Integrating AirWatch and VMware Identity Manager

VMware AirWatch 9.1.1

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

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

Contents

About Integrating AirWatch and VMware Identity Manager

The Integrating AirWatch and VMware Identity Manager guide provides information about integrating the VMware Identity Manager service with the AirWatch service.

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.

Integrating AirWatch With VMware Identity Manager

1

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.

This section includes the following topics:

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.

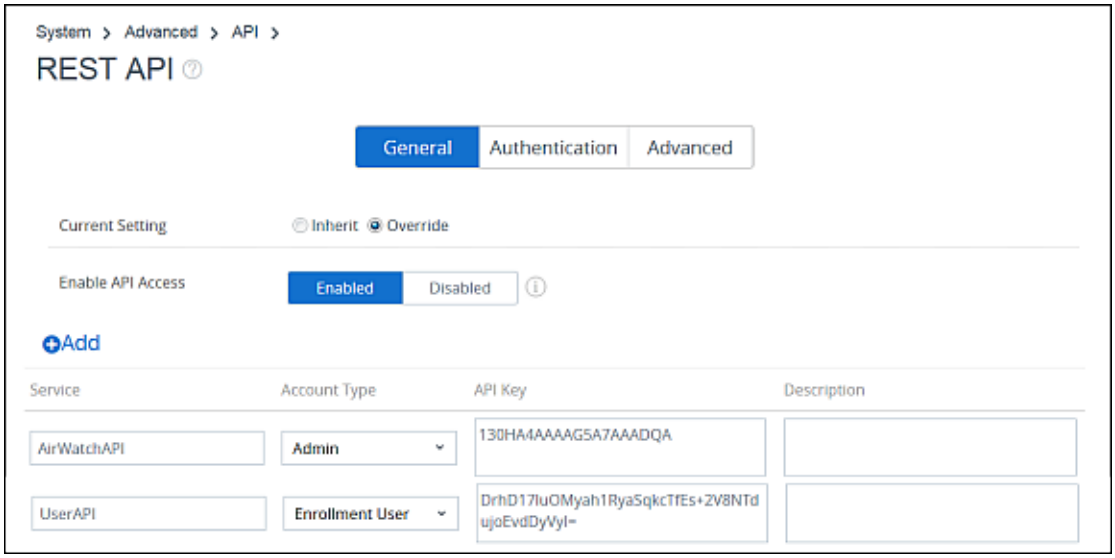
Procedure

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.



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

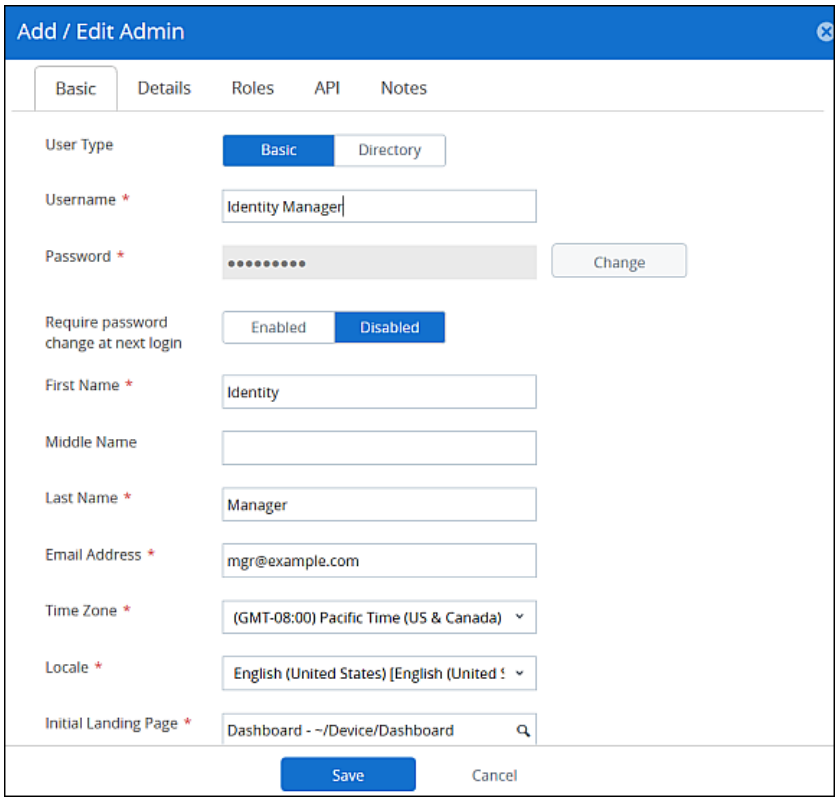
The AirWatch REST admin API key is created.

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.



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.

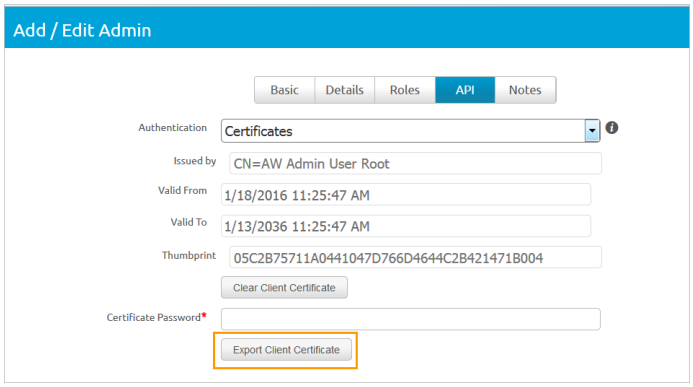
7 Click **Save**.

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 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.

Note If you map domains to multiple AirWatch organization groups, you cannot use AirWatch Cloud Connector for authentication.

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.

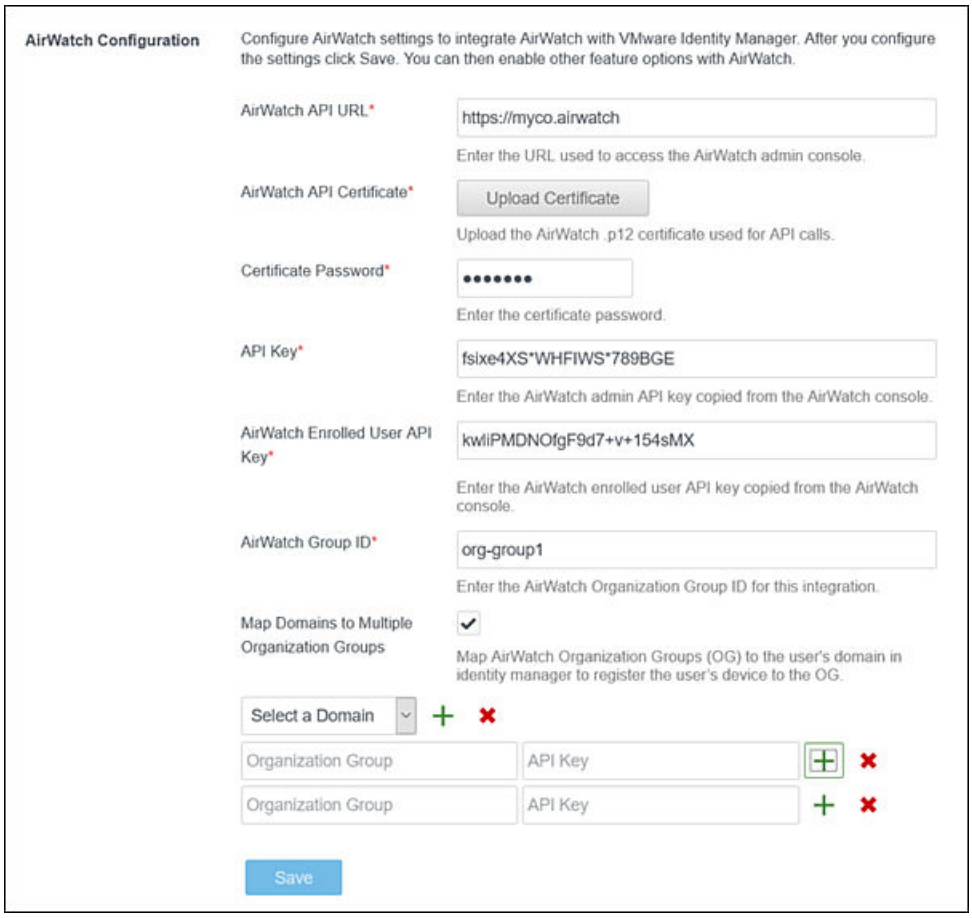
Procedure

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

3. 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 . Click **+** to map additional organization groups to the domain.
   b. enter the organization group name and the admin API key for that group in the text boxes that display
   c. Click **+** to map additional organization groups to the domain.
   d. To map another domain, click **+** next to the drop-down menu.

4 Click **Save**.



What to do next

- Enable the feature option Unified Catalog to merge apps set up in the AirWatch catalog to the unified catalog.
- Enable Compliance check to verify that AirWatch managed devices adhere to AirWatch compliance policies.

Mapping VMware Identity Manager Domains to Multiple Organization Groups in AirWatch

AirWatch uses organization groups to identify users and establish permissions. When VMware Identity Manager is integrated with AirWatch, you can link domains configured in VMware Identity Manager to specific organization groups in AirWatch.

When users log in to Workspace ONE from their devices, users' record are verified and the device is registered to the appropriate organization group in AirWatch. Mobile applications display in the user's catalog.

In the AirWatch integration page, you add the organization group ID and enter the AirWatch admin API key that is used to make API requests.

Note You cannot use AirWatch Cloud Connector password authentication when you enable mapping domains to multiple organization groups.

Enable Workspace ONE 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.

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

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

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 Chapter 2 Implementing Authentication with AirWatch Cloud Connector to use AirWatch Cloud Connector authentication.

Configure Access Policy Rule

To provide secure access to the users' 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 their apps portal 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 take actions such as block, allow, or step-up authenticate users based on conditions such as network, device type, AirWatch device enrollment and compliant status, or application being accessed. 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 Identity & Access Management tab, go to **Manage > Policies**.

2 Select the access policy to edit.

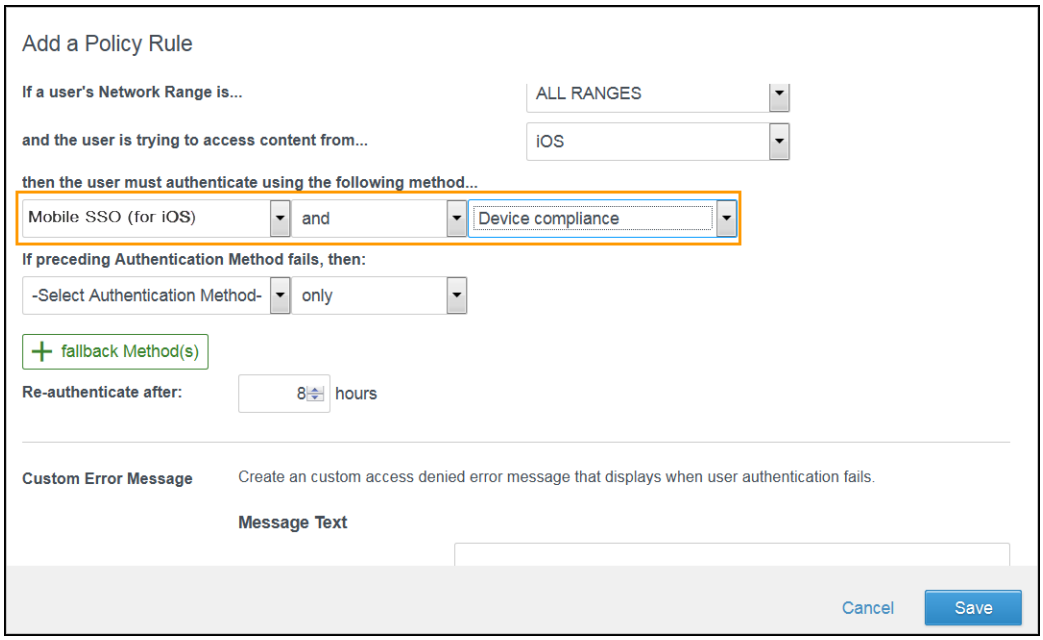
3 In the Policy Rules section, select the policy rule to edit.

4 In the drop-down menu for **then the user must authenticate using the following method**, click **+** and select the authentication method to use.

5 In the second drop-down menu for **then the user must authenticate using the following method**, select **Device Compliance (with AirWatch)**.

6 (Optional) In the Custom Error **Message Text** text box, create a custom message that displays when user authentication fails because of the device is not compliant. In the **Custom Error Link** text box, you can add a link in the message.

7 Click **Save**.



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 through AirWatch configuration options in the VMware Identity Manager service.

When you save these option 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 2

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 log in to their Workspace ONE portal, either from an iOS or Android device or 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.

This section includes the following topics:

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
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.

The VMware Identity Manager directory can be used with the AirWatch Cloud Connector for password authentication.

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, `https://myco.identitymanager.com`.
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
Enable AirWatch Password Authentication	This check box enables AirWatch password authentication.
AirWatch Admin Console URL	Pre-populated with the AirWatch URL.
AirWatch API Key	Pre-populated with the AirWatch Admin API key.
Certificate Used for Authentication	Pre-populated with the AirWatch Cloud Connector certificate.
Password for Certificate	Pre-populated with the password for the AirWatch Cloud Connector certificate.
AirWatch Group ID	Pre-populated with the organization group ID.
Number of authentication attempts allowed	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.
JIT Enabled	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
Identity Provider Name	Enter the name for this built-in identity provider instance.
Users	Select which users to authentication. The configured directories are listed.
Network	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.
Authentication Methods	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. For Device Compliance (with AirWatch) and Password (AirWatch Connector), make sure that the option is enabled in the AirWatch configuration page.

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.

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

For the VMware Identity Manager service on premises, two KDC service options are available. One option is to use the built-in KDC that you initialize in the VMware Identity Manager appliance before you enable the mobile SSO authentication method from the administration console. The second option is to use the VMware Identity Manager KDC cloud hosted service. For more information about the built-in KDC, see the Installing and Configuring VMware Identity Manager guide. To use the Cloud Hosted KDC Service, see Using the Cloud Hosted KDC Service.

When the identity manager is 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.

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.
- 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.

This section includes the following topics:

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

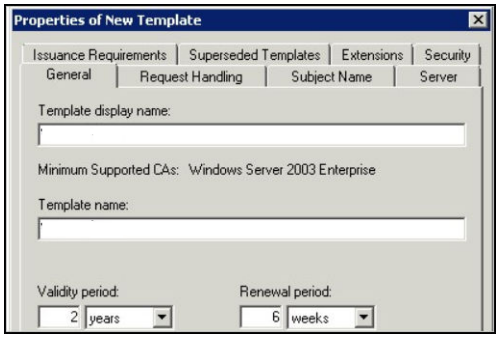
Configure the Certificate Template in AirWatch.

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.
- **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

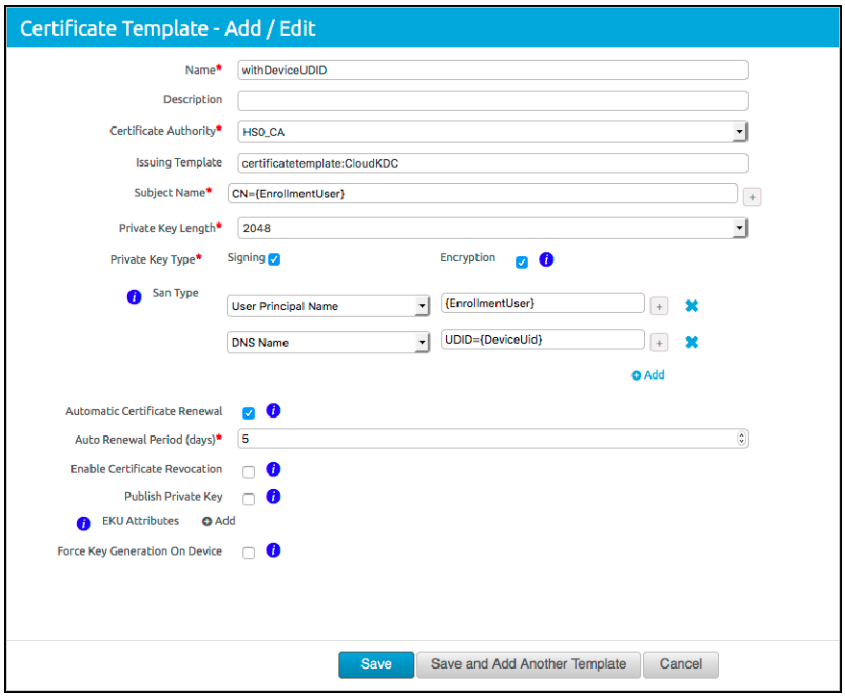
Configure the Certificate Authority in AirWatch.

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

4 Slick **Save**.



What to do next

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

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
Credential Source	Select **Defined Certificate Authority** from the drop-down menu.
Certificate Authority	Select the certificate authority from the list in the drop-down menu.
Certificate Template	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
Account Name	Enter **Kerberos**.
Kerberos Principal Name	Click **+** and select **{EnrollmentUser}**.
Realm	Enter the Identity Manager realm name for your tenant. The text in this parameter must be capitalized. Realm name choices are **VMWAREIDENTITY.COM**, **VMWAREIDENTITY.EU**, and **VMWAREIDENTITY.ASIA**. Enter the realm name you used when you initialized KDC in the VMware Identity Manager appliance. For example, EXAMPLE.COM
Renewal Certificate	Select **Certificate #1** from the drop-down menu. This is the Active Directory CA cert that was configured first under credentials.
URL Prefixes	Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. Enter the VMware Identity Manager server URL as `https://myco.example.com`. Enter the VMware Identity Manager server URL as `https://<tenant>.vmwareidentity.<region>`.
Applications	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 `com.apple.mobilesafari`. Continue to enter application bundle IDs. The applications listed must support SAML authentication

11 Click **Save & Publish**.

When the iOS profile is successfully pushed to users' devices, users can sign in to Workspace ONE using the Mobile SSO for iOS authentication method without entering their credentials.

What to do next

Create another profile to configure any other desired features, for example, Web Clips to create icons for Web Apps that you push from AirWatch to iOS device home pages or the app catalog.

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 console, select the KDC service option to use. See Configuring Mobile SSO for iOS Authentication in the Built-in Identity Provider

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

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 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
Credential Source	Select **AirWatch Certificate Authority** from the drop-down menu.
Certificate Authority	Select the **AirWatch Certificate Authority** from the drop-down menu.
Certificate Template	Select **Single Sign On** 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
Account Name	Enter **`Kerberos`**.
Kerberos Principal Name	Click **+** and select **{EnrollmentUser}**.

Option	Description
Realm	Enter the Identity Manager realm name for your tenant. The text in this parameter must be capitalized. Realm name choices are **VMWAREIDENTITY.COM**, **VMWAREIDENTITY.EU**, and **VMWAREIDENTITY.ASIA**. Enter the realm name you used when you initialized KDC in the VMware Identity Manager appliance. For example, **EXAMPLE.COM**.
Renewal Certificate	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.
URL Prefixes	Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. Enter the VMware Identity Manager server URL as **https://myco.example.com**. Enter the VMware Identity Manager server URL as **https://<tenant>.vmwareidentity.<region>**.
Applications	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 **com.apple.mobilesafari**. 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

Create another profile to configure any other desired features for iOS Kerberos, for example Web Clips to create icons for Web Apps that you push from AirWatch to iOS device home pages or the app catalog.

Configuring Mobile SSO for iOS Authentication in the Built-in Identity Provider

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

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.

VMware Identity Manager uses an identity provider that is built in to the 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.

In the VMware Identity Manager service, Kerberos can be integrated in one of two ways.

- 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 The KDC service hosted in the cloud is the only option when VMware Identity Manager is deployed with AirWatch in a Windows environment.

- Built-in KDC on the appliance. The built-in KDC requires initializing KDC on the appliance and creating public DNS entries to allow the Kerberos clients to find the KDC.

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 publically 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 in the Built-In Identity Provider

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
Enable KDC Authentication	Select this check box to enable users to sign in using iOS devices that support Kerberos authentication.
Realm	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 If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays. The realm value is read-only. The realm entered here is the identity manager realm name for your tenant.
Root and Intermediate CA Certificate	Upload the certificate authority issuer certificate file. The file format can be either PEM or DER.
Uploaded CA Certificate Subject DNs	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.
Enable OCSP	Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP Responder’s Signing Certificate	Upload the OCSP certificate for the responder. When you are using the AirWatch Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the AirWatch certificate here as well.
OCSP Responder’s Signing Certificate Subject DN	The uploaded OCSP certificate file is listed here.

Option	Description
Enable Cancel Link	When authentication is taking too long, give the user the ability to click Cancel to stop the authentication attempt and cancel the sign-in. When the Cancel link is enabled, **Cancel** appears at the end of the authentication error message that displays.
Cancel Message	Create a custom message that displays when the Kerberos authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials`.

4 Click **Save**.

What to do next

- Associate the Mobile SSO (for iOS) authentication method in the built-in identity provider.
- 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.
- 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 Identity Manager.

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 AirWatch Tunnel mobile application is installed on the Android device. The AirWatch 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 AirWatch Tunnel. Because you are not installing the Tunnel server, you do not enter the AirWatch Tunnel server host name and port. You still set up a profile using the AirWatch Tunnel profile form, but traffic is not directed to the Tunnel server. The Tunnel client is used only for single sign-on.

In theAirWatch admin console you configure the following settings.

- Per App Tunnel component in the AirWatch Tunnel. This configuration allows Android devices access to internal and managed public apps through the AirWatch 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 AirWatch Tunnel in the AirWatch admin console and installing the AirWatch Tunnel server before you configure Mobile SSO for Android in the VMware Identity Manager administration console. The AirWatch Tunnel service provides per app VPN access to AirWatch managed apps. AirWatch 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 AirWatch Tunnel. This configuration allows Android devices access to internal and managed public applications through the AirWatch Tunnel mobile app client.

  After the AirWatch Tunnel settings are configured in the admin console, you download the AirWatch Tunnel installer and proceed with the installation of the AirWatch 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 AirWatch Tunnel, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

This section includes the following topics:

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 AirWatch 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 > AirWatch Tunnel**.
2. The first time you configure AirWatch Tunnel, select **Configure** and follow the configuration wizard. Otherwise, select **Override** and select the **Enable AirWatch 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
Default	Select Default to use the AirWatch issued certificates.
Enterprise CA	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 AirWatch Tunnel configuration page.
7. Click **Next**.
8. In the Profile Association page, associate an existing or create a new AirWatch 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 AirWatch Tunnel VPN Access Settings from AirWatch Admin Console

You enable the Per App Tunnel component in the AirWatch 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. For detailed AirWatch Tunnel configuration instructions, see the VMware AirWatch Tunnel Guide on the AirWatch Resources Web site.

Procedure

1 In the AirWatch admin console, navigate to **System > Enterprise Integration > AirWatch Tunnel**.

2 The first time you configure AirWatch Tunnel, select **Configure** and follow the configuration wizard. Otherwise, select **Override** and select the **Enable AirWatch 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, for the Per-App Tunneling Configuration enter the AirWatch 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
Default	Select Default to use the AirWatch issued certificates.
Enterprise CA	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 AirWatch Tunnel configuration page.

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

7 Click **Next**.

8 In the Profile Association page, associate an existing or create a new AirWatch 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 AirWatch 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 Access Point to deploy the Tunnel server.

What to do next

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

Configure Per App Tunnel Profile for Android

After you configured and installed the AirWatch 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 **AirWatch Tunnel**.
Connection Name	Enter a name for this connect. For example, **`AndroidSSO Configuration`**.
Server	The AirWatch Tunnel server URL is automatically entered.
Per-App VPN Rules	Select the **Per-App VPN Rules** 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.

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

- AirWatch 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 AirWatch 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 AirWatch 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 AirWatch Tunnel Guide on the AirWatch Resources Web site.

Prerequisites

- The AirWatch 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** > **AirWatch Tunnel > Network Traffic Rules**.

2 In the **Device Traffic Rules** tab, configure the device traffic rules settings as described in the AirWatch 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 **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.

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 In the Action column, select Proxy and specify the HTTPS proxy information. Enter **`certproxy.vmwareidentity.com:5262`**.

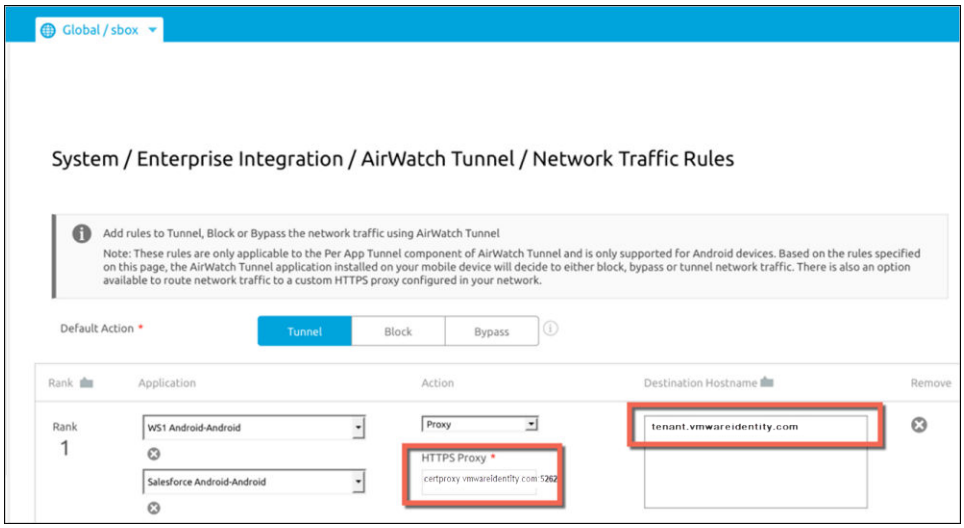
d In the Action column, select Proxy and specify the HTTPS proxy information. Enter the VMware Identity Manager host name and port. For example **`login.example.com:5262`**.

Note 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.

e 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 AirWatch Tunnel client routes the traffic to the HTTPS proxy from the VMware Identity Manager host name.

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

3 Click **Save**.



What to do next

Publish these rules. After the rules are published, the device receives an update VPN profile and the AirWatch 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. See the VMware Identity Manager Administration Guide.

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.

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
Enable Certificate Adapter	Select this check box to enable Mobile SSO for Android.
Root and Intermediate CA Certificate	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.
Uploaded CA Certificate Subject DNs	The contents of the uploaded certificate file is displayed here.
Use email if no UPN in certificate	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.
Certificate policies accepted	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 **Add another value** to add additional OIDs.
Enable Cert Revocation	Select the check box to enable certificate revocation checking. This prevents users who have revoked user certificates from authenticating.
Use CRL from certificates	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.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL.
Enable OCSP Revocation	Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP failure	If you configure both CRL and OCSP, you can check this box to fall back to using CRL if OCSAP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
OCSP Responder's Signing Certificate	Enter the path to the OCSP certificate for the responder. Enter as `/path/to/file.cer`

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.

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 AirWatch Tunnel proxy server.