VMware Workspace ONE Quick Start Guide

MAR 2018

VMware Identity Manager 3.2

VMware AirWatch 9.3

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

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

Contents

About Workspace ONE Getting Started

The *VMware Workspace ONE Quick Start Guide* guides you through using the VMware Workspace ONE™ Getting Started Wizards in the AirWatch administrator's console.

This guide details how to deploy key features of Workspace ONE, including configuring single sign-on (SSO), conditional access, and policies.

Intended Audience

This information is intended for administrators who will be deploying Workspace ONE for mobile SSO and device management. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Using the Workspace ONE Getting Started Wizard

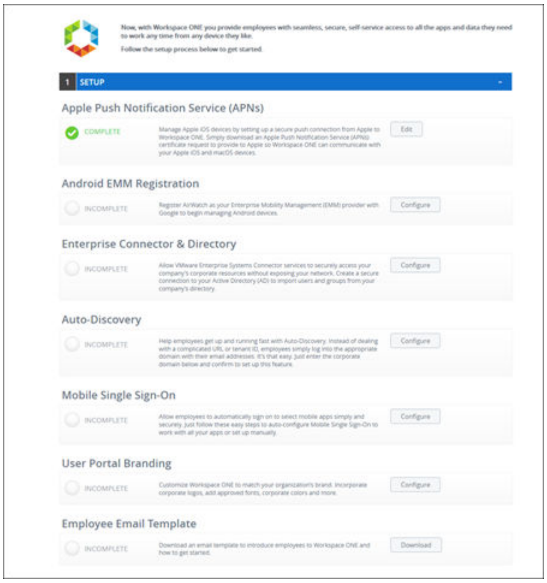
1

The Workspace ONE Getting Started wizards guide you through the configuration steps to integrate VMware AirWatch and VMware Identity Manager services to create the Workspace ONE environment.

The Workspace ONE wizard tracks how far along you are in the configuration process. The wizards can be started, paused, restarted later. You can review the configuration and change responses when necessary.

- Android EMM Registration. The wizard walks you through the steps to register AirWatch as your EMM provider for Android devices with Google.
- Enterprise Connector & Directory. The wizard walks you through the steps to set up the VMware Enterprise System Connector and configure the Active Directory connection to import users and groups from your company 's directory.
- Mobile Single Sign-on. The wizard runs through a series of steps to configure all settings for mobile single sign-on to iOS, Android, and Windows 10 devices.
- User Portal Branding. The wizard opens the User Portal Branding page in the VMware Identity Manager admin console where you can customize logos, fonts, and background details for the Workspace ONE application.

Figure 1-1. Workspace ONE Getting Started Wizards



Now, with Workspace ONE you provide employees with seamless, secure, self-service access to all the apps and data they need to work any time from any device they like.

Follow the setup process below to get started.

1 SETUP

Apple Push Notification Service (APNs)

COMPLETE — Manage Apple iOS devices by setting up a secure push connection from Apple to Workspace ONE. Simply download an Apple Push Notification Service (APNs) certificate request to provide to Apple so Workspace ONE can communicate with your Apple iOS and macOS devices. — Edit

Android EMM Registration

INCOMPLETE — Register AirWatch as your Enterprise Mobility Management (EMM) provider with Google to begin managing Android devices. — Configure

Enterprise Connector & Directory

INCOMPLETE — Allow VMware Enterprise Systems Connector services to securely access your company's corporate resources without exposing your network. Create a secure connection to your Active Directory (AD) to import users and groups from your company's directory. — Configure

Auto-Discovery

INCOMPLETE — Help employees get up and running fast with Auto-Discovery. Instead of dealing with a complicated URL or tenant ID, employees simply log into the appropriate domain with their email addresses. It's that easy. Just enter the corporate domain below and confirm to set up this feature. — Configure

Mobile Single Sign-On

INCOMPLETE — Allow employees to automatically sign on to select mobile apps simply and securely. Just follow these easy steps to auto-configure Mobile Single Sign-On to work with all your apps or set up manually. — Configure

User Portal Branding

INCOMPLETE — Customize Workspace ONE to match your organization's brand. Incorporate corporate logos, add approved fonts, corporate colors and more. — Configure

Employee Email Template

INCOMPLETE — Download an email template to introduce employees to Workspace ONE and how to get started. — Download

Apple Push Notification service (APNs) is the messaging protocol created by Apple to manage mobile devices. It requires that the MDM provider has a valid APNs certificate configured. Configuring APN is a prerequisite to managing iOS devices. To set up a secure push connection from Apple, see Generating and Renewing an APNS Certificate guide in resources.air-watch.com.

To set up auto-discovery, follow the directions in the Auto Discovery configuration page. Configuring auto-discovery is not required to configure and use Workspace ONE.

The Getting Started wizard might alert you if existing, potentially conflicting, configurations are already enable in AirWatch or the VMware Identity Manager service. If this occurs, or the getting started wizard only partially completes the steps, features can be configured manually. 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

Navigate to the Workspace ONE Getting Started Menu

Access the Workspace ONE Getting Started page from the main menu in the AirWatch admin console.

1 Select your organization group from the Global list.

2 Click **Getting Started** in the left navigation pane.

3 In the Getting Started > Workspace ONE section, click **Start Wizard**.

Configuring Enterprise System Connector 2

The Enterprise Connector & Directory setup wizard walks you through the steps to set up the VMware Enterprise Systems Connector to allow the components of Workspace ONE, AirWatch, and VMware Identity Manager to communicate with your Active Directory.

Installing the full VMware Enterprise Systems Connector, including the identity manager component, is the recommended configuration. The VMware Identity Manager service uses the identity management directory synchronization channel in the connector, instead of the AirWatch's ACC channel. This option provides the best compatibility with advanced active directory environments.

This chapter includes the following topics:

Configure Enterprise System Connector

VMware Enterprise System Connector configuration is always required for SaaS customers. On-premises customers might require this connector depending on their network architecture. Consult the VMware AirWatch Reference Architecture guide for recommendations and more information.

Prerequisites

To install the Enterprise System Connector, the following is required. See the *VMware Enterprise Systems Connector Installation and Configuration* guide for prerequisites and other detailed information.

- Secure Channel Certificate installed to establish security between AWCM and AirWatch Console, Device Services, API, and the Self-service Portal
- Log in to the VMware Identity Manager admin console as the local administrator and generate an activation code.

  a Go to the **Identity & Access Management > Setup** tab.

  b On the Connectors page, click **Add Connector**. Enter the name for the connector.

  c Click **Generate Activation Code**.

  d Copy the activation code and save it to use when you set up the connector.

Procedure

1 Log into the AirWatch console with the admin password. If necessary, create a password.

2 Accept the terms of use and set up the password recovery questions and security PIN.

3 For on-premises deployments, either create or select the customer-level organization group to run the wizard.

The customer-level organization group is the only level where the Getting Started wizard is available.

4 Select **Getting Started > Workspace ONE**.

5 In the Enterprise Connector & Directory section, click **Configure**.

6 To download the VMware Enterprise Systems Connector, create a password and click **Download VMware Enterprise Systems Connector Installer.**

To install the AirWatch ACC channel, click **Skip** and complete the ACC directory setup. See Creating ACC Active Directory.

7 Run the VMware Enterprise Systems Connector installer. Review the install shield wizard steps.

8 After the installation of the connector is finished, click **Test Connection**.

9 Click **Continue**.

The Settings > Enterprise Integration > Directory Services page is displayed.

10 If asked, select **Add Active Directory over LDAP/IWA**.

11 Enter the Active Directory server details.

Option	Description
Directory Name	Add a name to identify this directory.
Directory Type	Select **Active Directory over LDAP**.
Directory Sync and Authentication	Select the connector you installed. This connector syncs with Active Directory. Authentication is set to **Yes**. The Directory Search Attribute is usually set to **sAMAccountName**.
Server Location	Select this box to use the DNS Service Location records to locate the Active Directory domains. If you do not use DNS Service Location lookup, deselect the check box and enter the Active Directory server host name and port. The default port number is 389.

Option	Description
Certificates	If your Active Directory requires STARTTLS encryption, select the check box below and provide the Root CA certificate. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory.
Bind User Details	**Base DN** Enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. **Bind DN** Enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Bind DN Password** Enter the bind account password. Using a Bind DN user account with a non-expiring password is recommended.

12 Click **Test Connection** to verify connectivity.

13 Click **Save**.

What to do next

For directory service with VMware Identity Manger, review the user attributes that sync from Active Directory and select groups and users to sync.

- Go to the VMware Identity Manager admin console, Identity & Access Management page, Setup > User Attributes to verify users and group attributes.
- To manage the sync settings including adding users and groups, go to the Manage > Directories page and select the directory's Sync Settings view.

Run the Mobile Single Sign wizard to configure mobile SSO for iOS, Android, and Windows 10 devices.

Creating ACC Active Directory

Configuring ACC is a simple, but feature limited implementation. You set up a connection to the Active Directory to sync users and groups to the AirWatch directory.

Procedure

1 Select the Enterprise Connector & Directory wizard and to install the AirWatch ACC channel, click **Skip** and complete the ACC directory setup.

2 In the Directory Setup page, enter the Active Directory server details for ACC.

Option	Description
Directory Type	Active Directory is selected.
Server	Enter the host name or IP address of your directory server. For example, type the host name as `myco.example.com`.
Encryption Type	Select the encryption used for directory services communication, None, SSL, or Start TLS.
Port	Enter the TCP port that is used to communicate with the domain controller. The default port number is 389.

Option	Description
Protocol Version	Enter the version of the LDAP protocol that is in use. The version is either 2 or 3. If you are unsure of which protocol version to use, leave the value as 3.
Bind Authentication Type	Select the type of bind authentication that is used to enable the AirWatch server to communicate with the domain controller. The commonly used value is GSS-NEGOTIATE.
Bind Username	Enter the bind account user name to authenticate with the directory server.
Bind Password	Enter the bind account password.
Domain	Enter the default domain and server name for the directory-based user account.

3 Click **Save**.

4 Click **Test Connection** to verify connectivity.

What to do next

For directory service with ACC, go to the System > Enterprise Integration > Directory Services pages to configure users and groups, if not previously configured.

Run the Mobile Single Sign wizard to configure mobile SSO for iOS, Android, and Windows 10 devices.

Managing Access Policies to Apply to Users

To provide secure access to the users' Workspace ONE apps 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 to the apps portal and to use resources.

Access policies allow administrators to configure features such as mobile single sign-on, conditional access to applications based on enrollment, and compliance status, step up, and multi factor authentication.

Policy rules map the requesting IP address to network ranges and designate the type of devices that users can use to sign in. The rule defines the authentication methods and the number of hours the authentication is valid. You can select one or more groups to associate with the access rule.

A broad range of configuration options are available, but this quick start guide describes enterprise mobility managed and unmanaged tier of application access.

The default access policy is configured when you run the Configure Mobile Single Sign-on wizard to allow access to all devices types that were configured. This policy is considered as level 1 access for applications that can be accessed by unmanaged devices.

You can create policies for applications that require restricted access from managed compliant devices. VMware Identity Manager provides various built-in authentication adapters to accomplish this experience. When mobile single sign-on is configured, these authentication methods are enabled.

- Mobile SSO (for iOS). Kerberos-based adapter for iOS Devices
- Mobile SSO (for Android). Specially tailored implementation of certificate auth for Android

- Certificate (Cloud Deployment). Certificate authentication service aimed at Web browsers and desktop devices
- Password. Allows for authentication of directory passwords with a single connector when VMware Identity Manager and AirWatch are deployed together with both components of the VMware Enterprise Systems Connector
- Password (AirWatch Connector). Allows for authentication of directory passwords with a single connector when VMware Identity Manager and AirWatch are deployed together using only ACC
- Device Compliance (with AirWatch). Measures the health of managed devices resulting in a pass or fail based on AirWatch defined criteria. Compliance can be chained with any other built-in adapter except password

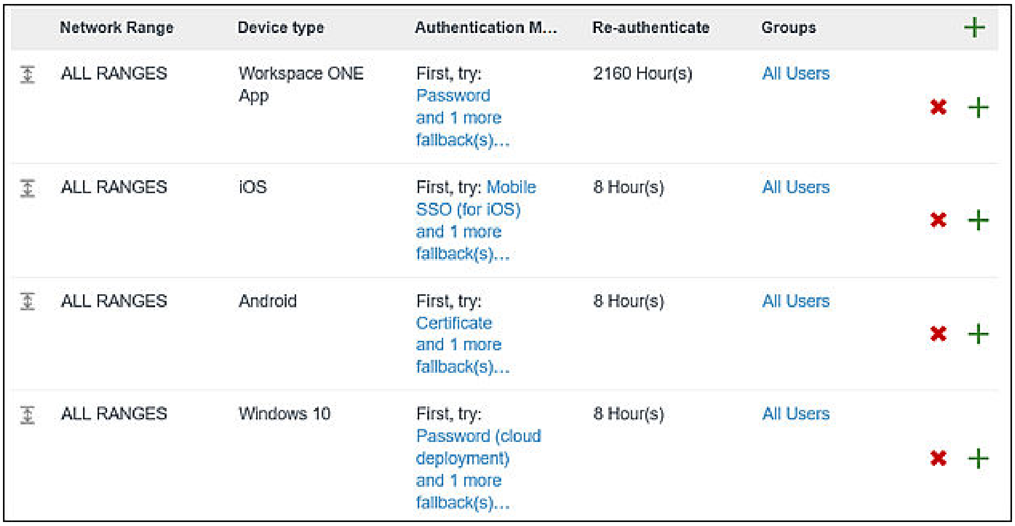
Level 1 Default Access Policy for Unmanaged Devices

Use the default access policy as a baseline L1 policy to access all applications. When mobile single sign-on is configured, access rules are created for iOS, Android, and Windows 10 devices. Each device is enabled for single sign-on using the authentication method specific to that device. In each rule, the fallback method is password. This setup provides the best experience to manage devices, while still providing a manual sign-in option for unmanaged devices.

The default policy is configured to allow access to all network ranges. The session timeout is eight hours.

You might want to further secure access for unmanaged devices with VMware Verify or other multi factor authentication.

Figure 2-1. Example of the Default Policy for Unmanaged Devices



Network Range	Device type	Authentication M...	Re-authenticate	Groups	+
ALL RANGES	Workspace ONE App	First, try: Password and 1 more fallback(s)...	2160 Hour(s)	All Users	✖ +
ALL RANGES	iOS	First, try: Mobile SSO (for iOS) and 1 more fallback(s)...	8 Hour(s)	All Users	✖ +
ALL RANGES	Android	First, try: Certificate and 1 more fallback(s)...	8 Hour(s)	All Users	✖ +
ALL RANGES	Windows 10	First, try: Password (cloud deployment) and 1 more fallback(s)...	8 Hour(s)	All Users	✖ +

When mobile single-sign on wizard is used to configure mobile SSO, the default access policy rules reflect this level of access control.

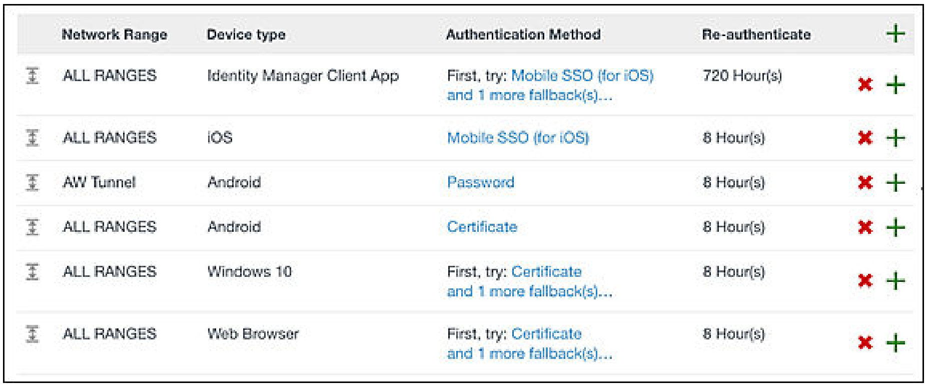
Configuring Level 2 Policies for Managed Devices

If your organization deploys applications that contain sensitive data, you can restrict access to these applications to only MDM-managed devices. Managed devices can be tracked and wiped, if necessary, and enterprise data are removed when the device is unenrolled.

To enforce this managed requirement on a selection of applications, you create application-specific policies for these applications. When you create the policy, in the **Applies to** section you select the applications that apply to this policy.

Create a policy rule for each device platform in your deployment. Define the correct SSO authentication method. However, because unmanaged devices should not access these applications, do not define a fallback authentication method. For example, if an unmanaged iOS device tries to connect to an application configured only for managed devices access, the device does not respond with the appropriate Kerberos wrapped certificate. The authentication attempt fails, and the user is not able to access the content.

Figure 2-2. Example of Level 2 Access Policy for Managed Devices



Network Range	Device type	Authentication Method	Re-authenticate	+
ALL RANGES	Identity Manager Client App	First, try: Mobile SSO (for iOS) and 1 more fallback(s)...	720 Hour(s)	✖ +
ALL RANGES	iOS	Mobile SSO (for iOS)	8 Hour(s)	✖ +
AW Tunnel	Android	Password	8 Hour(s)	✖ +
ALL RANGES	Android	Certificate	8 Hour(s)	✖ +
ALL RANGES	Windows 10	First, try: Certificate and 1 more fallback(s)...	8 Hour(s)	✖ +
ALL RANGES	Web Browser	First, try: Certificate and 1 more fallback(s)...	8 Hour(s)	✖ +

Set Up AirWatch Enterprise Mobility Management on Google for Android

3

To manage Android devices in Workspace ONE, you must register AirWatch as the Enterprise Mobility Management (EMM) provider with Google. The wizard walks you through the steps to register AirWatch as the EMM provider.

Note If you are deploying the G Suite, see the VMware AirWatch Integration with Android for Work Guide for configuration details.

Prerequisites

A Google user account.

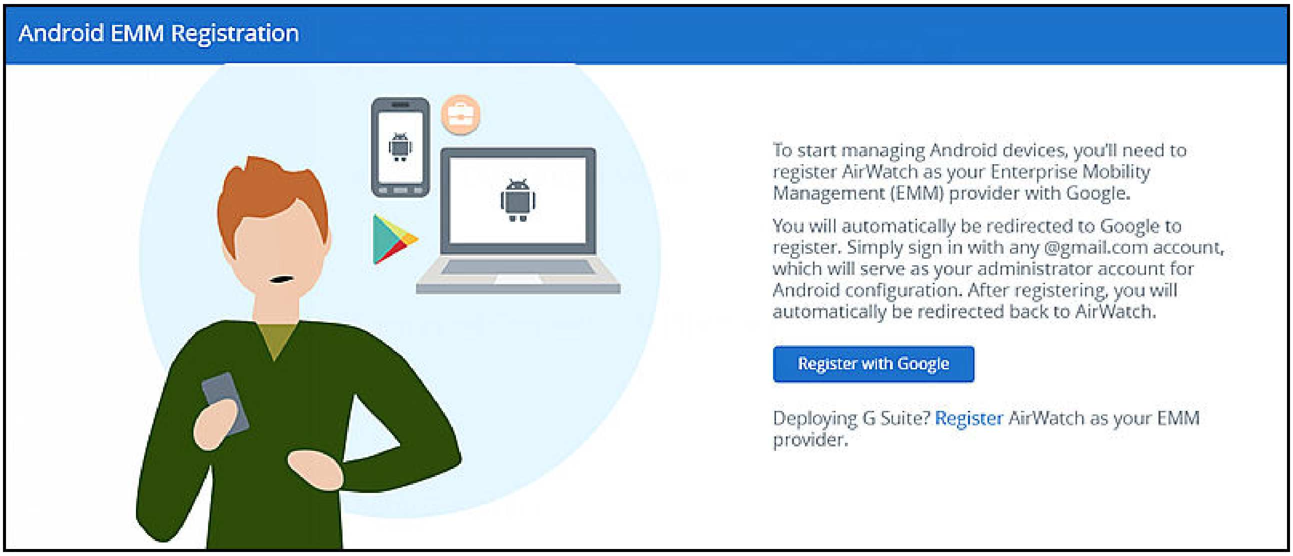
Procedure

1 Select the organization group for Workspace ONE from the Global list.

2 Click **Getting Started** in the left navigation pane.

3 In the Getting Started > Workspace ONE section, click **Start Wizard**.

4 In the Android EMM Registration section, click **Configure**.



Android EMM Registration

To start managing Android devices, you'll need to register AirWatch as your Enterprise Mobility Management (EMM) provider with Google.

You will automatically be redirected to Google to register. Simply sign in with any @gmail.com account, which will serve as your administrator account for Android configuration. After registering, you will automatically be redirected back to AirWatch.

Deploying G Suite? Register AirWatch as your EMM provider.

5. Click **Register with Google**.

   You are redirected to Google Play to add your organization name. The EMM provider is already populated with AirWatch.

6. Complete the configuration on the page and click **CONFIRM**.

7. Click **COMPLETE REGISTRATION**.

   You are returned to the AirWatch admin console, Android for Work page. The Google Admin Console and API settings have been added to the page.

8. Click **Save** and then **Test Connection**.

You are now ready to enroll Android devices using Android Enterprise.

Configuring Mobile Single Sign-On

4

Mobile single sign-on lets users automatically sign on to selected mobile applications simply and securely.

The devices that are configured for mobile single sign-on (SSO) are iOS version, Android, and Windows 10.

iOS Single Sign-On Component Configuration

Mobile single sign-on for iOS uses the PKINIT Kerberos protocol for certificate transport, but does not require on premises infrastructure. A built-in Kerberos adapter is available in the identity manager service, which can handle iOS authentication without the need for device communication to your internal domain controller. In addition, AirWatch can distribute identity certificates to devices, eliminating the requirement to maintain an on-premises CA.

Supported Devices

- iOS Version 9 and later

Android Single Sign-On Component Configuration

Workspace ONE offers universal Android mobile single sign-on. Mobile single sign-on allows users to sign in to enterprise applications securely, without the need for a password. The VMware Tunnel mobile application is installed on Android devices to add certificates and device ID information into authentication flows. This solution supports both classic Android management and Android for Work.

Supported Devices

- Android 5 and later
- Applications must support SAML or another supported federation standard

Mobile single sign-on authentication for Android devices can be configured to bypass the Tunnel server when VPN access is not required. For single sign-on, only the Tunnel mobile application is required.

Deploying the Workspace ONE application to all Android devices does not automatically deploy the application Android for Work containers. Android for Work is required to use the Workspace ONE application Adaptive Management feature. To add this application to Android for Work devices as well and for more detail on the additional options available as part of AirWatch MAM, review the VMware AirWatch Integration with Android for Work guide, available on AirWatch Resources.

Windows 10 Single Sign-On Component Configuration

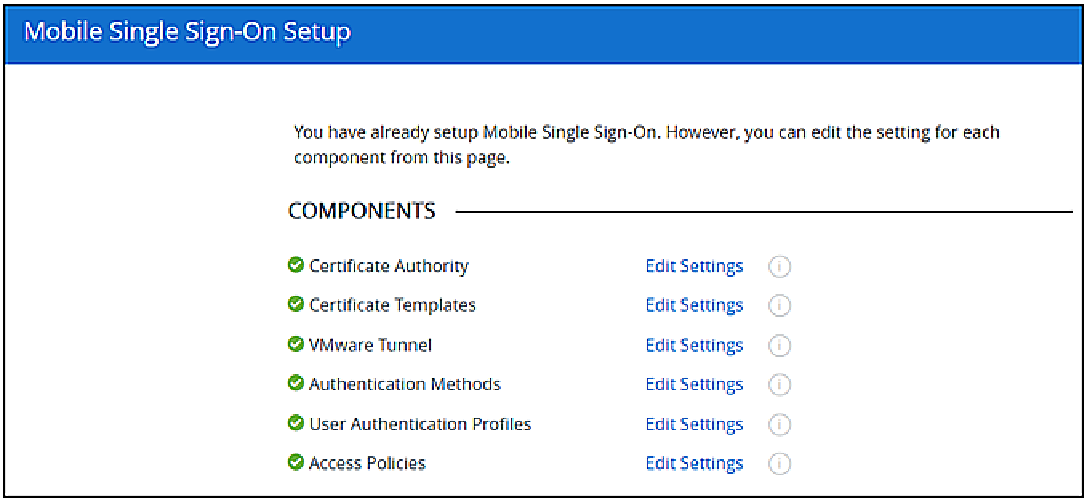
Certificate-based SSO is the recommended experience for managed Windows desktops and laptops. Cert authentication is supported on all x86-based Windows installations.

Configure Mobile Single Sign-on Wizard

Configure mobile single sign-on (SSO) to allow users from AirWatch enrolled devices to log in to their enabled application securely without entering multiple passwords.

The wizard runs through a series of steps to configure all settings for all of the supported platforms. You can edit the configuration after the wizard configuration is complete.

Figure 4-1. List of Components that are Configured



Mobile Single Sign-On Setup

You have already setup Mobile Single Sign-On. However, you can edit the setting for each component from this page.

COMPONENTS

✓ Certificate Authority	Edit Settings	ⓘ
✓ Certificate Templates	Edit Settings	ⓘ
✓ VMware Tunnel	Edit Settings	ⓘ
✓ Authentication Methods	Edit Settings	ⓘ
✓ User Authentication Profiles	Edit Settings	ⓘ
✓ Access Policies	Edit Settings	ⓘ

The wizard configuration can take some minutes. Do not refresh or navigate away from the wizard configuration page while the configuration is in progress.

You can also select individual components to configure manually.

Procedure

1 Log in to the AirWatch console with the admin password.

2 Select **Getting Started > Workspace ONE**.

3 In the Mobile Single Sign-on section, click **Configure**.

4 In the Fast and Easy Setup! page, click **Get Started** to have the wizard configure all the mobile single sign-on components for Workspace ONE.

Click **Manual Setup** to configure mobile single sign-on manually.

5 In the Get Started page, click **Continue**.

6 In the Auto-Configure page, click **Start Configuration**.

As a step is finished, a checkmark appears in front of the step.

7 Click **Finish**, when the configuration is complete.

You can click **Edit Settings** to change or review the component configuration, otherwise click **Close**.

The mobile single sign-on wizard automatically configures the following components to set up mobile single sign-on for iOS, Android for Work, and Windows 10 devices with Workspace ONE.

Table 4-1. Components Configured for Mobile Single Sign-on

Component Configured	Description	Admin Console Settings Page
Certificate Authority	A connection to the native AirWatch Certificate Authority used to issue authentication certificates for mobile SSO for managed iOS devices is set up.	AirWatch console > System > Enterprise Integration > Certificate Authorities
Certificate Templates	An AirWatch Certificate Template is pre-configured to issue certificates for mobile single sign-on.	AirWatch console > System > Enterprise Integration > Request Templates
VMware Tunnel	VMware Tunnel is configured and configures a certificate to provide local single sign-on services to third-party Android applications connected to VMware Identity Manager.	AirWatch console > System > Enterprise Integration > VMware Tunnel
Authentication Methods	The authentication methods required for mobile single sign-on are configured in the VMware Identity Manager service. These authentication methods establish a trust chain between the AirWatch Certificate Authority and the VMware Identity Manager service. The authentication methods that are configured are Mobile SSO for iOS, Mobile SSO for Android, Password (AirWatch Connector), Certificate (Cloud Deployment). In addition, Device Compliance with AirWatch is enabled.	VMware Identity Manager admin console > Identity & Access Management > Manage > Authentication Methods
User Authentication Profiles	AirWatch configuration profiles for iOS and Windows are created. The profiles are used to distribute a certificate and configure devices to authenticate with the VMware Identity Manager service.	AirWatchconsole > Devices > Profiles & Resources > Profiles
Access Policies	The default access policy in the VMware Identity Manager service is configured with access rules for each iOS device, Android devices, and Windows 10 devices. Users authenticate using mobile single sign-on for managed devices. See Managing Access Policies to Apply to Users.	VMware Identity Manager admin console > Identity & Access Management > Manage > Policies

What to do next

- For iOS devices, the services must be integrated with Kerberos. This authentication method for iOS devices uses a Key Distribution Center (KDC) without the use of a third-party system. For on-premises deployments, two KDC options are available. KDC as a VMware identity Manager cloud hosted service and a built-in KDC on the appliance. This is configured from the VMware Identity Manager admin console. See Using a Key Distribution Center for Authentication from iOS Devices.
- Enable VPN for each Android app that uses the application tunnel functionality from the AirWatch admin console.

- Publish the iOS profile to enable SSO from the AirWatch admin console. The profile is generated, but not automatically published.
- For Windows deployments, the certificate for cloud deployment must be configured manually. This is configured from the VMware Identity Manager admin console. See the VMware Identity Manager Administration guide.
- Create access policies for applications that require restricted access from managed devices. See Managing Access Policies to Apply to Users.

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.

Customize Workspace ONE User Portal

5

The User Portal Branding wizard directs you to the Workspace ONE User Portal Branding page on the VMware Identity Manager admin console. you can customize the logos, fonts, and background appearance in the Workspace ONE portal to match the look and feel of your company's colors, logos, and design.

Prerequisites

VMware Identity Manager service configured.

Procedure

1 Log in to the AirWatch console with the admin password.

2 Select **Getting Started > User Portal Branding**.

You are directed to the identity manager admin console. If you are not logged into the identity manager admin console, the sign-in screen displays. Enter the VMware Identity Manager admin name and password and navigate to the Catalog > Settings > User Portal Branding page.

If you are already logged in, the User Portal Branding page displays.

3 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 Workspace ONE portal web pages. The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG or GIF.
	Portal
Masthead Background Color	Enter a 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.

Form Item	Description
Background Color	The color that displays for the background of the Web portal screen. Enter a new six-digit hexadecimal color code over the existing one to change the background color. The background color changes in the application portal preview screen when you type in a new color code. Select **Background Highlight** 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. Select **Background Pattern** to set the predesigned triangle pattern in the background color.
Icon Background Color	Enter a six-digit hexadecimal color code to change the background color box surrounding application icons.
Icon Background Opacity	To set transparency, move the slider on the bar.
Name and Icon Color	You can select the text color for names listed under the icons on the app portal pages. Enter a hexadecimal color code over the existing one to change the font color.
Lettering effect	Select the type of lettering to use for the text on the 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 background images, the pattern 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.

4 Click **Save**.

Review the appearance of the branding changes. 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.