

The Tunnel Device Root Certificate is automatically generated.

---

**Note** SAN certificates are not supported. Make sure that your cert is issued for the corresponding server host name or is a valid wildcard certificate for the corresponding domain.

---

- 6 In the Authentication page, select the certificate authentication type to use. Click **Next**.

Option	Description
<b>Default</b>	Select Default to use the AirWatch issued certificates.
<b>Enterprise CA</b>	A drop-down menu listing the certificate authority and certificate template that you configured in AirWatch is displayed. You can also upload the root certificate of your CA.

If you select Enterprise CA, make sure that the CA template contains the subject name **CN=<udid>:<string>**. You can download the CA certificates from the VMware Tunnel configuration page.

If device compliance check is configured for Android, make sure that the CA template contains the Subject Name CN={DeviceUid} or set a SAN type to include the UDID. Select the San type DNS Name. The value must be UDID={DeviceUid}.

- 7 Click **Next**.
- 8 In the Profile Association page, associate an existing or create a new VMware Tunnel VPN profile for Android.  
  
If you create the profile in this step, you still must publish the profile. See [Configure Android Profile in AirWatch](#).
- 9 (Optional) In the Miscellaneous page, enable the access logs for the Per-App Tunnel components. Click **Next**.  
  
You must enable these logs before you install the VMware Tunnel server.
- 10 Review the summary of your configuration and click **Save**.

You are directed to the system settings configuration page.



## 11 Select the **General** tab and download the **Tunnel virtual appliance**.

You can use VMware Unified Access Gateway to deploy the Tunnel server.

### What to do next

Install the VMware Tunnel server. For instructions, see the VMware Tunnel Guide on the AirWatch Resources Web site.

## Configure Per App Tunnel Profile for Android

After you configured and installed the VMware Tunnel Per App Tunnel component, you can configure the Android VPN profile and add a version to the profile.

### Procedure

- 1 In the AirWatch admin console, navigate to **Devices > Profiles > Add Profile** and select **Android** or **Android for Work**.
- 2 Configure the General settings for Android if they are not already set up.
- 3 In the left column, select **VPN** and click **Configure**.
- 4 Complete the VPN Connection information.

Option	Description
Connection Type	Select <b>VMware Tunnel</b> .
Connection Name	Enter a name for this connect. For example, <b>AndroidSSO Configuration</b> .
Server	The VMware Tunnel server URL is automatically entered.
Per-App VPN Rules	Select the <b>Per-App VPN Rules</b> check box.

- 5 Click **Add Version**.
- 6 Click **Save & Publish**.

### What to do next

Enable per-app VPN for the Android apps that can be accessed using Mobile SSO for Android. See [Enable Per-App VPN for Android Apps](#).

Assign the device profile to a smart group. Smart groups are customizable groups that determine which platforms, devices, and users receive an assigned application, book, compliance policy, device profile, or provision. See [Assign an AirWatch Device Profile](#).

## Enable Per-App VPN for Android Apps

The Per-App VPN Profile setting is enabled for Android apps that are accessed with VMware Identity Manager Mobile SSO for Android.

### Prerequisites

- VMware Tunnel configured with the Per-App Tunnel component installed.

- Android VPN profile created.

#### Procedure

- 1 In the AirWatch admin console, navigate to **Apps & Books > Applications > List View**.
- 2 Select the Internal tab.
- 3 Select **Add Application** and add an app.
- 4 Click **Save & Assign**.
- 5 In the Assignment page, select **Add Assignment** and in the Advanced section **Per-App VPN Profile** drop-down menu select the Android VPN profile you created.
- 6 Click **Save & Publish**.

Enable Per-App VPN for every Android app that is accessed with Mobile SSO for Android. For more information about adding or editing apps, see the VMware AirWatch Mobile Application Management Guide, on the AirWatch Resources Web site.

#### What to do next

Create the Network Traffic Rules. See [Configure Traffic Rules in AirWatch](#).

## Configure Traffic Rules in AirWatch

Configure the network traffic rules so that the VMware Tunnel client routes traffic to the HTTPS proxy for Android devices. You list the Android apps that are configured with the per app VPN option to the traffic rules, and configure the proxy server address and the destination host name.

Configure the device traffic rules to control how devices handle traffic from specified applications. Device traffic rules force the VMware Tunnel app to send traffic through the tunnel, block all traffic to specified domains, bypass the internal network straight to the Internet, or send traffic to an HTTPS proxy site.

For detailed information about creating network traffic rules, see the VMware Tunnel Guide on the AirWatch Resources website.

#### Prerequisites

- The VMware Tunnel option configured with the per-app tunnel component installed.
- Android VPN profile created.
- Per-App VPN enabled for each Android App that is added to the Network Traffic rules.

#### Procedure

- 1 In the AirWatch admin console, navigate to **System > Enterprise Integration > VMware Tunnel > Network Traffic Rules**.

- 2 In the **Device Traffic Rules** tab, configure the device traffic rules settings as described in the VMware Tunnel Guide. Specific to the Mobile SSO for Android configuration, configure the following settings.

- a Select the default action.

Option	Description
Tunnel	For the VPN configuration with single-sign on to Android, select Tunnel as the default action. All apps on the device configured for Per App VPN send the network traffic through the tunnel.
Bypass	For single sign-on to Android, select <b>Bypass</b> as the default action.  <b>Important</b> With Bypass as the default action, all apps configured for Per App VPN on the device bypass the tunnel and connect to the Internet directly. With this implementation, no traffic is sent to the Tunnel server when the Tunnel client is used only for single sign-on.

For single sign-on to Android with using VPN, select **Bypass** as the default action.

**Important** With Bypass as the default action, all apps configured for Per App VPN on the device bypass the tunnel and connect to the Internet directly. With this implementation, no traffic is sent to the Tunnel server when the Tunnel client is used only for single sign-on.

- b In the Application column, add the Android apps that are configured with the per app VPN profile.
- c For tenants hosted in the cloud, in the Action column, select Proxy and specify the HTTPS proxy information. Enter **certproxy.vmwareidentity.com:5262**.

In the Destination Hostname column, enter your destination VMware Identity Manager host name. Enter as **<tenant>.vmwareidentitymanager.<region>**. The address choices are vmwareidentity.com, vmwareidentity.eu, or vmwareidentity.asia. The VMware Tunnel client routes the traffic to the HTTPS proxy from the VMware Identity Manager host name.

- d For on premises, in the Action column, select Proxy and specify the HTTPS proxy information. Enter the VMware Identity Manager host name and port. For example, **login.example.com:5262**.

**Note** For on-premises deployments, if you are providing external access to the VMware Identity Manager host, the firewall port 5262 must be opened or port 5262 traffic must be proxied through reverse proxy in the DMZ.

In the Destination Hostname column, enter your destination VMware Identity Manager host name. For example, **myco.example.com**. The VMware Tunnel client routes the traffic to the HTTPS proxy from the VMware Identity Manager host name.

### 3 Click **Save**.

Global / sbox

## System / Enterprise Integration / AirWatch Tunnel / Network Traffic Rules

**i** Add rules to Tunnel, Block or Bypass the network traffic using AirWatch Tunnel  
 Note: These rules are only applicable to the Per App Tunnel component of AirWatch Tunnel and is only supported for Android devices. Based on the rules specified on this page, the AirWatch Tunnel application installed on your mobile device will decide to either block, bypass or tunnel network traffic. There is also an option available to route network traffic to a custom HTTPS proxy configured in your network.

Default Action \* Tunnel Block Bypass ⓘ

Rank	Application	Action	Destination Hostname	Remove
1	WS1 Android-Android	Proxy	tenant.vmwareidentity.com	✕
	Salesforce Android-Android	HTTPS Proxy *	certproxy.vmwareidentity.com:5262	

#### What to do next

Publish these rules. After the rules are published, the device receives an update VPN profile and the VMware Tunnel application is configured to enable SSO.

Go the VMware Identity Manager administration console and configure Mobile SSO for Android in the Built-in Identity Provider page.

## Configure Mobile SSO for Android Authentication in the Built-in Identity Provider

To provide single sign-on from AirWatch-managed Android devices, you configure Mobile SSO for Android authentication in the VMware Identity Manager built-in identity provider.

#### Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.

#### Procedure

- 1 In the administration console, Identity & Access Management tab, select **Manage > Identity Providers**.
- 2 Click the identity provider labeled **Built-in**.

- 3 Verify that the Users and Network configuration in the built-in identity provider is correct.

If it is not, edit the Users and Network sections as needed.

**Note** The network range that you use in the policy rule for Mobile SSO for Android should consist of only the IP addresses used to receive requests coming from the VMware Tunnel proxy server.

- 4 In the Authentication Methods section, click the **Mobile SSO (for Android devices)** gear icon.
- 5 In the CertProxyAuthAdapter page configure the authentication method.

Option	Description
<b>Enable Certificate Adapter</b>	Select this check box to enable Mobile SSO for Android.
<b>Root and Intermediate CA Certificate</b>	Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded. The file format can be either PEM or DER.
<b>Uploaded CA Certificate Subject DNs</b>	The contents of the uploaded certificate file is displayed here.
<b>Use email if no UPN in certificate</b>	If the user principal name (UPN) does not exist in the certificate, select this check box to use the emailAddress attribute as the Subject Alternative Name extension to validate user accounts.
<b>Certificate policies accepted</b>	Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID number (OID) for the Certificate Issuing Policy. Click <b>Add another value</b> to add additional OIDs.
<b>Enable Cert Revocation</b>	Select the check box to enable certificate revocation checking. This prevents users who have revoked user certificates from authenticating.
<b>Use CRL from certificates</b>	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate a certificate's status of revoked or not revoked.
<b>CRL Location</b>	Enter the server file path or the local file path from which to retrieve the CRL.
<b>Enable OCSP Revocation</b>	Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
<b>Use CRL in case of OCSP failure</b>	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
<b>Send OCSP Nonce</b>	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
<b>OCSP URL</b>	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
<b>OCSP Responder's Signing Certificate</b>	Enter the path to the OCSP certificate for the responder. Enter as /path/to/file.cer
<b>Enable Cancel Link</b>	When authentication is taking too long, if this link is enabled, users can click Cancel to stop the authentication attempt and cancel the sign-in.
<b>Cancel Message</b>	Create a custom message that displays when the authentication is taking too long. If you do not create a custom message, the default message is Attempting to authenticate your credentials.

- 6 Click **Save**.
- 7 Click **Save** on the built-in identity provider page.

### **What to do next**

Configure the default access policy rule for Mobile SSO for Android.

# Direct Enrollment in AirWatch Using Workspace ONE

# 5

Direct enrollment through Workspace ONE requires users to enroll their devices before they can access resources in the Workspace ONE application.

When direct enrollment is through the Workspace ONE application, you can direct all users to go to the appropriate application store, download Workspace ONE, enter their email address, and follow the prompts to begin using Workspace ONE on their devices.

## Supported Devices

- Apple iOS 9.0 and later
- Android Enterprise (formerly Android for Work) 5.1 and later
- Android Legacy 4.1 and later

An Android Legacy device is any Android device that is not Android Enterprise capable, or an Android Enterprise capable device connecting to an AirWatch instance that does not have Android Enterprise enabled.

This chapter includes the following topics:

- [Enable Workspace ONE for Direct Enrollment](#)
- [User Experience When Directly Enrolling into AirWatch with Workspace ONE](#)

## Enable Workspace ONE for Direct Enrollment

You enable direct device enrollment through Workspace ONE from the AirWatch admin console Enrollment > Restriction page for your organization group (OG).

When Workspace ONE is enabled for direct enrollment, qualified devices logging in for the first time are directly enrolled. Devices that do not qualify for direct enrollment are granted mobile application management-only access in a Workspace ONE registered state.

### Procedure

- 1 In the AirWatch admin console, select the organization group to enable Direct Enrollment for Workspace ONE.
- 2 Navigate to **Groups & Settings > All Settings > Device & Users > General > Enrollment** and select the **Restrictions** tab.

- 3 For Current Settings, select **Override** if required.
- 4 Scroll down to the Management Requirements for Workspace ONE and select the configuration options.

Setting	Description
<b>Require MDM for Workspace ONE</b>	When this is enabled, qualified devices and users are prompted to enroll immediately upon login to Workspace ONE.
<b>Assigned User Group</b>	All Users is the default user group. You can select a specific user group to include in the direct enrollment process.
<b>iOS</b>	Enable to include iOS devices. iOS devices are not eligible for direct enrollment if this is disabled. If this is disabled, devices can still register in AirWatch in an unmanaged state.
<b>Android Legacy</b>	Enable to include Android Legacy devices. Android Legacy devices are not eligible for direct enrollment if this is disabled. If this is disabled, devices can still register in AirWatch in an unmanaged state.
<b>Android Enterprise</b>	Enable to include Android Enterprise devices. Android Enterprise devices are not eligible for direct enrollment if this is disabled. If this is disabled, devices can still register in AirWatch in an unmanaged state.

- 5 Click **Save**.
- 6 Continue to configure the enrollment tabs with the enrollment options supported for Workspace ONE. See [Workspace ONE Direct Enrollment Configuration Options](#).

For more information about configuring Direct Enrollment for Workspace ONE, see the [VMware AirWatch Mobile Device Management Guide](#), Device Enrollment chapter.

## Workspace ONE Direct Enrollment Configuration Options

Configure direct enrollment with Workspace ONE in the AirWatch admin console. Navigate to **Groups & Settings > All Settings > Device & Users/General/Enrollment**. The Workspace ONE Device Enrollment Options Table lists the menu items that can be configured.

The Enrollment settings page lets you configure options related to device and user enrollment. The page is divided into tabs which are described below. For detailed information about configuring device enrollment, see the VMware AirWatch Mobile Device Management guide.

**Figure 5-1. AirWatch Console Enrollment Page**





**Table 5-1. Workspace ONE Direct Enrollment Configurable Menu Items**

Enrollment Tab	Configurable Menu Items for Direct Enrollment to Workspace ONE
<b>Authentication</b>	<p>Directory users are supported.</p> <p>In addition, SAML plus Active Directory Users are supported "on-the-fly". SAML without LDAP users are supported when the user record exists in AirWatch at the time of the initial login.</p> <p>For Devices Enrollment Mod, only <b>Open Enrollment</b> is supported. Registered Devices Only is not supported.</p>
<b>Terms of Use</b>	<p>Terms of use can be created to require users accept the terms of use before proceeding with the direct enrollment process.</p>
<b>Grouping</b>	<p>All grouping menu options are compatible with Workspace ONE direct enrollment.</p> <p><b>Sync Users Groups in Real Time for Workspace ONE</b> is enabled by default. When a device is enrolling, AirWatch makes a real time call to Active Directory to sync the user's user groups. If the user does not exist in AirWatch, the AirWatch console first syncs the user and then syncs the user groups in real time. If this feature is not enabled, the AirWatch console does not sync the user groups.</p> <p><b>Note</b> This feature is CPU-intensive. If user groups are not frequently changing or the user groups already exist in AirWatch, disable this setting for improved performance and to prevent latency issues when launching the Workspace ONE app.</p> <p>See Placing Devices in the Correct Organization Group section in <a href="#">Deployment Strategies for Setting Up Multiple AirWatch Organization Groups</a>.</p>
<b>Restrictions</b>	<ul style="list-style-type: none"> <li>■ In <b>User Access Control</b>, you can select both Restrict Enrollment to Known Users and Restrict Enrollment to Configured Groups.</li> <li>■ Maximum device limit is supported.</li> <li>■ <b>Policy Setting</b> is partially supported. <ul style="list-style-type: none"> <li>■ <b>Allowed Ownership Types</b>. Workspace ONE only prompts for Employee Owned and Corporate - Dedicated.</li> </ul> </li> </ul> <p><b>Note</b> Container Allow enrollment type is not supported.</p>
<b>Optional Prompt</b>	<p>The two optional prompts that can be enabled are <b>Prompt for Ownership Type</b> and <b>Enable Device Asset Number Prompt</b>. The request to enter the asset number is only prompted for when the ownership type is Corporate Owned.</p>
<b>Customization</b>	<p>Customization menu options supported.</p> <ul style="list-style-type: none"> <li>■ Post-Enrollment Landing URL (iOS only)</li> <li>■ MDM Profile Message (iOS only)</li> <li>■ Use Custom MDM Applications</li> </ul> <p>Use specific Message Template for each Platform can be enabled, but specific Workspace ONE message templates are not available for Workspace ONE 3.2.</p>

## User Experience When Directly Enrolling into AirWatch with Workspace ONE

When mobile device management is implemented through Workspace ONE, users download the Workspace ONE application, authenticate with AirWatch, and enroll their device. After the device is enrolled, users can use Workspace ONE to add and use their entitled resources immediately.

The process users experience when using Workspace ONE to enroll their devices is similar for iOS and Android Enterprise devices. Android Legacy enrollment is redirected to the AirWatch Agent for enrollment. AirWatch Agent automatically hands control back to Workspace ONE when enrollment is complete. Users can access Workspace ONE in each of these variations.

### Direct Enrollment Through Workspace ONE on iOS Devices

Direct users to download, install, and run the Workspace ONE application from the Apple App store.

#### Procedure

- 1 Users open the app, enter their server URL and email address, and authenticate according to the configuration for their environment.
- 2 The **Additional setup is required by your company screen** displays.

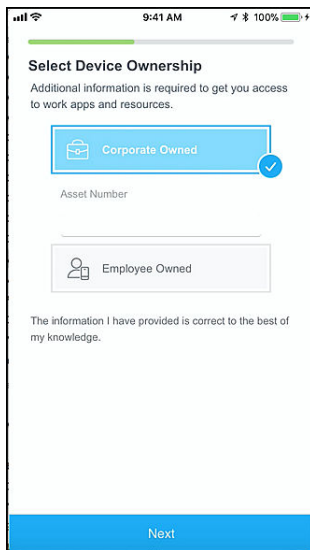
Figure 5-2. Notification of Setting up Device Enrollment



- 3 If Terms of Use is configured, users are asked to accept the terms of use before proceeding.

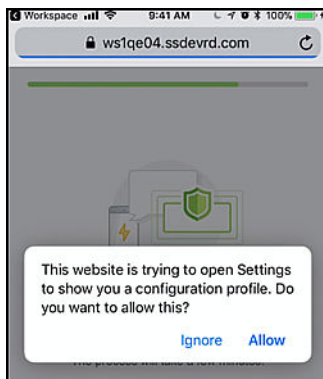
- 4 If you set up the optional prompts to show the device ownership type and request the device asset number, this information is displayed.

**Figure 5-3. Device Ownership Selection**



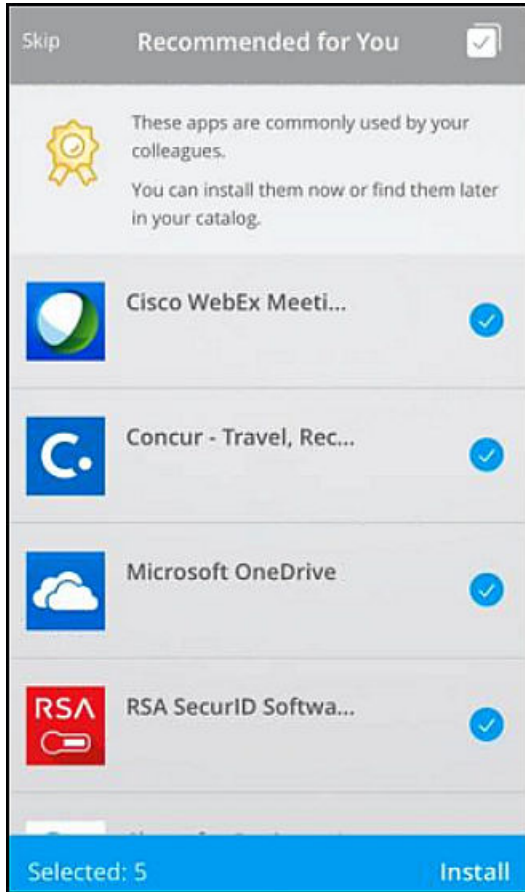
- 5 Safari is opened and users click **Allow** to open the Settings page.

**Figure 5-4. Allow Configuration Profile Settings**



The Workspace Services and configuration profile are configured on the device.

The device is now enrolled in AirWatch and Workspace ONE is launched. The Recommended for You screen is displayed.

**Figure 5-5. Recommended Applications Screen**

- 6 Users can select the applications they want to install or they can skip this step for now.

The device is now managed by AirWatch MDM. If recommended applications were selected to be installed, users begin to receive push notifications for those applications.

## Direct Enrollment Using Workspace ONE on Android Enterprise Devices

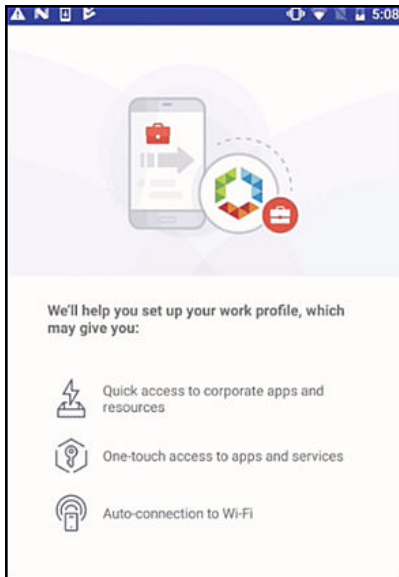
Direct users to download, install, and run the Workspace ONE application from the Google App Store or the repository.

### Procedure

- 1 Users enter their server URL and email address, and authenticate according to the configuration for their environment.

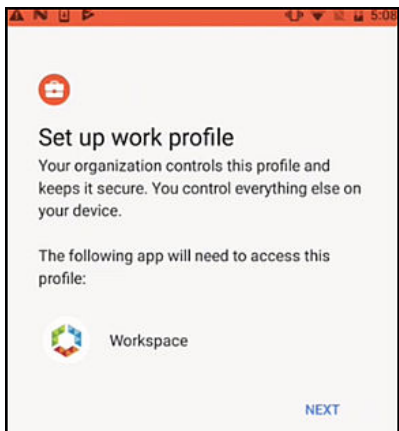
- 2 The **Additional setup is required by your company screen** displays. The user clicks **Continue**.

**Figure 5-6. Notification of Setting up Device Enrollment**



- 3 If Terms of Use is configured, users are asked to accept the terms of use before proceeding.
- 4 If you set up the optional prompts to show the device ownership type and request the device asset number, this information is displayed.
- 5 The Workspace Services and work profile are configured on the device.

**Figure 5-7. Set Up Work Profile Notification**

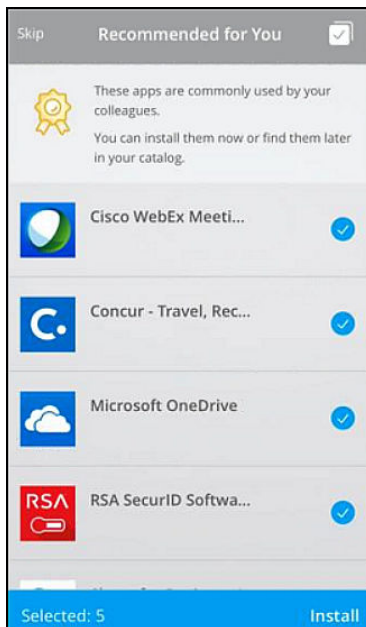


Users see a message describing device management control with this work profile and click **OK**.

The Workspace ONE application is installed and the Android Work Account is registered.

- 6 The device is now enrolled in AirWatch and Workspace ONE is launched. The Recommended for You screen is displayed.

**Figure 5-8. Recommended Applications Screen**



- 7 Users can select which applications they want to install or skip this step for now.

The device is now managed by AirWatch MDM. If recommended applications were selected to be installed, those applications begin to be installed with a badged Android Enterprise briefcase icon.

## Device Enrollment for Android Legacy Devices

Device enrollment for Android Legacy devices redirects to the AirWatch Agent for enrollment. AirWatch Agent automatically hands control back to Workspace ONE when the enrollment is complete.

Direct users to go to the application store to download Workspace ONE.

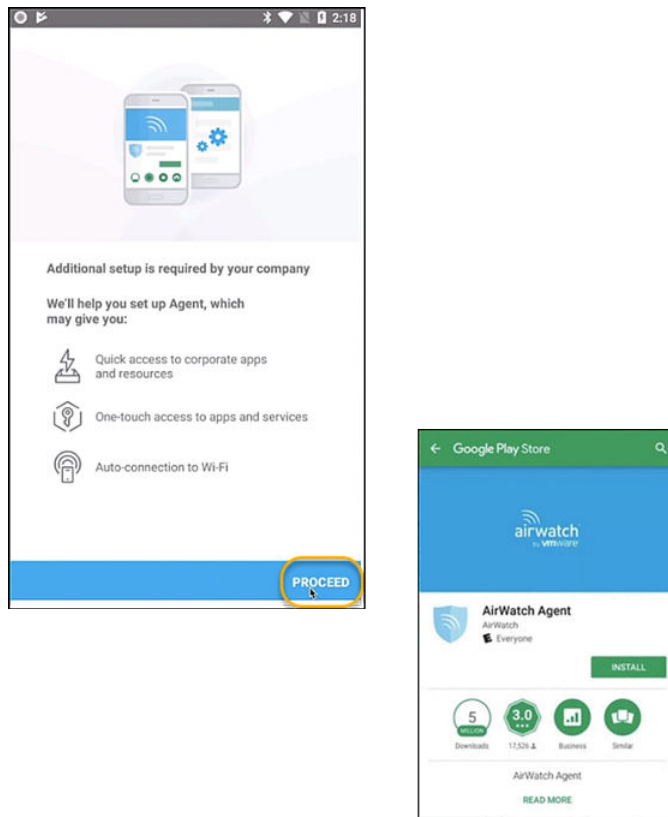
### Procedure

- 1 Users open the app, enter either their server URL or email address and enter their user name and password to sign in.

At this point, the Workspace ONE application can detect that the device is not enabled for Android Enterprise and if the device requires direct enrollment before resources on Workspace ONE can be accessed.

- 2 The **Additional setup is required by your company** screen displays and when users click **Proceed**, they are redirected to the AirWatch Agent application in the Google Play Store.

**Figure 5-9. AirWatch Agent Application Download Request**



- 3 Users download the AirWatch Agent application.

---

**Note** If the AirWatch Agent application is already installed on the device, Workspace ONE automatically launches the application. They are not redirected to the app store.

---

The authentication details that were entered for Workspace ONE are passed to the AirWatch Agent application so users do not reenter this information.

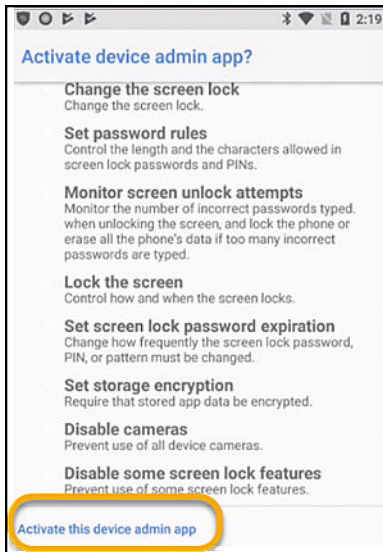
The AirWatch Agent application is launched. During the device enrollment with the AirWatch agent, users select the ownership type and enter the device asset number, if configured.

- 4 When **Allow Agent to make and manage phone calls** displays, users click **Allow**.

AirWatch Agent validates the enrollment, authenticates the user, and grants permissions to AirWatch on this device.

- 5 When the **Activate device admin app?** screen displays, users click **Activate this device admin app**.

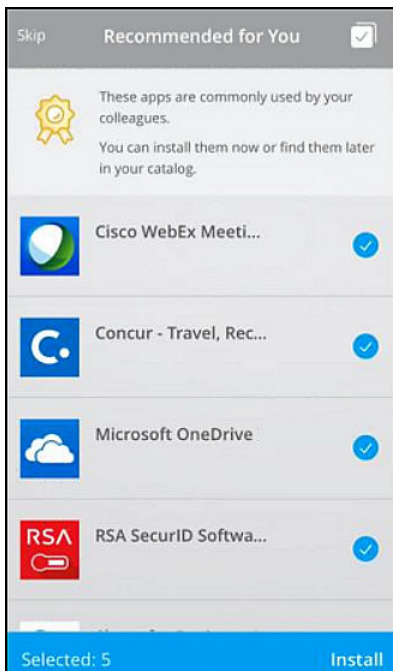
**Figure 5-10. Activate Device Admin App**



- 6 Users are asked to grant permission to access various device capabilities.

The device is now enrolled in AirWatch and Workspace ONE is launched. The Recommended applications screen is displayed.

**Figure 5-11. Recommended Applications Screen**



- 7 Users can select the applications they want to install or they can skip this step for now.



The device is now managed by AirWatch MDM. If recommended applications were selected to be installed, users begin to receive notifications for those applications.

# Leveraging Workspace ONE to Support Apple Device Enrollment Program Integration

## 6

The Apple Device Enrollment Program (DEP) does not support scenarios where a customer is using SAML for user authentication. However Workspace ONE has implemented a unique way to support this use case.

Through AirWatch device staging, admins can assign the device to a multi-device staging user and allow Workspace ONE to reassign the device the appropriate user when they sign in to the Workspace ONE application.

The Workspace ONE application must be installed on the device as part of the staging user enrollment. When users sign in to Workspace ONE the first time, Workspace ONE authenticates the user through the configured SAML provider. After the user is authenticated, the ownership of the device is switched from the multi-device staging user to the authenticated directory user.

## Prerequisite

The directory user must exist in AirWatch when the user signs in to the Workspace ONE application. You can pre-load users in a bulk load through CSV or apply the following API to generate users on an as needed basis.

---

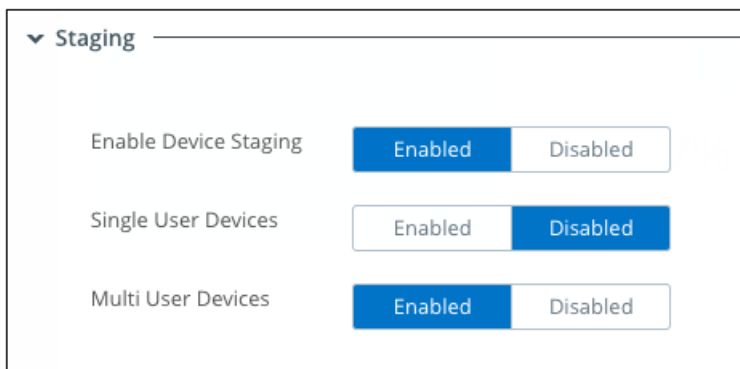
**Note** The Security Type value must equal directory.

```
https://<API_SERVER_ADDRESS>/api/help/#!/apis/10006?!/User/User_AddUser
```

## Flow for Workspace ONE Support of DEP Integration

The following tasks must be completed to implement support of the Apple Device Enrollment Program using Workspace ONE

- Install the Workspace ONE application on the iOS devices.
- Ensure that a staging user exists with the following staging configuration.
  - a Navigate to **Accounts > Users > List View** and select the user account for which you want to enable device staging to edit.
  - b In the **Add/Edit User** page, select the **Advanced** tab. Scroll down to the **Staging** section and enable **Device Staging** and **Multi User Devices**.

**Figure 6-1. Multi User Devices Setting in AirWatch**

- Assign the device to the staging user in the Apple DEP portal and deliver the device to the end user.

For more information about the Apple Device Enrollment Program, see the [VMware AirWatch Guide for the Apple Device Enrollment Program](#).

## How the Integration Works

When the user turns on the device the first time, the device is enrolled and assigned to the multi-device staging user. The user launches the Workspace ONE application that is available on the home screen and signs in. Workspace ONE authenticates the user through the configured SAML provider.

After the user is authenticated, the ownership of the device is switched from the multi-device staging user to the authenticated directory user. Applications, profiles, and resources assigned to the authenticated user are pushed to the device.

---

**Note** The organization group of the device does not change. This feature does not support user group mapping (or manual user selection based on drop down menu) located in the Enrollment Setting section of the AirWatch console.

---

# Enabling the Out of Box Experience for Workspace ONE on Dell Windows 10 Devices



When users receive a new Dell® Windows 10 device with out-of-box (OOBE) provisioning enabled in the AirWatch Windows 10 Provisioning Service, the Workspace ONE application can be configured to open automatically and deliver applications to the device.

To deliver this OOBE with the Workspace ONE application, you must enable the External Access Token authentication method as part of the AirWatch integration. Then the authentication method is enabled in the built-in provider and you create an access policy rule to use the External Access Token authentication method.

The Workspace ONE OOBE runs the Workspace ONE application without requiring users to enter their sign-in credentials a second time. If this authentication method is not enabled, users must sign in to Workspace ONE in addition to signing in to the device during the Windows registration process.

---

**Note** Other services that must be set up for the OOBE in Dell Windows 10 devices include the AirWatch Provisioning Service for Windows 10 and federation to Microsoft Azure Active Directory. See Windows 10 Provisioning Service and Windows Desktop Enrollment Overview and Windows in the AirWatch Windows Desktop Platform Guide for provisioning service configuration details.

---

This chapter includes the following topics:

- [Enable External Access Token in AirWatch](#)
- [Activate External Access Token as an Authentication Method](#)
- [Associate External Access Token Authentication Method to the Built-in Identity Provider](#)
- [Create Access Policy for Workspace ONE Out-of-Box Experience Process](#)
- [Workspace ONE for Windows 10 Custom Out-of-Box Branding](#)

## Enable External Access Token in AirWatch

To enable the out of box experience for Workspace ONE on Dell Windows 10 devices, you must first enable the External Access Token authentication method on the AirWatch configuration page.

### Procedure

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

- 2 In the User External Access Token Authentication through AirWatch section, select **Enable**.
- 3 Click **Save**.

#### What to do next

Activate the external access token as an authentication method.

## Activate External Access Token as an Authentication Method

In VMware Identity Manager, the External Access Token authentication method is unique to the AirWatch integration and is required for both single sign-on (SSO) and triggering the out-of-box experience (OOBE) in Workspace ONE on Windows 10 devices.

#### Prerequisites

When using AirWatch External Access Token authentication, the AirWatch Cloud Connector component of VMware Enterprise Systems Connector must be deployed and configured.

- External Access Token Authentication enabled on the AirWatch page in the Identity & Access Management tab.
- Microsoft Azure Active Directory service configured.
- AirWatch Provisioning Service for Windows 10 devices configured.

The configuration of External Access Token is read-only and is based off the AirWatch configuration in VMware Identity Manager. The exception is the token lifetime field.

#### Procedure

- 1 To review and manage the configuration, in the Identity & Access Management tab, select **Authentication Methods**.
- 2 In the **Airwatch External Access Token Configure** column, click the pencil icon.
- 3 Review the configuration.

Option	Description
<b>Enable AirWatch External Access Token</b>	This check box is enabled on the AirWatch page.
<b>AirWatch Admin Console URL</b>	Pre-populated with the AirWatch URL.
<b>AirWatch API Key</b>	Pre-populated with the AirWatch Admin API key.
<b>Certificate Used for Authentication</b>	Pre-populated with the AirWatch Cloud Connector certificate.

Option	Description
<b>Password for Certificate</b>	Pre-populated with the password for the AirWatch Cloud Connector certificate.
<b>AirWatch External Access Token Lifetime in Seconds</b>	<p>The access token is used to validate the authentication with VMware Identity Manager. Access tokens have a limited lifetime. The time configured is the maximum time that the access token is valid. The token life is editable and defaulted to 600 seconds, which is 10 minutes.</p> <p>If the access token expires, users are prompted to authenticate again in the Workspace ONE application.</p>

- 4 Click **Save**.

#### What to do next

Associate the AirWatch External Access Token authentication method in the built-in identity provider. See [Configure Built-in Identity Providers](#)

After the AirWatch External Access Token is associated to the built-in identity provider, create an access policy rule to use this auth method. See [Create Access Policy for Workspace ONE Out-of-Box Experience Process](#).

## Associate External Access Token Authentication Method to the Built-in Identity Provider

When External Access Token is configured as an authentication method, the authentication method is available in the built-in identity provider. You must associate this authentication method with a user directory in the built-in identity provider.

#### Prerequisites

External Access Token enabled in the AirWatch configuration page.

External Access Token activated as an authentication method.

#### Procedure

- 1 In the Identity & Access Management tab, go to **Manage > Identity Providers**.
- 2 Click the **Built-in** from the list view.

Option	Description
<b>Users</b>	The configured directories are listed. Select the users directories to use the external access token authentication method.
<b>Network</b>	The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication.
<b>Authentication Methods</b>	The authentication methods that are configured on the service are displayed. Select the <b>AirWatch External Access Token</b> check box.

- 3 Click **Save**.

## What to do next

Configure the default access policy rule to list the External Access Token authentication method as the last fallback method in the rule. See [Create Access Policy for Workspace ONE Out-of-Box Experience Process](#).

Go to the Catalog Settings page to create a custom branded welcome page and message for users who sign in to Workspace ONE as part of the Windows 10 out-of-box experience. See [Workspace ONE for Windows 10 Custom Out-of-Box Branding](#).

## Create Access Policy for Workspace ONE Out-of-Box Experience Process

To establish the Workspace ONE out-of-box experience (OOBE) after the External Access Token is enabled and added to the built-in identity provider, you must add the External Access Token authentication method to the default access policy set.

### Procedure

- 1 In the administration console Identity & Access Management tab, select **Manage > Policies**.

- 2 Click **Edit Default Policy** and then click **Next**.

- 3 Select the row that lists the **Workspace ONE App** in the Device Type column.

If the Workspace ONE App rule is not listed, click **Add Policy Rule**.

- 4 Select the authentication methods to use to access content from the Workspace ONE application.

List the External Access Token authentication method as the last fallback method in the rule. When the External Access Token is detected in the authentication request, the authentication method is honored. Any other authentication methods listed after the External Access Token are not detected.

- 5 Click **Next** to review the configuration.

- 6 Click **Save**.

**Figure 7-1.**

The screenshot shows the 'Add Policy Rule' configuration page. It has a breadcrumb 'Configuration' and a title 'Add Policy Rule'. The configuration is as follows:

- Conditions:**
  - \* If a user's network range is: All Ranges (dropdown)
  - \* and user accessing content from: Workspace ONE App (dropdown)
  - and user belongs to group(s): Select Groups... (search box)

Rule applies to all users if no group(s) selected.
- Actions:**
  - Then perform this action: Authenticate using... (dropdown)
  - \* then the user may authenticate using: Password (dropdown)
  - If the preceding method fails or is not applicable, then: Airwatch External Access Token (dropdown)
  - + Add fallback method (button)
- Re-authentication:**
  - \* Re-authenticate after: 8 (input) Hours (dropdown)

- 7 On the Configuration page, review the order of the rules in the rules list. If the Workspace ONE app rule is not the first rule in the default access policy list, drag the rule to be the first row in the list.

Workspace ONE App must be the first rule in the default access policy rules list.

- 8 Click **Next**.
- 9 Review the Summary page and click **Save**.

## Workspace ONE for Windows 10 Custom Out-of-Box Branding

When the Windows 10 Provisioning Service by VMware AirWatch is used for new Windows 10 device provisioning, custom branding and a welcome message can be set up in the Workspace ONE application.

As users power on their new computers and sign in with their credentials for the first time, the AirWatch provisioning agent ensures that the Workspace ONE application is available. Workspace ONE is launched after Windows is fully prepared. Users see a custom welcome message with the company's branding before the Workspace ONE application catalog opens. During this time, if Show recommended apps in Bookmarks tab is enabled in the Catalog > Settings > User Portal Configuration page, recommended applications are downloaded by Workspace ONE.

**Note** See the *Windows Desktop Platform Guide* for information about the Windows 10 provisioning service by AirWatch.



## Procedure

- 1 In the administration console Catalogs tab, select **Settings > User Portal Branding**.
- 2 In the **Desktop Out-of-Box-Experience** section, edit the settings to customize the Workspace ONE registration pages.

Form Item	Description
Welcome Screen Logo	Add a logo to be centered at the top of the Welcome screen. The maximum size of the image is 250 x 250 px. The format is PNG.
Welcome Screen Background Color	The color that displays for the background of the Start and Welcome screens. Enter a six-digit hexadecimal color code over the existing one to change the background color. The preview screen is updated with the new color.
Welcome Screen Next Button Color	Enter a six-digit hexadecimal color code to change the background color for the Next button that displays on the Welcome screen.
Welcome Screen Font Color	Enter a six-digit hexadecimal color code to change the font color for the Next button.
Welcome Message	Create a welcome message about using Workspace ONE that displays on the Welcome page.

- 3 Click **Save**.

# Deploying the VMware Workspace ONE Mobile Application

## 8

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

Users can access their entitled applications 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 applications.

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 managed application.

This chapter includes the following topics:

- [Device Management Options in AirWatch for Public and Internal Apps for Workspace ONE](#)
- [Managing Access to Applications](#)
- [Requiring Terms of Use to Access the Workspace ONE Catalog](#)
- [Getting and Distributing the Workspace ONE Application](#)
- [Registering Email Domains for Auto Discovery](#)
- [Session Authentication Setting](#)
- [Deployment Strategies for Setting Up Multiple AirWatch Organization Groups](#)

## Device Management Options in AirWatch for Public and Internal Apps for Workspace ONE

You can configure to deploy public and internal applications based on the device management status. Any device can access applications that are configured as open access. Only devices that are granted permission, either by being enabled through the Workspace Services or Agent Enrollment, can access applications that are configured for managed access.

The table outlines capabilities for both managed and unmanaged scenarios.

Access Type	Features	Description	Suggested Uses
Open Access (unmanaged)	<ul style="list-style-type: none"> <li>Self-service app catalog for Web, Horizon, and Citrix resources</li> <li>Launch web/virtual with single sign-on (SSO)</li> <li>Touch ID / PIN application protection</li> <li>Device jailbreak detection</li> <li>Support for VMware Identity Manager conditional access, including authentication policies and blocking devices.</li> <li>Native application access.</li> <li>Internal App and SDK app distribution.</li> </ul>	<p>Users access resources on their device without granting admins permission to access their device.</p> <p>The applications with open access are available to devices no matter their managed status. Admins cannot systematically remove native applications when they are set to Open Access.</p>	<ul style="list-style-type: none"> <li>Provide application access to end-users immediately upon login, without elevated security permissions.</li> <li>Recommend the use of an application without requiring that the application be installed. Users can install the application on their device when they want.</li> <li>Applications do not contain sensitive corporate data and do not access protected corporate resources.</li> <li>To distribute applications to auxiliary personnel without the AirWatch MDM profile.</li> </ul>
Managed Access	<ul style="list-style-type: none"> <li>Self-service app catalog for Web, Horizon, and Citrix resources</li> <li>Launch web/virtual with single sign-on (SSO)</li> <li>Touch ID / PIN application protection</li> <li>Device jailbreak detection</li> <li>Support for VMware Identity Manager conditional access, including authentication policies and blocking devices.</li> <li>Managed and direct installation of Native Apps</li> <li>Internal App and SDK app management.</li> <li>Support for app configuration</li> <li>Per-app VPN</li> <li>One Touch SSO for SAML enabled native apps</li> <li>Device profiles</li> <li>AirWatch compliance engine</li> </ul>	<p>Users install a management profile on their device to grant admins permission to access their device.</p> <p>Applications with managed access are available to devices that AirWatch manages.</p> <p>If AirWatch does not manage the device, Workspace ONE prompts the user on the device to enroll with AirWatch. If the device is enrolled, the user can use the device to access the application through Workspace ONE.</p>	<ul style="list-style-type: none"> <li>To remove sensitive corporate data from devices when users leave the organization or lose their device.</li> <li>Require app tunneling to authenticate and securely communicate with internal back-end resources when applications access the intranet.</li> <li>Enable single sign-on for applications.</li> <li>Track user adoption and installation status for applications.</li> <li>Deploy the application automatically upon enrollment.</li> </ul>

For information on where to configure managed access options for internal applications or how to add public application for deployment through Workspace ONE, see the AirWatch Mobile Application Management Guide.

## Supported Platforms for Open and Managed Access

Configure the access type for internal and public applications based on the platform.

	Managed Access	Open Access
INTERNAL APPLICATIONS		
Android	X	X
iOS	X	X
Windows 10 Desktop	X	-
Windows 10 Phone	X	-
PUBLIC APPLICATIONS		
Android	X	X
iOS	X	X
Windows 10 Desktop	-	X
Windows 10 Phone	-	X

## Managing Access to Applications

A single user might be entitled to a mix of open or managed access to native apps. The adaptive management approach allows for end users to use open access applications without requiring management. When users request a native app that requires management, adaptive management provides the additional security and control needed to manage that native app.

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, the access state displays as either open or managed based on configuration for that application. For example, if the **Send App Configuration** option is selected, an application is set to require management.

Applications that require management display a star icon when viewed in an unmanaged state in the catalog. Users must select to enable Workspace services through the adaptive management process to use the application. When users attempt to download an application that displays a star icon, they are prompted with a message that asks users to enable the Workspace Services. Users can click a privacy notice 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 star icon is removed from all the managed applications.

## Removing Access on Managed Devices

Users can disable the Workspace ONE app on their managed device through the Remove Account option. Removing the account executes an enterprise wipe of the device, removing corporate access and returning the user to the login screen. Administrators can perform an enterprise wipe from the AirWatch admin console to disable Workspace ONE services.

Executing a Remove Account action on managed devices revokes access granted through the Workspace ONE application and unenrolls the device from AirWatch. Applications that required management are removed from the device and access to AirWatch productivity applications such as Boxer, Browser, and Content Locker, is revoked.

## Requiring Terms of Use to Access the Workspace ONE Catalog

You can write your organization's own Workspace ONE terms of use and ensure the end user accepts this terms of use before using Workspace ONE.

The terms of use display after the user signs into Workspace ONE. Users must accept the terms of use before proceeding to their Workspace ONE catalog.

The Terms of Use feature include the following configuration options.

- Create versions of existing terms of use.
- Edit terms of use.
- Create multiple terms of use that can be displayed based on the device type.
- Create language-specific copies of the terms of use.

The terms of use policies that you setup are listed in the Identity & Access Management tab. You can edit the terms of use policy to make a correction to the existing policy or create a new version of the policy. Adding a new version of the terms of use, replaces the existing terms of use. Editing a policy does not version the terms of use.

You can view the number of users who have accepted or declined the terms of use from the terms of use page. Click either the accepted or declined number to see a list of users and their status.

## Set Up and Enable Terms of Use

In the Terms of Use page, you add the terms of use policy and configure the usage parameters. After the terms of use are added, you enable the Term of Use option. When users sign in to Workspace ONE, they must accept the terms of use to access their catalog.

### Prerequisites

The text of the terms of use policy formatted in HTML to copy and paste in the Terms of Use content text box. You can add terms of use in English, German, Spanish, French, Italian, and Dutch.

**Procedure**

- 1 In the administration console Identity & Access Management tab, select **Setup > Terms of Use**.
- 2 Click **Add Terms of Use**.
- 3 Enter a descriptive name for the terms of use.
- 4 Select **Any**, if the terms of use policy is for all users. To use terms up use policies by device type, select **Selected Devices Platforms** and select the device types that display this terms of use policy.
- 5 By default, the language of the terms of use that is displayed first is based on the browser language preference settings. Enter the terms of use content for the default language in the text box.
- 6 Click **Save**.  
  
To add a terms of use policy in another language, click **Add Language** and select another language. The Terms of Use content text box is refreshed and you can add the text in the text box.  
  
You can drag the language name to establish the order that the terms of use are displayed.
- 7 To begin using the terms of use, click **Enable Terms of Use** on the page that displays.

**What to do next**

If you selected a specific device type for the terms of use, you can create additional terms of use for the other device types.

**View Status of Terms of Use Acceptance**

The terms of use policies listed in the Identity & Management > Terms of Use page shows the number of users that accepted or declined the policy.

**Procedure**

- 1 In the administration console Identity & Access Management tab, select **Setup > Terms of Use**.
- 2 In the Accepted / Decline column, click either the Accepted number on the left or the Declined number on the right.

A status page displays the action taken, either accepted or declined, with the user name, device ID, version of the policy viewed, platform used, and the date.

- 3 Click **Cancel** to close the view.

**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 managed 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 managed application from the AirWatch admin console. You can also run the Workspace ONE Getting Started wizard to push the application.

---

**Note** For detailed information on configuring managed 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 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
<b>Info</b>	Enter and view information concerning supported device models, ratings, and categories.
<b>Assignment</b>	Assign the Workspace ONE mobile application to smart groups of end users who can use the application on their device.
<b>Deployment</b>	Configure availability and advanced enterprise mobility management (EMM) features, if applicable.  To automatically configure managed applications, enable <b>Send Application Configuration</b> and enter the App Configuration for Enterprise (ACE) key value pairs. See <a href="#">AirWatch Application Configuration for Enterprise Key Value Pairs</a> .
<b>Terms of Use</b>	(Optional) Enable <b>Terms of Use</b> for using the Workspace ONE application.

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

Complete these steps for each supported platform.

## AirWatch Application Configuration for Enterprise Key Value Pairs

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

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

**Table 8-1. 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.
iOS	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.
iOS	SkipDiscoveryScreen	Boolean	true	Beginning with the Workspace ONE application version 3.1, the SkipDiscoveryScreen configuration key can be configured. When set to True, Workspace ONE tries to move past the email address/server URL screen. When used with the AppServiceHost configuration key, users are immediately taken to the authentication screen. If mobile SSO is also used, admins can provide end users with a seamless experience whereby they start Workspace ONE and immediately begin loading their Workspace ONE app.



## Registering Email Domains for Auto Discovery

You can register your email domain in the auto discovery service in 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 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**.

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**.

## Set up Auto Discovery in VMware Identity Manager

To register a domain, you enter your email domain and email address in the 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 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 <a href="https://discovery.awmdm.com">https://discovery.awmdm.com</a> .
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.

## **Enabling Compliance Checking for AirWatch Managed Devices**

When users enroll their devices, 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.

The VMware Identity Manager service 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 Workspace ONE 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 unenrolls 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 website.

## Deployment Strategies for Setting Up Multiple AirWatch Organization Groups

AirWatch uses organization groups (OG) to identify users and establish permissions. When AirWatch is integrated with VMware Identity Manager, the admin and enrollment user REST API keys are configured at the AirWatch organization group type called Customer.

When users sign in to Workspace ONE from a device, a device registration event is triggered within VMware Identity Manager. A request is sent to AirWatch to pull any applications that the user and device combination is entitled to. The request is sent using the REST API to locate the user within AirWatch and to place the device in the appropriate organization group.

To manage organization groups, two options can be configured in VMware Identity Manager.

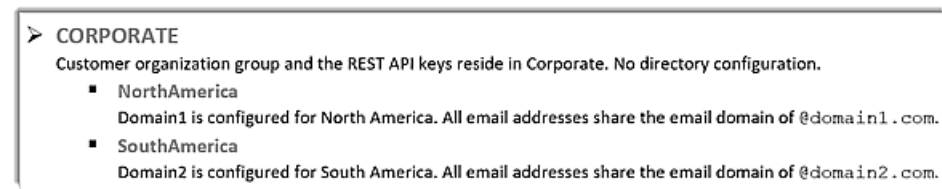
- Enable AirWatch auto discovery.
- Map AirWatch organization groups to domains in the VMware Identity Manager service.

If neither of these two options are configured, Workspace ONE attempts to locate the user at the organization group where the REST API key is created. That is the Customer group.

### Using AirWatch Auto Discovery

Set up Auto Discovery when a single directory is configured at a child group to the Customer Organization Group, or when multiple directories are configured below the Customer group with unique email domains.

**Figure 8-1. Example 1**



In example 1, the email domain of the organization is registered for auto discovery. Users enter only their email address in the Workspace ONE sign-in page.

In this example, when users in the NorthAmerica domain sign in to Workspace ONE, they enter the complete email address as user1@domain1.com. The application looks for the domain and verifies that the user exists or can be created with a directory call in the NorthAmerica organization group. The device can be registered.

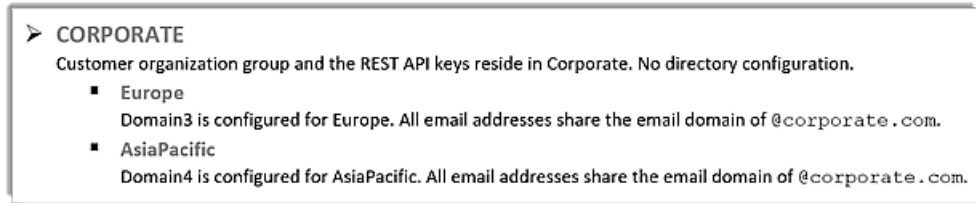
### Using AirWatch Organization Group Mapping to VMware Identity Manager Domains

Configure VMware Identity Manager to AirWatch organization group mapping when multiple directories are configured with the same email domain. You enable **Map Domains to Multiple Organization Groups** in the AirWatch configuration page in the VMware Identity Manager admin console.

When the Map Domains to Multiple Organization Groups option is enabled, domains configured in VMware Identity Manager can be mapped to AirWatch organization group IDs. The admin REST API key is also required.

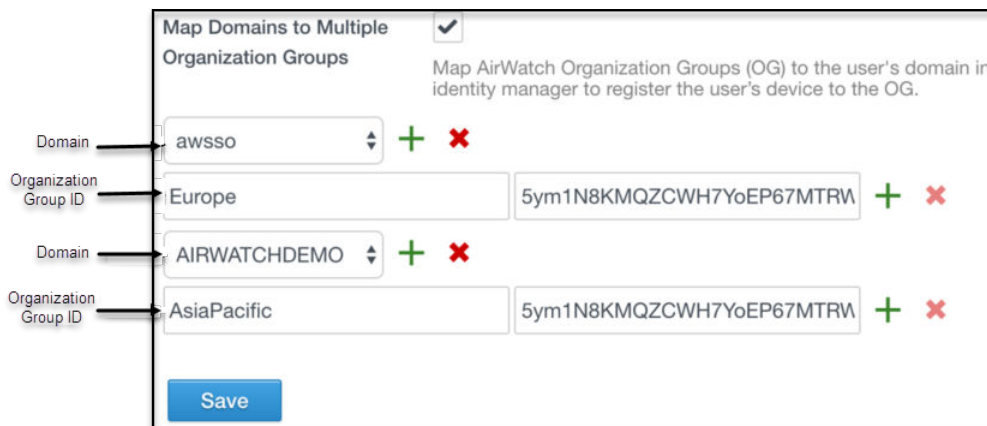
In example 2, two domains are mapped to different organization groups. An admin REST API key is required. The same admin REST API key is used for both organization group IDs.

**Figure 8-2. Example 2**



In the AirWatch configuration page in the VMware Identity Manager admin console, configure a specific AirWatch organization group ID for each domain.

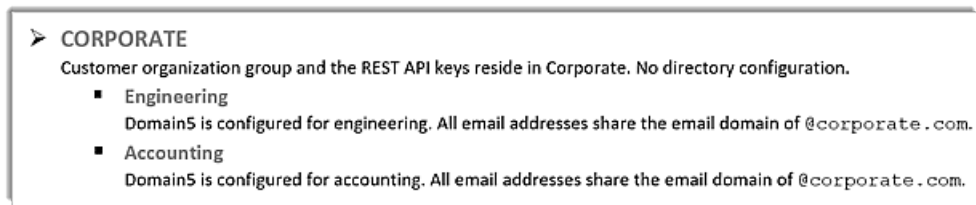
**Figure 8-3. Example 2 Organization Group Configuration**



With this configuration, when users logs in to Workspace ONE from their device, the device registration request attempts to locate users from Domain3 in the organization group Europe and users from Domain4 in organization group AsiaPacific.

In example 3, one domain is mapped to multiple AirWatch organization groups. Both directories share the email domain. The domain points to the same AirWatch organization group.

**Figure 8-4. Example 3**



In this configuration, when users sign in to Workspace ONE, the application prompts the users to select which group they want to register into. In this example, users can select either Engineering or Accounting.

**Figure 8-5. Organization Groups Where Directories Share the Same Domain**

**Map Domains to Multiple Organization Groups** ☒

Map AirWatch Organization Groups (OG) to the user's domain in identity manager to register the user's device to the OG.

Domain:  + -

Organization Group ID:

Engineering	5ym1N8KMQZCWH7YoEP67MTRM	+ -
Accounting	5ym1N8KMQZCWH7YoEP67MTRM	+ -

## Placing Devices in the Correct Organization Group

When a user record is successfully located, the device is added to the appropriate organization group. The AirWatch enrollment setting **Group ID Assignment Mode** determines the organization group to place the device. This setting is in the System Settings > Device & Users > General > Enrollment > Grouping page.

**Figure 8-6. AirWatch Group Enrollment for Devices**

Devices & Users > General > Enrollment ⓘ

Authentication Terms of Use **Grouping** Restrictions Optional Prompt Customization

Current Setting ☐ Inherit ☒ Override

Group ID Assignment Mode \* ☒ Default ☐ Prompt User To Select Group ID ☐ Automatically Select Based on User Group

In example 4, all users are at the Corporate organization group level.

**Figure 8-7. Example 4**

➤ **CORPORATE**

Customer organization group and the REST API keys reside in Corporate. Directory configuration resides in Corporate.

- Engineering
- Accounting

Device placement depends on the selected configuration for the Group ID Assignment Mode at the Corporate organization group.

- If Default is selected, the device is placed in to the same group where the user is located. For example 4, the device is placed into the Corporate group.

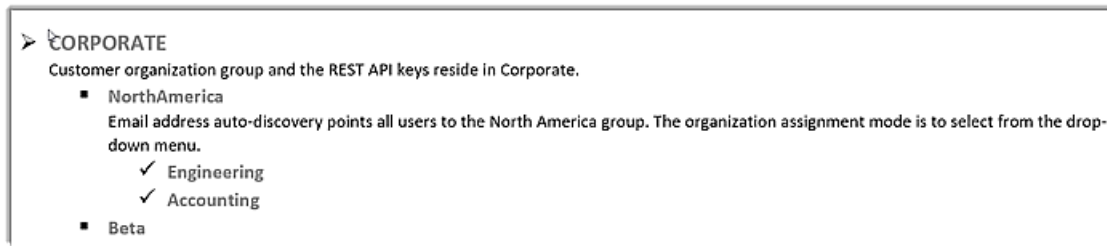
- If Prompt User to Select Group ID is selected, users are prompted to select which group to register their device into. For example 4, users see a drop-down menu within the Workspace ONE app with Engineering and Accounting as options.
- If Automatically Selected Based on User Group is selected, devices are placed into either Engineering or Accounting based on their user group assignment and corresponding mapping in the AirWatch admin console.

## Understanding the Concept of a Hidden Group

In example 4, when users are prompted to select an organization group from which to register, users also can enter a group ID value that is not in the list presented from the Workspace ONE app. This is the concept of a hidden group.

In example 5, in the Corporate organization group structure, North America and Beta are configured as groups under Corporate.

**Figure 8-8. Example 5**



In example 5, users enter their email address into Workspace ONE. After authentication, users are shown a list that displays Engineering and Accounting from which to choose. Beta is not an option that is displayed. If users know the organization group ID, they can manually enter Beta in to the group selection text box and successfully register their device into Beta.

# Working in the Workspace ONE Portal

# 9

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. The Catalog page in Workspace ONE displays resources that have been pushed to Workspace ONE. Users can tap or click to search, add, bookmark, and update applications. They can right-click on an app to remove it from the Bookmarked page, and go to the Catalog page to add entitled resources.

This chapter includes the following topics:

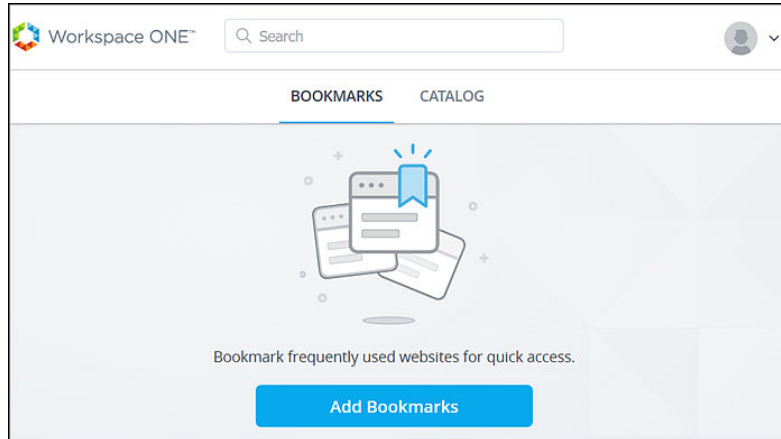
- [Working with Applications in Workspace ONE](#)
- [Setting Passcodes for the Workspace ONE Application](#)
- [Adding Native Applications](#)
- [Using VMware Verify for User Authentication](#)
- [Send Alerts to Workspace ONE Users](#)
- [Working with Workspace ONE for Android Devices](#)

## Working with Applications in Workspace ONE

The Workspace ONE user portal is made up of a Catalog tab and a Bookmarks tab. When users sign in to their Workspace ONE portal the first time, the Catalog tab is displayed if the Bookmarks tab is empty.

After the first launch, users are taken directly to the last tab visited. If users prefer to launch from the Catalog tab, they always can use the Catalog view.

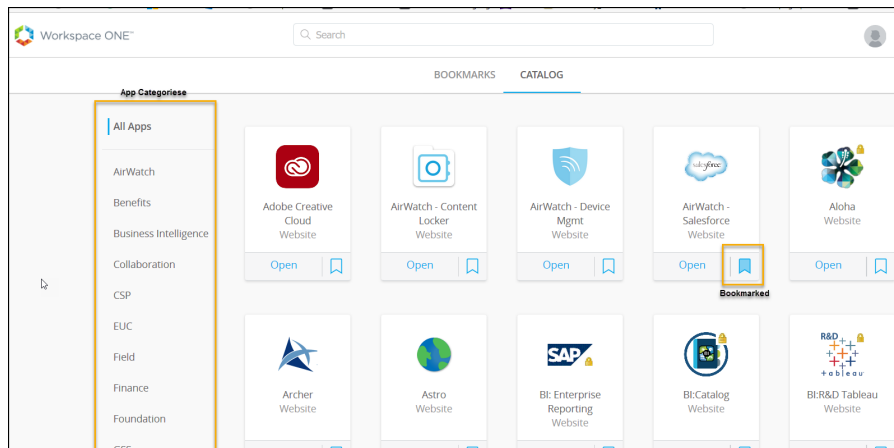
You can hide either the Catalog or the Bookmarks tab in the Workspace ONE portal to provide a user experience specific to your requirements. You can change the portal configuration from the Catalog > Settings > User Portal Configuration page.

**Figure 9-1. Initial View of Bookmarks Page**

From the catalog, users can open or install web, mobile, and virtual applications that they are entitled to. If the Bookmark tab is not hidden, users can select the ribbon icon to bookmark the application.

In the catalog pages, you can organize applications into logical categories to make it easier for users to locate the resources they need. One category, called Recommended, is listed by default. When you categorize applications as Recommended, you can enable **Show recommended apps in Bookmarks Tab** to prepopulate the Bookmarks page with these apps.

With this configuration, users are offered immediate access to recommended applications when they first sign in to the Workspace ONE portal.

**Figure 9-2. Workspace ONE Catalog Page**

**Note** Mobile applications are not available from the desktop browsers.

Users can launch web applications as follows.

- From the Bookmarks tab. Users click the application icon to launch the application.
- From the Catalog tab. Users click the box with the arrow icon to open the application.



- From Spotlight Search or Search within Workspace ONE. From the Spotlight Search on iOS devices, users select the application icon from the list. From the Workspace ONE search, users click the box with the arrow icon to open the application.

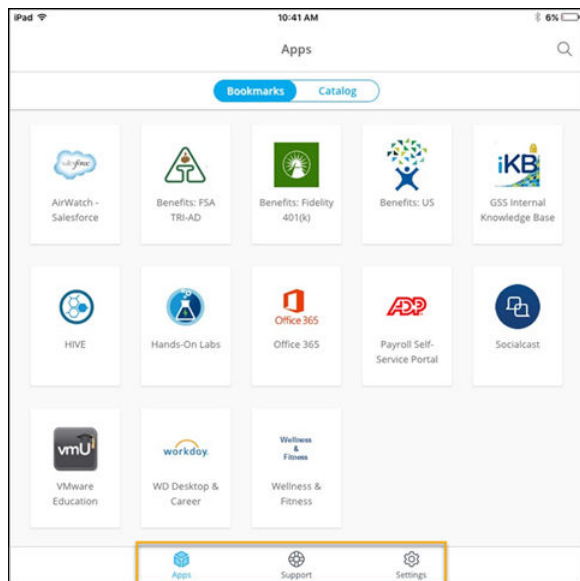
To launch installed native applications, users click the application icon in the iOS springboard.

Users can access the Workspace ONE settings from the drop-down arrow next to their name.

- Account. The profile information for the user, including their name, user name, and email address.
- Devices. The list of devices that have signed into the Workspace ONE application and the last login date and time.
- Application Tips. Tips about navigating Workspace ONE from the user's device.
- About. Workspace ONE copyright, patent, and license information.
- Preferences. The default launch setting when Horizon remote applications are accessed, either view the application from the Horizon Client or from a browser.

Users tap the Workspace ONE app icon on their devices to sign in to their apps portal. If they have bookmarked applications, the Bookmarks page displays. The Workspace ONE application on devices includes links to Support and to Settings.

**Figure 9-3. Device View of Workspace ONE Portal**



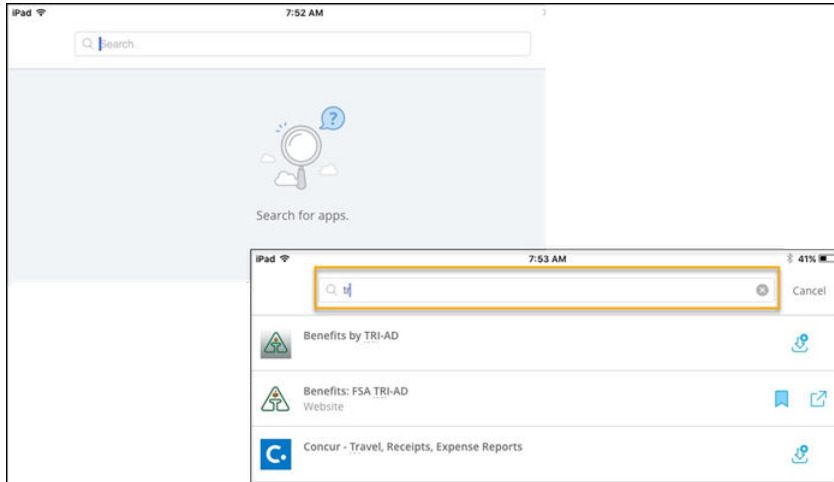
- The Support page includes a link to Devices and to Send Report. The Devices page shows when they last logged in to the device. Send Report offers the user a way to send diagnostics information or other feedback to you. Users can turn this feature off or on from their device settings.
- The Settings page shows the version of the Workspace ONE app and the VMware Workspace privacy policy. Users can remove the account from the Settings page to log out of the Workspace ONE application.

## Using Search in Workspace ONE

Users can use search in Workspace ONE to find applications by name or by category.

As users type in the search text box, applications that match the input display.

**Figure 9-4. Search Showing Results**



Users can launch a web app or download a native app directly from the search results.

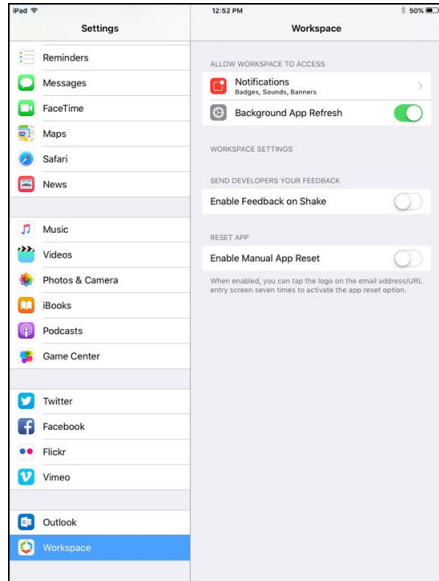
On iOS devices, users can use Spotlight to search for applications that are in the Workspace ONE portal. From the home screen on the iOS device, users touch their finger to the screen and drag down to reveal the Spotlight search field. When they enter an app name that is in their Workspace ONE portal, Workspace ONE opens and the application is launched.

## Helping Users Report Issues from iOS Devices

For iOS devices, the Rage Shake feature can be used to send logs to iOS app developers.

Users shake their device and the device logs its current state and sends details in an email message to the Workspace ONE application developers by default. Users can manually enter another email address to send the information to another address.

Users can turn on the Enable Feedback on Shake feature from the Settings > Workspace page on their device. Users can use Rage Shake from any screen in the Workspace ONE portal to send a report.

**Figure 9-5. Enable Feedback on Shake Feature**

When an iOS device receives an error message that reads similar to this device is registered to another user or environment, the Manual App Reset option can be used to clear out all app data that is stored locally on the device.

## 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 and Android 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.

## 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.

## Using VMware Verify for User Authentication

When the VMware Verify service is enabled as the second authentication method for two-factor authentication to sign in to Workspace ONE from their device, users must download the VMware Verify app from the device app store.

The first time users sign in to the Workspace ONE application, users are asked to enter their user name and password. When the user name and password are verified, users are prompted to enter their device phone number to enroll in the VMware Verify service.

When they click **Enroll**, the device phone number is registered with the VMware Verify service. If they have not downloaded the VMware Verify application, they are asked to download the application.

When the application is installed, users are asked to enter the same phone number that was entered before and to select a notification method to receive a one-time registration code. The registration code is entered on the registration pin page.

After the device phone number is registered, users can use a time-based one-time passcode displayed in the VMware Verify application to sign in to Workspace ONE. The passcode is a unique number that is generated on the device and is constantly changing.

Users can register more than one device. The VMware Verify passcode is automatically synchronized to each of the registered devices.

## Send Alerts to Workspace ONE Users

Admins can notify Workspace ONE users for upcoming system downtimes, compliance status, to request actions, or to send alerts. Notification can be sent via the AirWatch admin console. Can be viewed as device notification or in-app notification.

## Working with Workspace ONE for Android Devices

The following types of applications can be enabled through the Android Workspace ONE application.

- Web applications
- Remote applications that are enabled in the VMware Identity Manager service. For example, Horizon virtual applications, Citrix XenApp, and ThinApp.
- Native applications, both managed and unmanaged. Native applications are Android apps developed for Android platform. Two types are available.
  - Public applications that are distributed from the Google Play Store.

- Internal applications that are privately distributed through AirWatch and are not available from the Google Play Store.

Web applications open in a browser. Users can access virtual applications through either VMware Horizon Client or the Citrix Receiver.

## Registering Workspace ONE

Signing into Workspace ONE with a valid server URL and credentials allows users to access the Workspace ONE unified catalog. In the unified catalog, users can view all the applications that are assigned to them.

Users must register Workspace ONE to access the applications. In the Workspace ONE registered state, users can use web and virtual applications that are enabled through VMware Identity Manager, AirWatch productivity apps, and SDK apps without management.

---

**Note** SDK apps are containerized and managed through the AirWatch SDK and do not require the device to be managed.

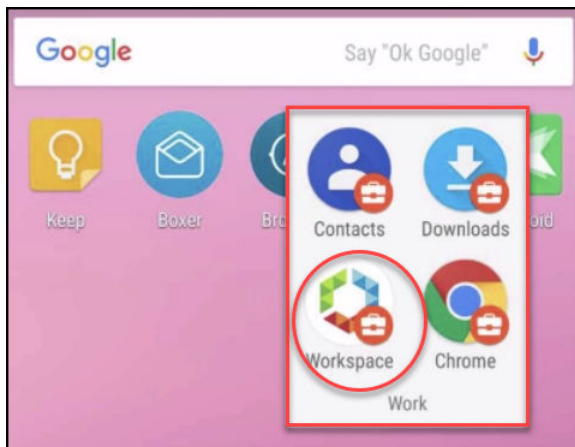
---

Users can initiate adaptive management, which enables Android for Work on the device and allows profiles, policies, and improved app distribution for the device.

## Managing Android for Work with Workspace ONE

Enabling Android for Work on devices separates personal data from the work data at the operating system level. Android for Work creates a clear separation between work and personal apps. Android for Work creates the work applications with a distinct Android work badge.

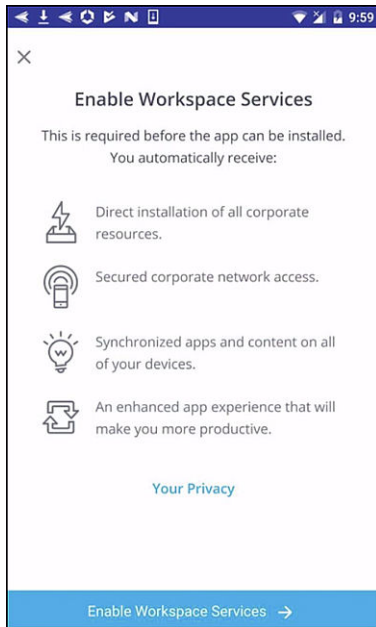
**Figure 9-6. Android for Work Content**



The admins determine which applications in the catalog require a device to be managed before the app can be accessed. Applications in the catalog that require management display a distinct star symbol next to the download button.

When users try to download one of these applications, they receive a message that the application requires the device to be managed. A screen displays that describes the features and benefits of device management.

**Figure 9-7. Workspace Services Introduction Page**



When users agree to enable Android for Work management, users are guided through the process to set up management. After the device is managed, the Android for Work container is created on the device.

# Using the Workspace ONE Catalog

# 10

When AirWatch and VMware Identity Manager are integrated, the Workspace ONE app catalog is the repository of all the resources that you can entitle to users. Users can access enterprise applications that you manage in the Workspace ONE catalog based on the settings you establish for the application.

Cloud, Mobile, and Windows applications can be accessed from the catalog. Native applications that are internally developed or publicly available in app stores can be made available to your end users from the Workspace ONE portal.

In the Workspace ONE Catalog pages, you can perform the following tasks

- Add new resources to your catalog
- View the resources to which you can currently entitle users
- Access information about each resource in your catalog

Some web application can be added to your catalog directly from the Catalog pages. Other resource types require you to take action outside the administration console. See the VMware Identity Manager *Setting Up Resources* guide for information about setting up resources.

## Managing Resources in the Catalog

Before you can entitle a particular resource to your users, you must populate your catalog with that resource. The method you use to populate your catalog with a resource depends on what type of resource it is.

The types of resources that you can define in your catalog for entitlement and distribution to users are Web applications, Windows applications captured as VMware ThinApp packages, Horizon Client desktop pools and Horizon virtual applications, or Citrix-based applications.

To integrate and enable Horizon Client desktop and application pools, Citrix-published resources, or ThinApp packaged applications, you use the Virtual Apps Collection feature available in the Catalog tab drop-down menu.

For information, requirements, installation, and configuration of these resources, see *Setting Up Resources in VMware Identity Manager*.

## Adding Web Applications to Your Organization's Catalog

You can add your organization's Web applications to your catalog and make these applications accessible to your users and groups.

You populate your catalog with Web applications directly on the Catalog page of the administration console. When you click a Web application displayed on the Catalog page, information about that application is displayed. From the displayed page, you can configure the Web application, such as by providing the appropriate SAML attributes to configure single sign-on between VMware Identity Manager and the target Web application. When the Web application is configured, you can then entitle users and groups to that Web application.

When you add an entry for a Web application to the catalog, you create an application record and configure the address of the Web application. The VMware Identity Manager service uses the application record as a template to establish a secure connection with the Web application.

The following methods can be used to add application records of Web applications to your catalog from the Catalog tab.

Method	Description
From the cloud application catalog	Popular enterprise Web application types are listed in the cloud application catalog. These federated applications are partially configured. You must complete the rest of the application record form.
Create a new one	You can add Web applications to your catalog that are not listed in the cloud application catalog. Non-federated applications are created as new applications. The application records for these Web applications are more generic than that of cloud application catalog applications. You enter the application description and configuration information to create the application record.
Import a ZIP or JAR file	You can import a Web application that you previously configured in the service. You might want to use this method to move a deployment from staging to production. In such a situation, you export a Web application from the staging deployment as a ZIP file. You then import the ZIP file to the production deployment.

After you add Web applications to the catalog, you can configure entitlements, access policies, licensing, and provisioning information.

## Grouping Resources into Categories

You can organize resources into logical categories to make it easier for users to locate the resource they need in their Workspace ONE portal.

When you create categories consider the structure of your organization, the job function of the resources, and type of resource. You can assign more than one category to a resource. For example, you might create a category called Sales Associate and another category called Staff Sales Resources. Assign Sales Associate to all the sales resources in your catalog. Also assign Staff Sales Resources to specific sales resources that are shared with only the staff associates.

After you create a category, you can apply that category to any of the resources in the catalog. You can apply multiple categories to the same resource.



When users sign in to their Workspace ONE portal, they see the categories that you enabled for their view.

See the VMware Identity Manager Administration guide, [Managing the Catalog](#).

# Custom Branding for VMware Identity Manager Services

11

You can customize the logos, fonts, and background that appear in the administration console, the user and administrator sign-in screens, the Web view of the Workspace ONE applications portal, and the Web view of the Workspace ONE application on mobile devices.

You can use the customization tool to match the look and feel of your company's colors, logos, and design.

This chapter includes the following topics:

- [Customize Branding in VMware Identity Manager Service](#)
- [Customize Branding for the User Portal](#)

## Customize Branding in VMware Identity Manager Service

You can add your company name, product name, and favicon to the address bar for the administration console and the user portal. You can also customize the sign-in page to set background colors to match your company's colors and logo design.

### Procedure

- 1 In the administration console Identity & Access Management tab, select **Setup > Custom Branding**.
- 2 Edit the following settings in the form as appropriate.

Form Field	Description
Names and Logos Tab	
Company Name	Company Name applies to both desktops and mobile devices. You can add your company's name as the title that appears in the browser tab. Enter a new company name over the existing one to change the name.
Product Name	Product Name applies to both desktops and mobile devices. The product name displays after the company name in the browser tab.
Favicon	A favicon is an icon associated with a URL that is displayed in the browser address bar. The maximum size of the favicon image is 16 x 16 px. The format can be JPEG, PNG, GIF, or ICO. Click <b>Upload</b> to upload a new image to replace the current favicon. You are prompted to confirm the change. The change occurs immediately.
Sign-In Screen Tab	

Form Field	Description
Logo	Click <b>Upload</b> to upload a new logo to replace the current logo on the sign-in screens. When you click <b>Confirm</b> , the change occurs immediately.  The minimum image size recommended to upload is 350 x 100 px . If you upload images that are larger than 350 x 100 px, the image is scaled to fit 350 x 100-px size. The format can be JPEG, PNG, or GIF.
Background Color	The color that displays for the background of the sign-in screen. Enter the six-digit hexadecimal color code over the existing one to change the background color.
Box background color	The sign-in screen box color can be customized. Enter the six-digit hexadecimal color code over the existing code.
Login button background color	The color of the login button can be customized. Enter the six-digit hexadecimal color code over the existing one.
Login button text color	The color of the text that displays on the login button can be customized. Enter the six-digit hexadecimal color code over the existing one.

When you customize the sign-in screen, you can see your changes in the Preview pane before you save your changes.

### 3 Click **Save**.

Custom branding updates to the administration console and the sign-in pages are applied within five minutes after you click Save.

#### What to do next

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

Update the appearance of the end-user Workspace ONE portal and mobile and tablet view. See [Customize Branding for the User Portal](#)

## Customize Branding for the User Portal

You can add a logo, change the background colors, and add images to customize the Workspace ONE portal.

#### Procedure

- 1 In the 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 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	

Form Item	Description
Masthead Background Color	Enter a six-digit hexadecimal color code over the existing one to change the background color of the masthead. The background color changes in the application portal preview screen when you type in a new color code.
Masthead Text Color	Enter a six-digit hexadecimal color code over the existing one to change the color of the text that displays in the masthead.
Background Color	<p>The color that displays for the background of the Web portal screen.</p> <p>Enter a new six-digit hexadecimal color code over the existing one to change the background color. The background color changes in the application portal preview screen when you type in a new color code.</p> <p>Select <b>Background Highlight</b> to accent the background color. If Background Highlight is enabled, browsers that support multiple background images show the overlay in the launcher and catalog pages.</p> <p>Select <b>Background Pattern</b> to set the predesigned triangle pattern in the background color.</p>
Icon Background Color	Enter a six-digit hexadecimal color code to change the background color box surrounding application icons.
Icon Background Opacity	To set a transparency, move the slider on the bar.
Name and Icon Color	<p>You can select the text color for names listed under the icons on the app portal pages.</p> <p>Enter a hexadecimal color code over the existing one to change the font color.</p>
Lettering effect	Select the type of lettering to use for the text on the Workspace ONE portal screens.
Background Highlight	If enabled, for browsers that support multiple background images, the background overlay displays in the bookmark and catalog pages.
Background Pattern	If enabled, for browsers that support multiple bg images, the background overlays display in the bookmark and catalog pages.
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

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

## Accessing Other Documents

When setting up Workspace ONE, you might need to reference documentation for both VMware Identity Manager and VMware AirWatch.

For a complete list documentation for AirWatch 9.2 release, navigate to [https://my.air-watch.com/help/9.2/en/Content/Release\\_Notes/Doc\\_List\\_PDFs.htm](https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm).

For general AirWatch documentation, you can navigate to [AirWatch Resources on my AirWatch](#) and search for other versions of the documentation.

For general VMware Identity Manager documentation, you can navigate to <https://docs.vmware.com/en/VMware-Identity-Manager/index.html>.