VMware Workspace ONE Quick Configuration Guide

VMware AirWatch 9.1

APRIL 2017 V2

vmware

Revision Table

The following table lists revisions to this guide since the April 2017 release

Date	Reason
April 2017	Initial release
June/July, 2017	• Removed the optional steps to configure OCSP or enable CRL in an authentication adapter configuration. • Updated Android proxy URL to cert-proxy.vmwareidentity.com:5262 • Updated the Destination Hostname example to remove “https://”

&ɪ–ˇ–¹#

Introduction ..... 3#
Using the Workspace ONE Getting Started Wizard ..... 3#
Unified Workspace Setup Component ..... 3#
Workspace ONE Setup Wizard ..... 5#
Extend a Third-party Identity Provider in the VMware Identity Manager Service (optional) ..... 7#
Adding Your Existing Identity Provider ..... 7#
Adding the VMware Identity Manager Service as an Authentication Provider ..... 7#
iOS SSO ..... 8#
Step 1: Enable the AirWatch Certificate Authority ..... 8#
Step 2: Enable Authentication Adapter ..... 8#
Step 3: Create an Access Policy in VMware Identity Manager. ..... 9#
Step 4: Create your iOS Single Sign-on Profile in AirWatch ..... 9#
Android SSO ..... 11#
Requirements ..... 11#
Step 1: Enable Single Sign-on in AirWatch ..... 11#
Step 2: Enable Authentication Adapter ..... 11#
Step 3: Create an Access Policy in VMware Identity Manager Service. ..... 12#
Android SSO – User Experience ..... 13#
Android for Work ..... 13#
Windows Desktop SSO ..... 14#
Step 1: Enable Built-in Adapters ..... 14#
Step 2: Create an Access Policy in VMware Identity Manager ..... 16#
Step 3: Distribute Certificates through AirWatch ..... 17#
Enable Compliance Status Checking ..... 17#
Distribute Certificates ..... 17#
Authentication Policies ..... 18#
Configuring an L1 policy ..... 18#
Configuring an L2 policy ..... 18#
Appendix – Additional Resources ..... 20#
VMware Identity Manager Documents ..... 20#
VMware AirWatch Documents ..... 20#

Introduction

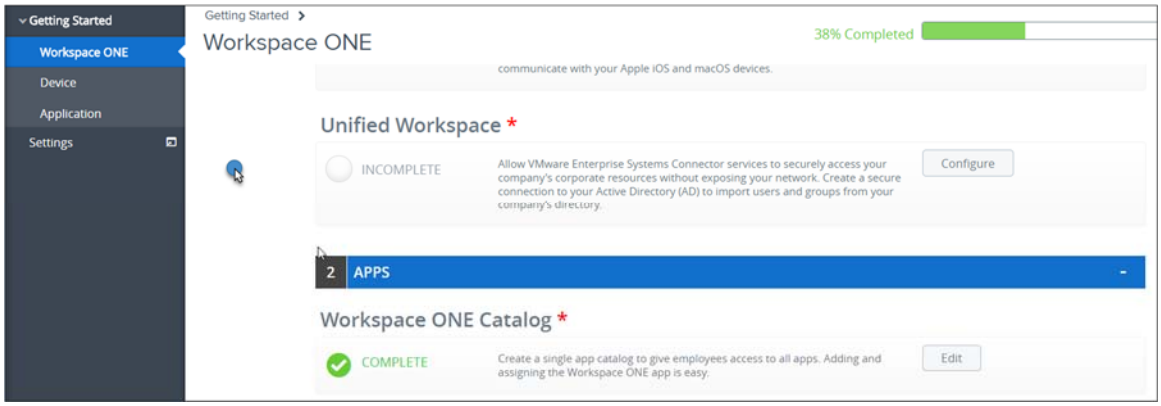
The Workspace ONE Getting Started Wizard in the AirWatch Console guides you through configuration of Active Directory synchronization and authentication with VMware Identity Manager™. The Wizard enables the Workspace™ ONE™ application to be is used as a replacement for the VMware AirWatch® App Catalog™, as an enrollment agent, or as a container.

This guide also details how to deploy key features of Workspace ONE, such as cross platform mobile single sign-on (SSO), conditional access, and authentication adapters and policies. Complete administration of VMware Identity Manager is included in the VMware Identity Manager Administration guide.

Using the Workspace ONE Getting Started Wizard

The Getting Started Wizard serves as a checklist that walks you through the AirWatch Console settings step by step. In the Workspace ONE Getting Started page you can set up the Workspace ONE components and configure Workspace ONE catalog and applications.

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.



Unified Workspace Setup Component

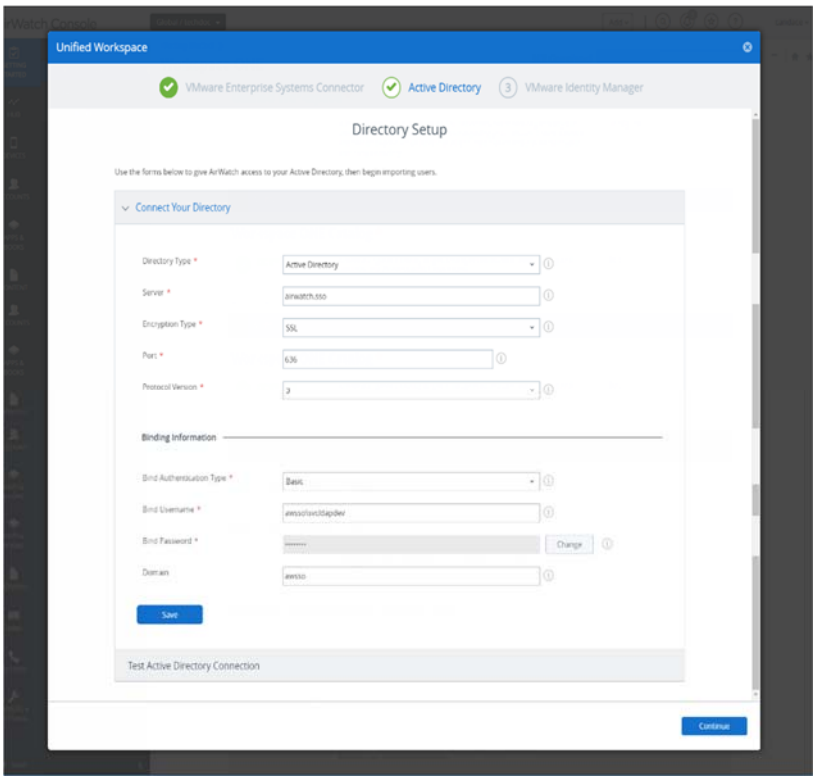
The Unified Workspace setup wizard walks you through the steps to set up the VMware Enterprise System Connector and configure the Active Directory connection from the AirWatch Cloud Connector to import users and groups from your company's directory.

Note: VMware Enterprise System Connector configuration is always required for SaaS customers. On premises customers may or may not require a connector depending on their network architecture. Consult the VMware AirWatch Reference Architecture guide for recommendations and more information.

1. Log into the AirWatch console with the admin password. If necessary create a new password.
2. Accept the terms of use and set up the password recovery questions and security PIN, if required.
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** and in the Unified Workspace section, click **Configure**.
5. If the installation of a connector is necessary to communicate with your Active Directory server, download the VMware Enterprise Systems connector and install or upgrade your connector.

   For installation instructions, access the VMware Enterprise Systems Connector guide.

6. After installation is complete, click **Test Connection** to verify the connector installation.
7. Proceed to the **Active Directory** configuration.



8. Enter the Active Directory server details.
   a. Select the type of directory service that your organization uses.
   b. Enter the address of your directory server. For example, type as 10.10.255.255
   c. Enter the TCP port that is used to communicate with the domain controller. The default port number is 389.
   d. Enter the version of the LDAP protocol that is in use. This is either 2 or 3. If you are unsure of which protocol version to use, leave the value as 3.
   e. 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.
   f. Enter the bind account user name. This account allows read-access permission on your directory server.
   g. Enter the password for the bind account.
   h. Enter the default domain and server name for the directory-based user account.
   i. Click **Save**.
9. Click **Test Connection** to verify connectivity.
10. In the Configure VMware Identity Manager section, for the question, **Do you want to use AirWatch to authenticate users?**, on premises customers should select **Yes**.

    SaaS customers must also select Yes, if only the AirWatch Cloud Connector (ACC) component of the VMware Enterprise Systems Connector is installed in their tenant.

    If the full VMware Enterprise Systems Connector is installed, including the identity manager

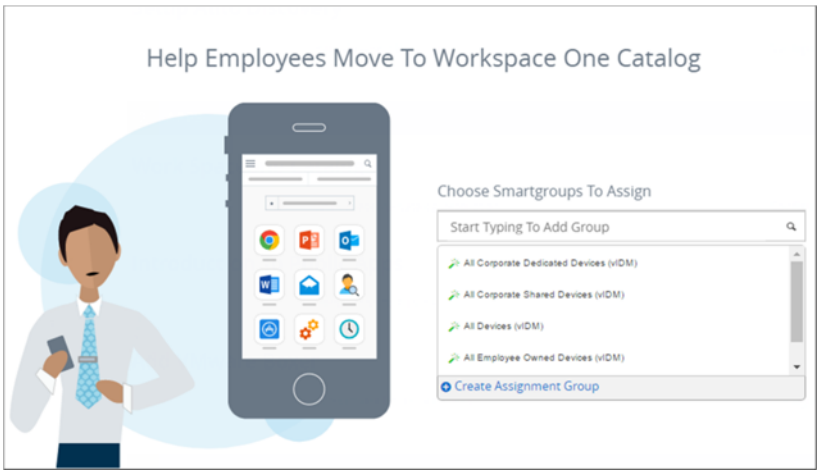
component, you should select No. Selecting No means that VMware Identity Manager uses the identity management directory synchronization channel in the connector, instead of using AirWatch's ACC channel. This option provides the best compatibility with advanced active directory environments.

Workspace ONE Setup Wizard

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 you company's brand information to the Workspace ONE Catalog and application.

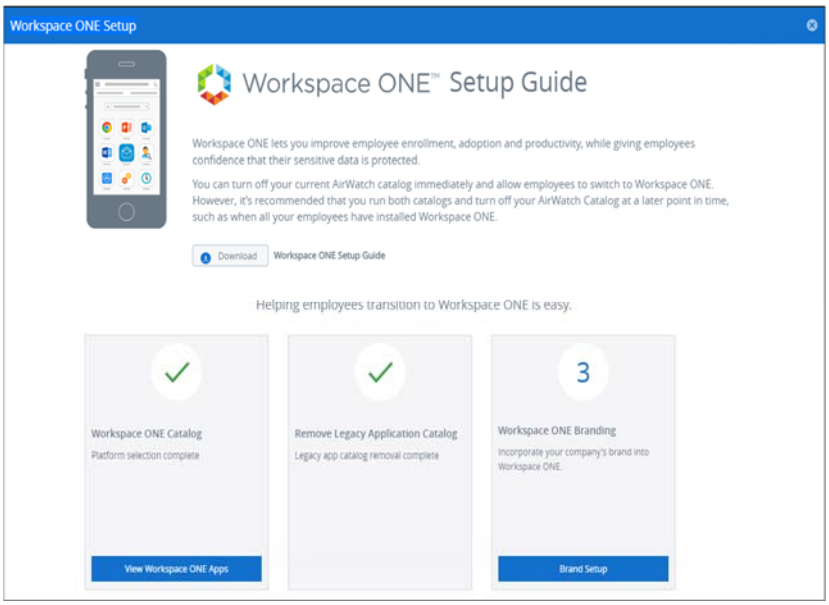
The Workspace ONE application serves as a replacement for the AirWatch app catalog. The Workspace ONE app provides a number of new features as it is a native application, and its integration with identity management. The features include TouchID authentication, SSO to web apps, integration with virtual apps and desktops, and the ability to optionally provision internal applications to unmanaged devices. Workspace ONE is the development platform for new catalog features going forward.

1. Log into the AirWatch console with the admin password. If necessary create a new password.
2. Select **Getting Started > Workspace ONE** and in the Apps section, to enable the Workspace ONE Catalog, click **Configure**.
3. In the **Choose Smartgroups to Assign** section, select the groups that can use the Workspace ONE catalog.



Workspace ONE **will not** be automatically deployed to these devices, only assigned. You will have the option to change the deployment type to **automatic** in the AirWatch Mobile Application Management (MAM) service after completing the wizard, if you want to push the application automatically.

4. Click **Continue**.



5. Click **View Workspace ONE Apps** to see the list of Workspace ONE apps and modify their deployment configurations.
6. Click **Brand Setup** to customize the branding design. The VMware Identity Manager admin console is displayed. You can customize the Workspace ONE catalog portal, sign on pages, and application view. You will need your VMware Identity Manager admin credentials in order to modify Workspace ONE branding.

Extend a Third-party Identity Provider in the VMware Identity Manager Service (optional)

The VMware Identity Manager service supports daisy chaining with a third-party identity provider (IdP) to use an existing identity solution for some use cases. This can be accomplished in one of two ways, depending on whether you want to keep SP-IdP relationships already configured in your existing identity provider, or allow VMware Identity Manager to take them over.

Adding Your Existing Identity Provider

Add your existing identity provider to the VMware Identity Manager service as a third-party identity provider and migrate your existing SAML applications to identity manager.

1. To add another third-party IdP in, in the identity manager service admin console, navigate to Identity and Access Management -> Identity Providers -> Add Identity Provider.
2. Import your third-party IdP's details.
3. Download the VMware IDM metadata from the SAML Metadata page.
4. Import this metadata into your third-party IdP as a new application or service provider.
5. If you encounter any difficulty, follow the steps in the Administering VMware Identity Manager Services in AirWatch Guide.
6. To add AD FS as a third-party IdP in VMware Identity Manager, access the VMware Identity Manager Integration with Active Directory Federation Services 2.0 document located here. https://www.vmware.com/support/pubs/vidm_webapp_sso.html

Adding the VMware Identity Manager Service as an Authentication Provider

Add the VMware Identity Manager Service as an Authentication Provider to your third-party identity provider. This model allows you to deploy mobile SSO and conditional access services without migrating apps to Identity Manager. However, this is not supported by all third-party providers.

- Contact your VMware AirWatch representative for more information on this deployment model.
- Contact your third-party IdP to find out if it supports the following configuration.
  - The ability to add third-party SAML identity providers. This is sometimes referred to support for inbound SAML, or acting as a service provider.
  - The ability to conditionally redirect mobile traffic to that provider.

iOS SSO

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.

These steps are recommended for all iOS SSO customers. On-premises KDC authentication should only be used if dictated by IT security or network policy.

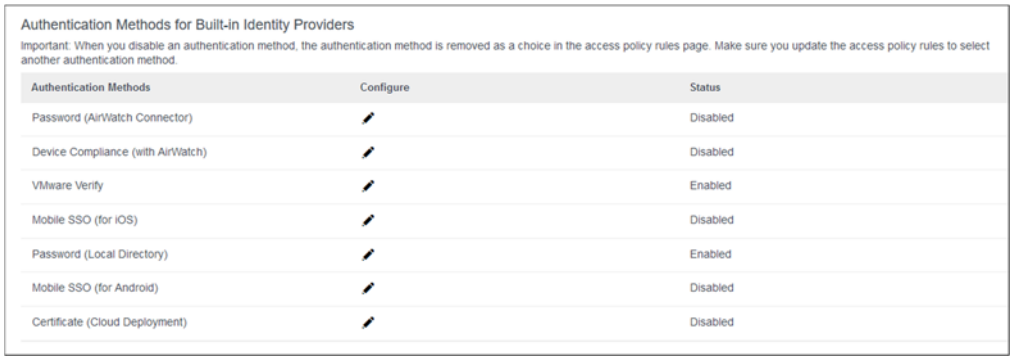
Step 1: Enable the AirWatch Certificate Authority

1. In the AirWatch console, select your Customer level organization group. This should be the organization group with your company name.
2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager**.
3. Under the **Certificate** header, select **Enable**.

   The **Enable** button changes to Export.
4. Click **Export** to download the issuer certificate required for the built-in iOS SSO adapter.

Step 2: Enable Authentication Adapter

1. Log in to the VMware Identity Manager admin console.
2. Select the **Identity & Access Management** tab.
3. Select **Authentication Methods**



   a. Select the **pencil** icon next Mobile SSO (for iOS).

   b. Select Enable KDC Authentication.

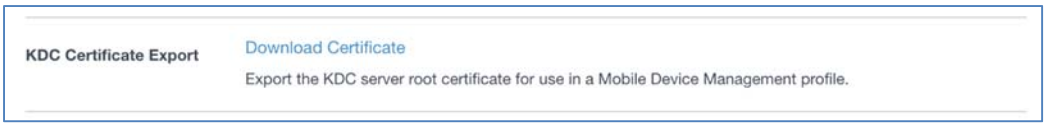
   c. In the Root and Intermediate CA Certificates section, upload your AirWatch CA issuer certificate, downloaded as part of Step 1.

   d. Click **Save**.

4. Go to Identity Providers page and select the built-in identity provider

   a. In the Connector authentication Methods section, associate Mobile SSO (iOS) to this built-in identity provider.

   b. Download the trust certificate for the built-in KDC at the bottom of the page after saving, next to KDC Certificate Export.



Save the trust certificate so you can set up your single sign-on profile in AirWatch.

c. Click **Save**.

Step 3: Create an Access Policy in VMware Identity Manager.

1. Navigate to your VMware Identity Manager admin console.
2. Select the **Identity & Access Management > Manage > Policies** tab.
3. Edit your default policy set, or add a new policy for a specific application.
4. In the Policy Rules section, select a rule to edit or click + to create a new policy rule.
5. Select the **Network Range** to be ALL RANGES or an appropriate network range.
6. In the line **and the user is trying to access content from** to select **iOS**.
7. In the **Select Authentication Methods** drop-down menu, choose **Mobile SSO (for iOS)**.

   To allow devices to fall back to another authentication method, add an additional authentication method such as “Password”.
8. Click **OK** and then **Save** to save the policy set.

Step 4: Create your iOS Single Sign-on Profile in AirWatch

1. In the AirWatch Admin Console, navigate to **Devices > Profiles and Resources > Profiles.**
2. Select **Add > Add Profile**.
3. Select **Apple iOS**.
4. Fill out the **General** tab.
   a. Give the profile a name.
   b. Set it the **Assignment Type** to **Auto**.
   c. Specify Assigned Groups.
5. Navigate to **Credentials > Configure.**
   a. Upload your KDC trust certificate downloaded from Step 2.
6. Navigate to **SCEP > Configure**.
   a. In Credential Source, select AirWatch Certificate Authority Source.

      Certificate authority and template change automatically.
7. Navigate to **Single Sign-On** > **Configure**.
   a. Add a descriptive account name.
   b. In **Kerberos Principle Name**, select the enrolment user value.

      Select a different option if enrollment user does not correspond to SAMAccountName.
   c. In the **Realm** text box, North American customers should add **VMWAREIDENTITY.COM** to the **Realm** text box.

      Other regions will enter .EU, or .ASIA depending on the location of your environment.

      Be sure not to add any preceding or trailing spaces when filling out this text box.
   d. In **Kerberos Principle Name**, select the enrolment user value.
   e. Select **SCEP #1** as your renewal certificate. This certificate represents your users’ identities

f. In the **URL Prefixes** section, add your VMware Identity Manager tenant URL, in the form of **https://tenant.vmwareidentity.com**.

g. In the **Applications** section, add the bundle ID of any applications you wish to enable for single sign-on. For example, add com.air-watch.appcenter and com.apple.mobilesafari as a baseline to allow the mobile SSO framework access to Safari applications.

Note: Many applications use Safari View Controller as a web viewer. If you are using this type of application, add com.apple.safariviewcontroller in addition to the application bundle id. Safari View Controller usage in an app is characterized by a full screen browser window, a URL bar, and a done button.

Additional application IDs can be found by enrolling a device with the desired application(s) into AirWatch and navigating to the **Application** section of the Device Details page for the device.

8. Select **Save and Publish.**

Android SSO

Workspace ONE offers universal Android mobile single sign-on. Mobile single sign-on allows users to sign in to enterprise apps securely, without the need for a password. The solution uses the VMware Tunnel application to inject certificates and device ID information into authentication flows. This solution supports both classic Android management and Android for Work. The following section describes how to enable the single sign-on framework and enable applications to use it.

Requirements

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

Note: Installation of the VMware Tunnel server is NOT required for Mobile SSO.

Step 1: Enable Single Sign-on in AirWatch

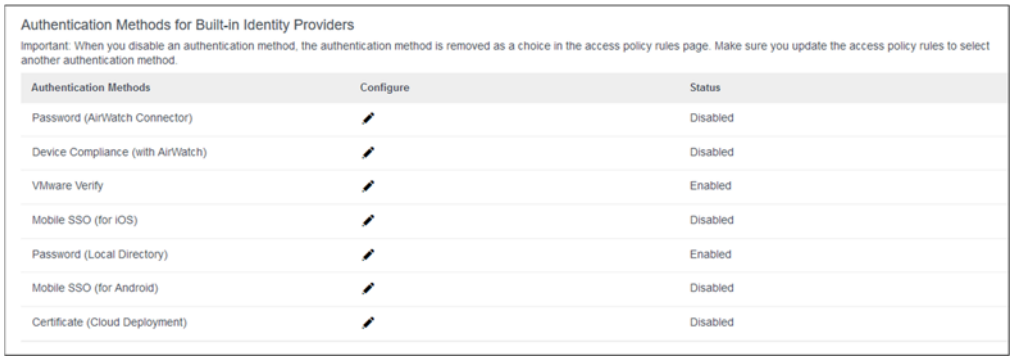
1. In AirWatch, navigate to **Apps & Books > Applications > List View**.
2. Select either **Internal**, **Public**, or **Purchased**, and click **Add Application** to add a new app.
   a. Give the application a name and either select to upload or link to the application.
   b. Complete the details, assignment and terms of use for the application
   c. Repeat these steps to add new applications.
3. Navigate to **System > Enterprise Integration > VMware Tunnel > Network Traffic Rules**.

   a. Click **Add** and select the application you wish to use for SSO.
   b. Select the action as **Proxy** and enter the URL for the Android SSO Adapter. This URL is based on your tenant and takes the form of **cert-proxy.vmwareidentity.com:5262**.

      Repeat this step any time you need to add a new application for SSO.
   c. In the **Destination Hostname** field, enter the VMware Identity Manager's hostname so that the Tunnel client routes the traffic to the Android Single sign-on adapter as soon as it comes across the VMware Identity hostname. For SaaS customers, the hostname displays as **{tenant}.vmwareidentity.com**.
4. Clck, **Publish Rules**. On publishing, your device receives an update VPN profile and the VMware Tunnel application is configured to enable SSO.

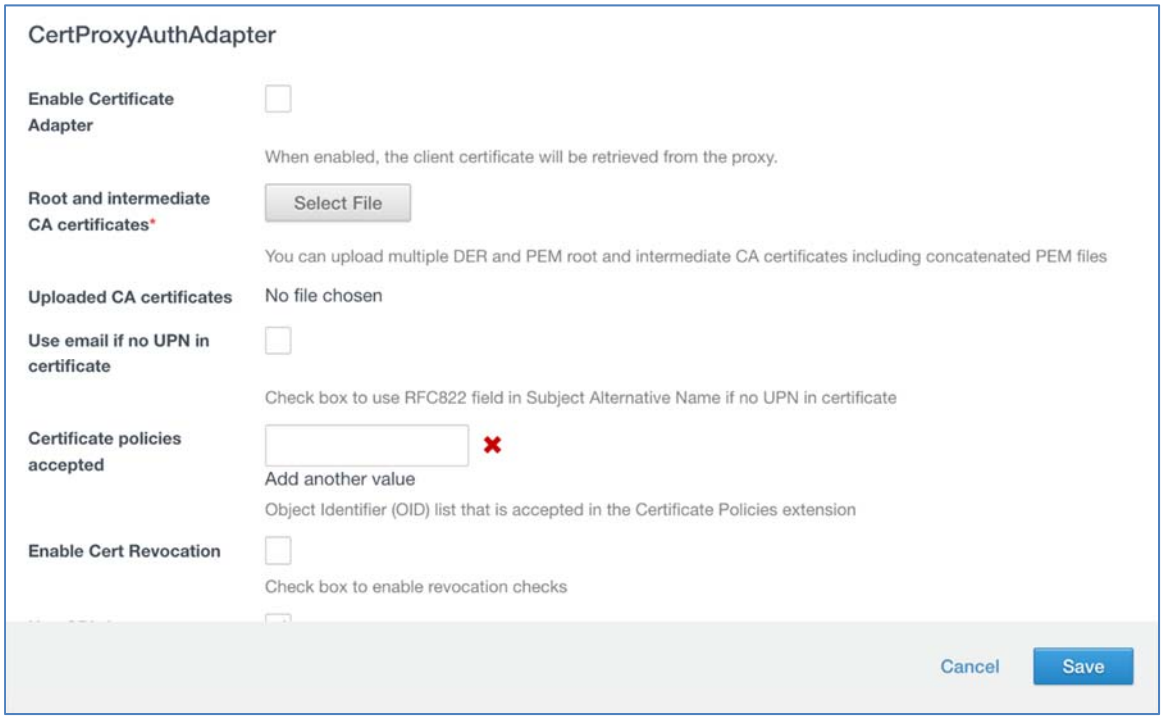
Step 2: Enable Authentication Adapter

1. Log in to the VMware Identity Manager admin console.
2. Select the **Identity & Access Management** tab.
3. Select **Authentication Methods**



a. Select the pencil icon next to **Mobile SSO (for Android).**

b. Select **Enable Certificate Adapter**.



c. Upload your CA's root and intermediate certificates to establish a trust chain.

d. Select **Save**.

4. Go to the configured Built-in Identity Provider and associate the Mobile SSO (Android SSO) in the Authentication Methods section.

Step 3: Create an Access Policy in VMware Identity Manager Service.

1. Navigate to your VMware Identity Manager admin console.
2. Select **Identity & Access Management > Policies**.
3. Edit your default policy set, or add a new policy for a specific application.
4. Select the Policy Rule to edit or click **+** to create a new policy rule.
5. Select the **Network Range** to be ALL RANGES or an appropriate network range.

6. In the line **and the user is trying to access content from** to select **Android**.
7. In the **Select Authentication Methods** drop-down menu, choose **Mobile SSO (for Android)**.

   To allow devices to fall back to another authentication method, add an additional authentication method such as “Password”.

8. Click **OK** and then **Save** to save the policy set.

Android SSO – User Experience

Android mobile single sign-on relies on the VMware Tunnel application, so the initial user experience differs from that of iOS. After an Android device enabled with SSO enrolls, the user must open the VMware Tunnel application and accept the prompt. This action grants the Tunnel application the permissions required to function. If you are employing conditional access policies to prevent applications from being accessed on unmanaged devices, these applications will also be unavailable until the Tunnel client is activated.

Android for Work

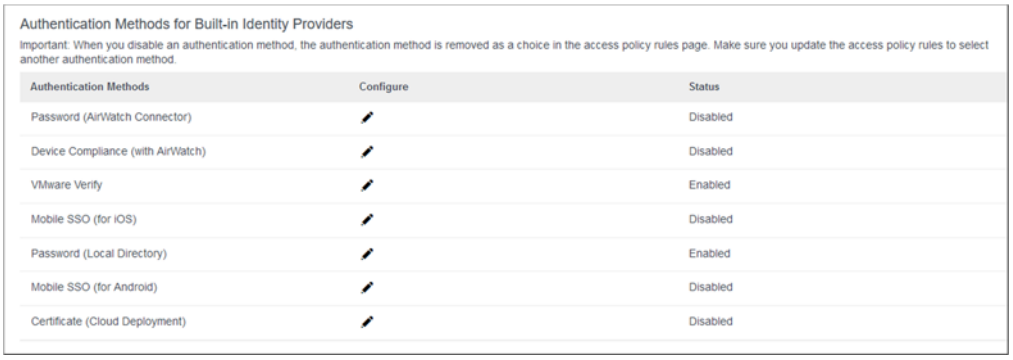
Deploying the Workspace ONE application to all Android devices does not automatically deploy the application Android for Work containers. Android for Work is required to use the Workspace ONE application Adaptive Management feature. To add this application to Android for Work devices as well and for 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 Desktop SSO

Certificate-based SSO is the recommended experience for managed Windows desktops and laptops. The following steps describe how to enable VMware Identity Manager for certificate-based SSO.

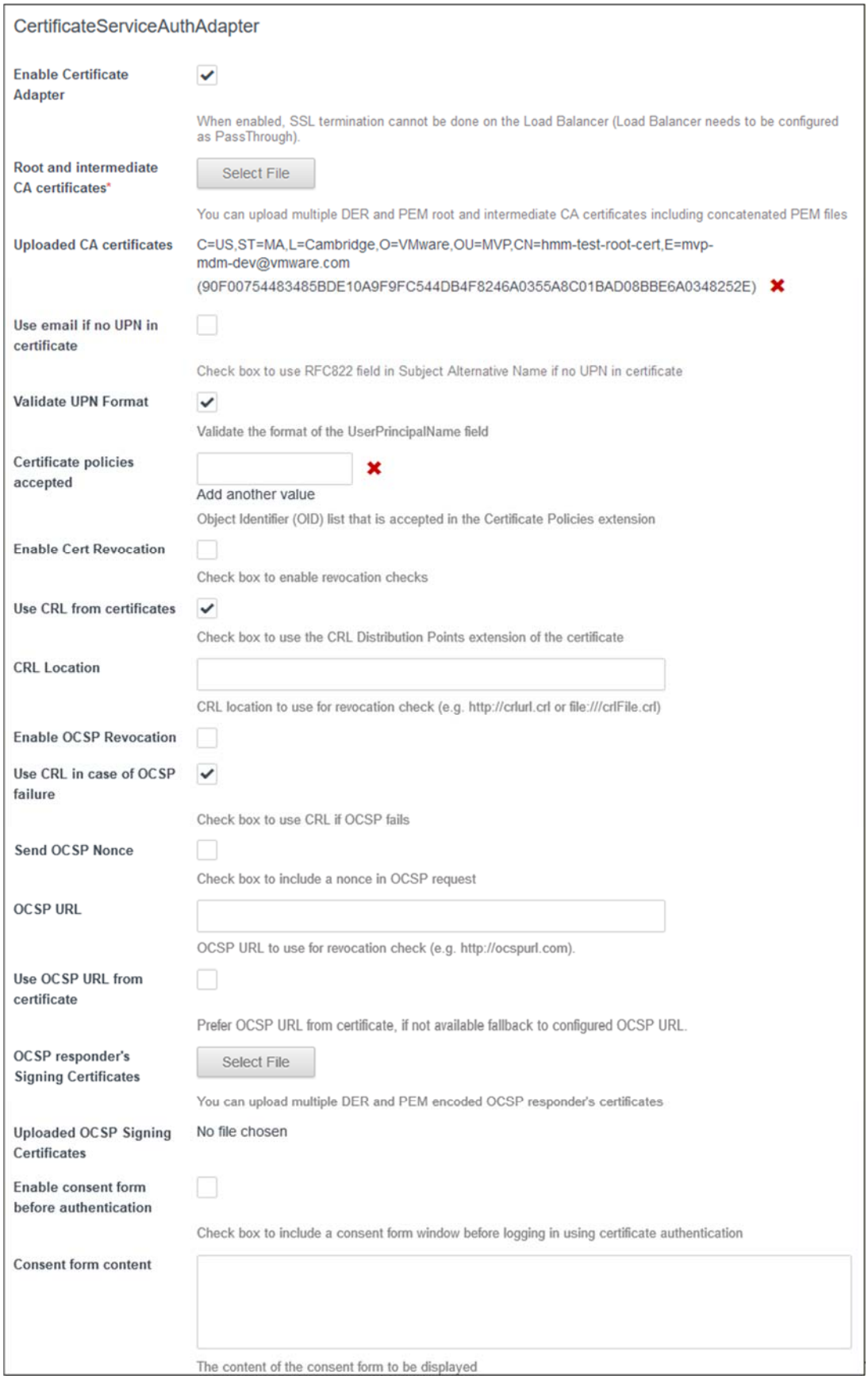
Step 1: Enable Built-in Adapters

1. Log in to the VMware Identity Manager admin console.
2. Select the **Identity & Access Management** tab.
3. Select **Authentication Methods**



   a. Select the pencil icon next to Certificate (Cloud Deployment).

   b. Select Enable Certificate Adapter.


CertificateServiceAuthAdapter
Enable Certificate Adapter
When enabled, SSL termination cannot be done on the Load Balancer (Load Balancer needs to be configured as PassThrough).
Root and intermediate CA certificates*
Select File
You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files
Uploaded CA certificates
C=US,ST=MA,L=Cambridge,O=VMware,OU=MVP,CN=hmm-test-root-cert,E=mvp-mdm-dev@vmware.com
(90F00754483485BDE10A9F9FC544DB4F8246A0355A8C01BAD08BBE6A0348252E)
Use email if no UPN in certificate
Check box to use RFC822 field in Subject Alternative Name if no UPN in certificate
Validate UPN Format
Validate the format of the UserPrincipalName field
Certificate policies accepted
Add another value
Object Identifier (OID) list that is accepted in the Certificate Policies extension
Enable Cert Revocation
Check box to enable revocation checks
Use CRL from certificates
Check box to use the CRL Distribution Points extension of the certificate
CRL Location
CRL location to use for revocation check (e.g. http://crlurl.crl or file:///crlFile.crl)
Enable OCSP Revocation
Use CRL in case of OCSP failure
Check box to use CRL if OCSP fails
Send OCSP Nonce
Check box to include a nonce in OCSP request
OCSP URL
OCSP URL to use for revocation check (e.g. http://ocspurl.com).
Use OCSP URL from certificate
Prefer OCSP URL from certificate, if not available fallback to configured OCSP URL.
OCSP responder's Signing Certificates
Select File
You can upload multiple DER and PEM encoded OCSP responder's certificates
Uploaded OCSP Signing Certificates
No file chosen
Enable consent form before authentication
Check box to include a consent form window before logging in using certificate authentication
Consent form content
The content of the consent form to be displayed

c. Upload the CA's root and intermediate certificates to establish a trust chain.

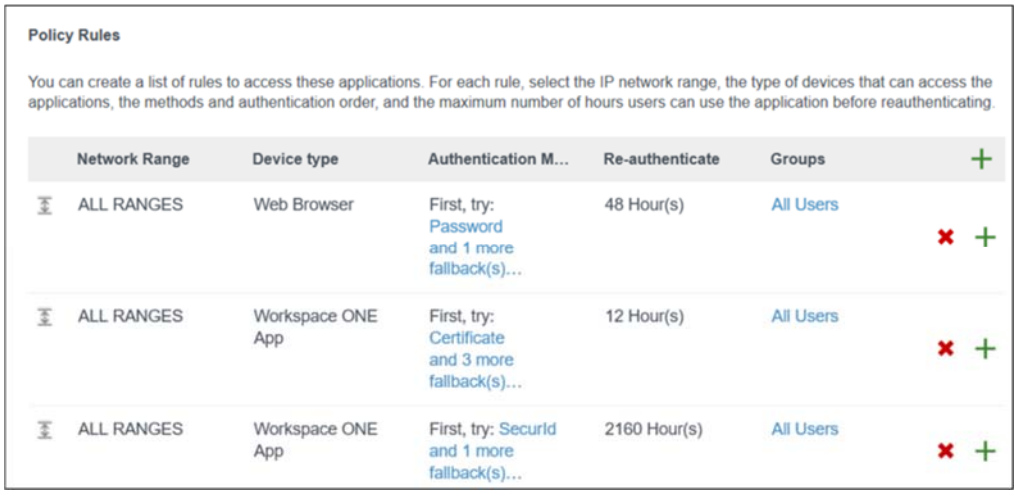
d. Select **Save**.

Step 2: Create an Access Policy in VMware Identity Manager

1. Navigate to your VMware Identity Manager admin console.
2. Select **Identity & Access Management tab > Manage > Policies**.
3. Edit your default policy set, or add a new policy for a specific application.
4. Select the Policy Rule to edit or click **+** to create a new policy rule.
5. Set **Network Range** to **ALL RANGES** or the appropriate network range.
6. Set **and the user is trying to access content from** to **Web Browser**.
7. Under authentication methods, choose **Certificate (cloud deployment)**. If you wish to allow devices to fall back to another authentication method, you can check an additional authentication method such as "Password."
8. **Save** the policy.

   To create additional policies for Windows 10 or OS X, repeat this process, but specify **Windows 10** or **OS X** when prompted to define where the user is trying to access content from. This allows you to create platform specific rules, separate from your standard policy for all web browsers.

9. The Web Browser policy should be ranked below any platform specific policies, as shown in the screenshot below. VMware Identity Manager will try policies in ranked order, and web browser will catch all requests before hitting the platform specific policies. Use the drag icon on the left in the policies list to move your **Web Browser** policy below any platform specific policies.



10. **Save** the policy sets.

Step 3: Distribute Certificates through AirWatch

To distribute certificates to these devices, you can either use the AirWatch CA or you can integrate your company CA with AirWatch. To learn more about certificate authorities, reference the CA documentation available on AirWatch Resources (resources.air-watch.com).

Enable Compliance Status Checking

This section applies only if you wish to use your own enterprise CA. This step is automatically configured in the AirWatch certificate authority.

1. After completing the integration of your enterprise CA and configuration of the standard user certificate template, navigate back to the Certificate Template interface.
2. Edit the template and include the SAN value as **DNS Name** as **{DeviceUid}**. This allows VMware Identity Manager to process compliance status during authentication attempts.

3. Click **Save**.

Distribute Certificates

1. In the AirWatch Admin Console, navigate to **Devices > Profiles & resources >Profiles.**
2. Select **Add Profile**.
3. Select the platform, and if asked, the device type.
4. In the **General** tab, fill in the deployment options.
5. To use an enterprise CA the **Credential** payload, or to use AirWatch CA select the SCEP payload.
6. Select your configured CA and template.
7. **Save and publish** the profile.

Authentication Policies

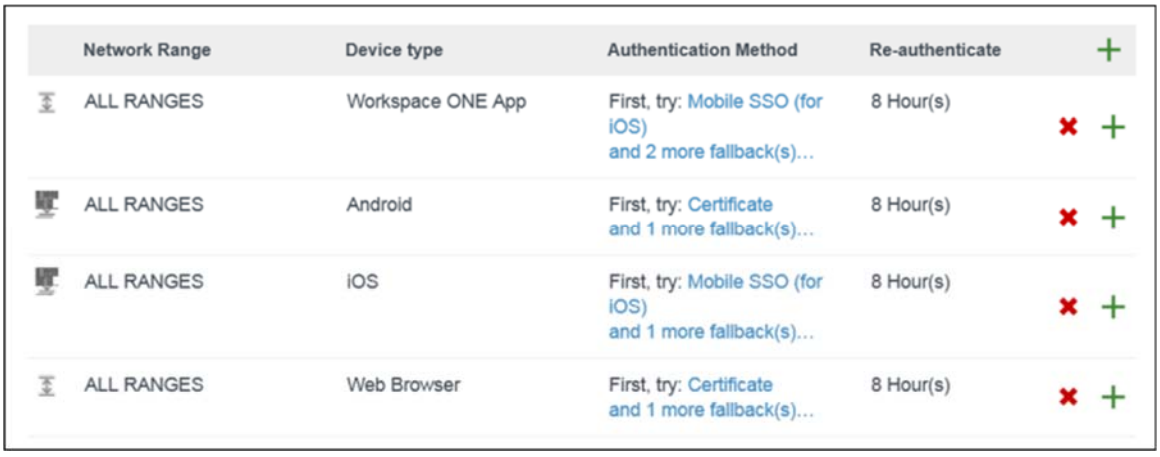
Authentication policies allow administrators to configure features like mobile single sign-on, conditional access to applications based on enrollment and compliance status, step up and multifactor authentication.

While there are a broad range of configuration options available, for the purposes of this guide we will create an EMM managed, and unmanaged tier of application access. L1 access applications allow unmanaged devices to access them. L2 access applications are restricted to users accessing them from managed, compliant devices. VMware Identity Manager provides a number of built-in authentication adapters to accomplish this experience.

- **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.

Configuring an L1 policy

Use your default policy as a baseline “L1” policy for all apps. In the default policy, for each platform of devices in your deployment, create a rule that defines that platform’s preferred authentication method, enabling SSO as well as at least one fallback method. This setup provides the best experience to manage devices, while still providing a manual login option for unmanaged devices. You might wish to further secure access from unmanaged devices with VMware Verify or other multifactor authentication. An example L1 policy is displayed.



Network Range	Device type	Authentication Method	Re-authenticate
ALL RANGES	Workspace ONE App	First, try: Mobile SSO (for iOS) and 2 more fallback(s)...	8 Hour(s)
ALL RANGES	Android	First, try: Certificate and 1 more fallback(s)...	8 Hour(s)
ALL RANGES	iOS	First, try: Mobile SSO (for iOS) and 1 more fallback(s)...	8 Hour(s)
ALL RANGES	Web Browser	First, try: Certificate and 1 more fallback(s)...	8 Hour(s)

Configuring an L2 policy

If your organization has a selection of applications containing sensitive data, you might want to restrict access to these applications to only MDM managed devices. Managed devices can be tracked and wiped if necessary and enterprise data is removed when they are unenrolled.

To enforce this managed requirement on a selection of apps, create a new policy specifically configured for

these applications. After you create the policy, in the **Applies to** section, select the applications that apply to this policy. Create a policy rule for each type of device in your deployment and define the correct SSO authentication type. However, since unmanaged devices should not be able to access these apps, do not define a fallback authentication type. If an unmanaged iOS device for example tries to connect to an application configured only for managed device SSO, the device will not be able to respond with the appropriate Kerberos wrapped certificate, the authentication attempt will fail and the user will not be able to access the content. An example L2 policy is displayed.

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)

Appendix – Additional Resources

Reference the following guides as needed when performing the steps in this document. Because integrating AirWatch with Identity Manager for mobile SSO uses a number of pre-existing components working together, you may need to initially configure or modify other modules of the product such as certificate authority integration.

VMware Identity Manager Documents

Locate VMware Identity Manager documentation from the following Documentation Center site:

https://www.vmware.com/support/pubs/identitymanager-pubs.html

Ensure you have the correct Identity Manager version (Cloud or an On-Premise version) when accessing documentation.

VMware AirWatch Documents

Locate VMware AirWatch documentation from AirWatch Resources:

https://resources.air-watch.com

Ensure you have your appropriate AirWatch version selected when searching for resources.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com