Guide to Deploying VMware Workspace ONE UEM with VMware Workspace ONE Access

MARCH 2024

VMware Workspace ONE Access

vmware®
by Broadcom

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

https://docs.vmware.com/

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

Contents

Workspace ONE UEM Integration with Workspace ONE Access

1

To set up Workspace ONE® UEM mobile management services with Workspace ONE™ Access® service for single sign-on and identity management for users, you integrate Workspace ONE Access and Workspace ONE UEM services.

When the Workspace ONE UEM and Workspace ONE Access services are integrated, you can use Hub Services to configure how employees use the Workspace ONE® Intelligent Hub app to access apps, receive notifications, and search for people in your organization. Users from Workspace ONE UEM enrolled devices can log in to their Workspace ONE Intelligent Hub app to access their enabled applications securely without entering multiple passwords. Workspace ONE Access users can access their work resources from their Hub portal in a browser or from the Workspace ONE Intelligent Hub app on their devices.

To integrate Workspace ONE Access and Workspace ONE UEM, you run the Getting Started Wizard from the Workspace ONE UEM console to start the integration with Workspace ONE Access. Workspace ONE UEM generates the REST API keys and certificate and shares them with Workspace ONE Access to establish the trusted connection between the two services. You complete the set up in the Workspace ONE Access console.

For information about configuring Hub Services, see the Setting Up Hub Services to Support Workspace ONE Intelligent Hub guide.

Read the following topics next:

- Using the Getting Started Wizard to Connect Workspace ONE UEM with Workspace ONE Access
- Enabling Workspace ONE Access URL Endpoint in Workspace ONE Access Appliance (On premise only)
- Configure Workspace ONE UEM Integration in Workspace ONE Access
- Mapping Workspace ONE Access Domains to Multiple Organization Groups in Workspace ONE UEM
- Maintaining Your Workspace ONE UEM Integration with Workspace ONE Access

Using the Getting Started Wizard to Connect Workspace ONE UEM with Workspace ONE Access

You run the Getting Started Wizard in the Workspace ONE UEM console to connect the Workspace ONE UEM service to the Workspace ONE Access service and establish a trusted relationship between the two services.

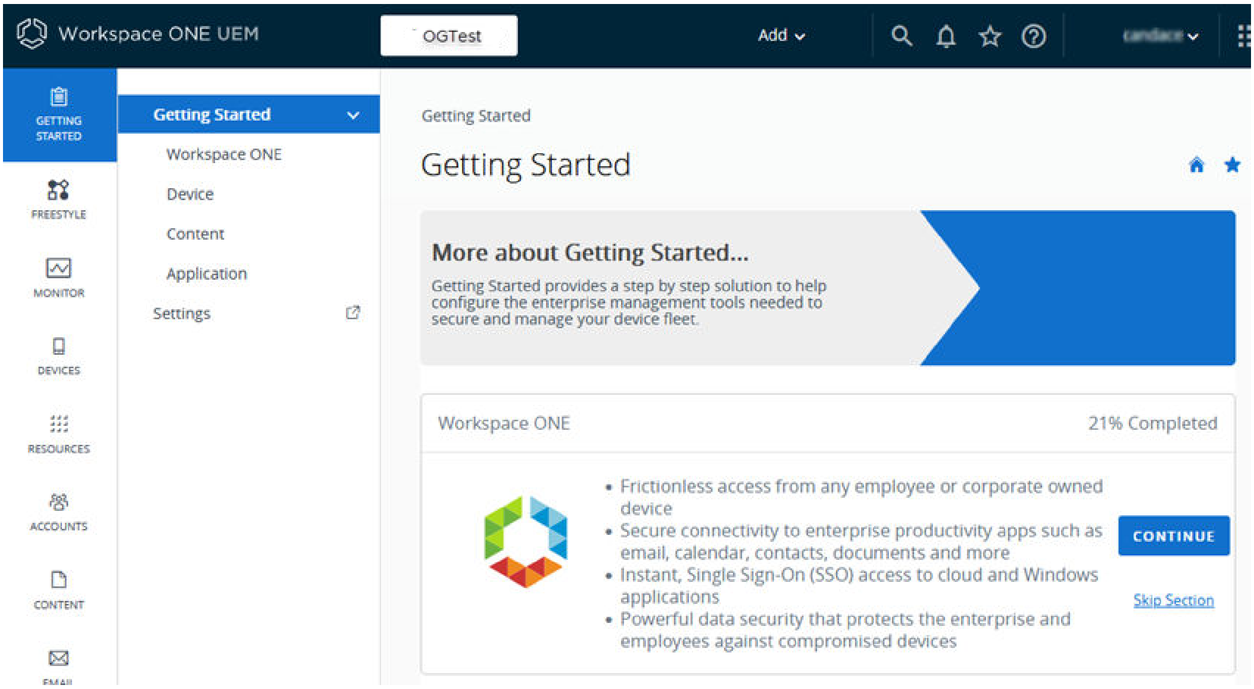
Before you can configure the integration, to establish a connection between Workspace ONE Access and Workspace ONE UEM, an OAuth 2.0 service client must be configured in Workspace ONE Access. The Workspace ONE Access OAuth 2.0 client ID and shared secret are configured in the Workspace ONE UEM console Getting Started wizard to establish the connection with Workspace ONE Access.

For newly created SaaS tenants, the OAuth 2.0 service client is generated on behalf of a new Workspace ONE Access client when the tenant is established. The information is prepopulated to the Getting Started wizard for that tenant.

For integration with an on-premises Workspace ONE Access deployment, the Workspace ONE Access admin generates the Workspace ONE Access OAuth 2.0 service client in the Workspace ONE Access console, Settings > OAuth 2.0 Management > UEM page. The UEM admin adds the client ID and shared secret to the Getting Started wizard when they start the configuration. See the Creating an OAuth 2.0 Service Client for Workspace ONE UEM article in the Workspace ONE Access Administration guide.

The Getting Started wizard serves as a checklist that walks you through the settings required to set up a Workspace ONE UEM and Workspace ONE Access. This configuration is set up in the Workspace ONE UEM console for the organization group of type **Customer**.

The Getting Started Wizard tracks how far along you are in the configuration process. You can start, pause, restart later, review, and change prior responses.



More about Getting Started...

Getting Started provides a step by step solution to help configure the enterprise management tools needed to secure and manage your device fleet.

Workspace ONE 21% Completed

- Frictionless access from any employee or corporate owned device
- Secure connectivity to enterprise productivity apps such as email, calendar, contacts, documents and more
- Instant, Single Sign-On (SSO) access to cloud and Windows applications
- Powerful data security that protects the enterprise and employees against compromised devices

Important Before you run the Getting Started Wizard, in the on-premises versions 23.09 and later Workspace ONE Access appliance, you must activate the API login URL endpoint `/SAAS/API/1.0/REST/auth/system/login` hosted by the Workspace ONE Access appliance. This is deactivated by default. See Enabling Workspace ONE Access URL Endpoint in Workspace ONE Access Appliance (On premise only).

1 In the Workspace ONE UEM console, click **Getting Started** > **Workspace ONE**.

2 Scroll down to the **Identity and Access Management** > **Connect to Workspace ONE Access** section and click **CONFIGURE**.

3 Enter your Workspace ONE Access tenant URL, the client ID and shared secret, if it is not prepopulated on the page.

   Click **TEST CONNECTION** to verify that Workspace ONE UEM and Workspace ONE Access services can communicate.

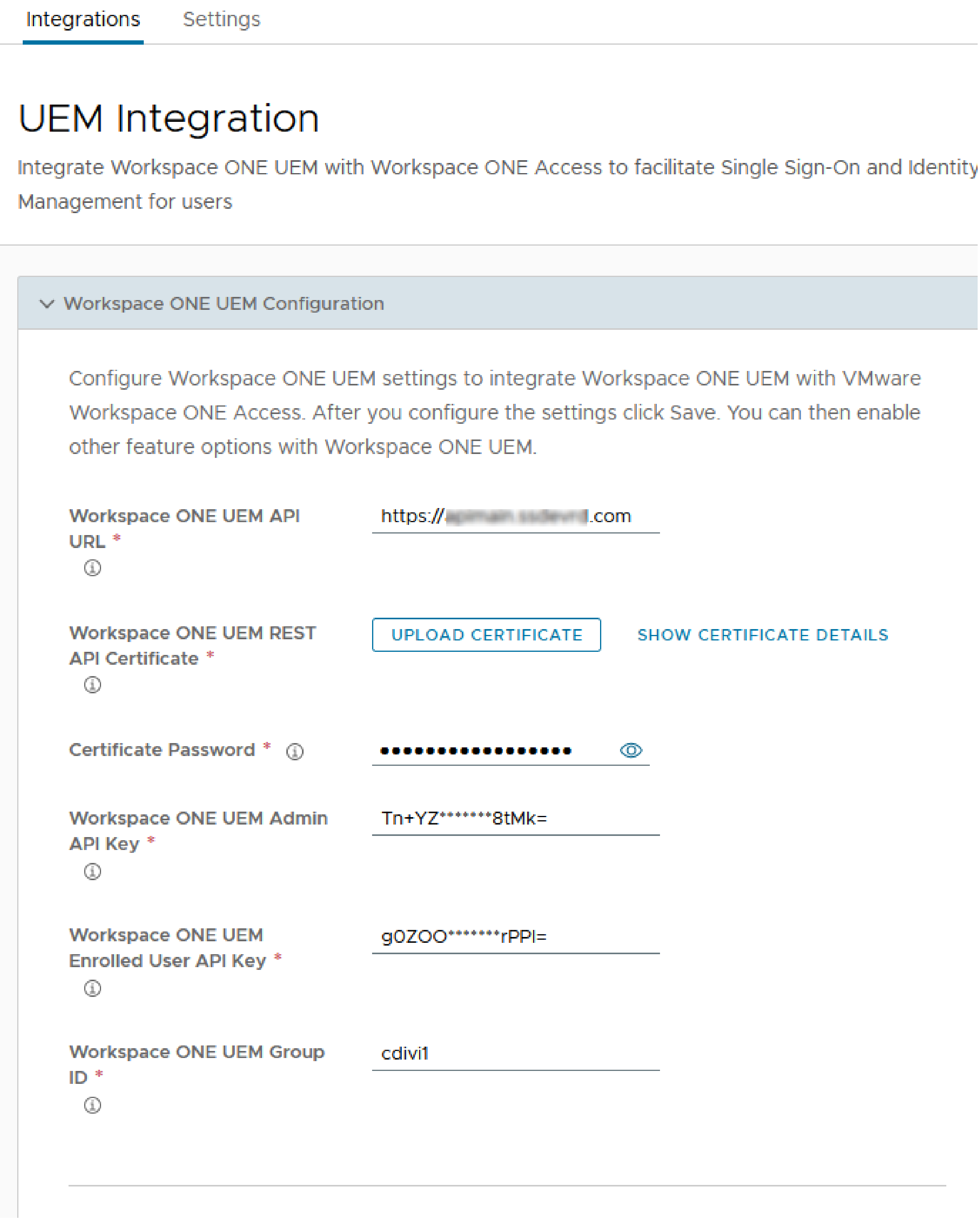
   Click **SAVE**.

   The wizard creates the service account and the API Keys that are exempt from the Workspace ONE UEM built-in rate limit.

4 Go to the **Settings** > **System** > **Devices & Users** > **General** > **Enrollment** page and scroll to **Source for Authentication for Intelligent Hub**, to verify that **Workspace ONE Access** is enabled.

The following settings are automatically configured in the Workspace ONE UEM console to establish a trusted relationship between the two services and the settings values are automatically populated to the Workspace ONE Access console Integrations > UEM Integration page.

- Basic administrator role of Console Administrator service account is created in your Organization Group.
- REST API Admin key is generated and shared with the Workspace ONE Access service to communicate between the services.
- REST API Enrollment User key is generated and shared with the Workspace ONE Access service.
- After the admin API key is created, an admin account is added and certificate authentication is set up in the Workspace ONE UEM console. For REST API certificate-based authentication, a user-level certificate is generated in the Workspace ONE UEM console. The certificate used is a self-signed Workspace ONE UEM certificate generated from the Workspace ONE UEM admin root cert.



UEM Integration

Integrate Workspace ONE UEM with Workspace ONE Access to facilitate Single Sign-On and Identity Management for users

Workspace ONE UEM Configuration

Configure Workspace ONE UEM settings to integrate Workspace ONE UEM with VMware Workspace ONE Access. After you configure the settings click Save. You can then enable other feature options with Workspace ONE UEM.

Workspace ONE UEM API URL * ⓘ: https://[redacted].com

Workspace ONE UEM REST API Certificate * ⓘ: UPLOAD CERTIFICATE | SHOW CERTIFICATE DETAILS

Certificate Password * ⓘ: ●●●●●●●●●●●●●●●●●●

Workspace ONE UEM Admin API Key * ⓘ: Tn+YZ*******8tMk=

Workspace ONE UEM Enrolled User API Key * ⓘ: g0ZOO*******rPPI=

Workspace ONE UEM Group ID * ⓘ: cdivi1

You complete setting up the integration with Workspace ONE UEM in the Workspace ONE Access console. See Configure Workspace ONE UEM Integration in Workspace ONE Access.

Enabling Workspace ONE Access URL Endpoint in Workspace ONE Access Appliance (On premise only)

When you use the Getting Started Wizard in the Workspace ONE UEM console to integrate an on-premises deployment of Workspace ONE Access version 23.09 with Workspace ONE UEM, you must activate the API login URL endpoint before you can start the integration. The login URL endpoint `/SAAS/API/1.0/REST/auth/system/login` hosted by the Workspace ONE Access appliance is deactivated by default.

To learn more about this Workspace ONE Access security setting, see Workspace ONE Access Security Settings Guidelines.

Enable/SAAS/API/1.0/REST/auth/system/login

Enable `/SAAS/API/1.0/REST/auth/system/login` so that system domain admin users can log into the Workspace ONE Access console.

Procedure

1 SSH into the Workspace ONE Access appliance as the root user.

2 To enable the login to the service node, enter

```
$cd /usr/local/horizon/bin
$hznAdminTool configureBreakGlassLogin -systemLogin -enable
```

3 Restart the service on the appliance. Enter **`service horizon-workspace restart`**.

Repeat this process for all appliances in your environment.

When `/SAAS/API/1.0/REST/auth/system/login` is enabled, the admin can use the Getting Started Wizard in the UEM console to integrate the Workspace ONE UEM and Workspace ONE Access services.

Deactivate /SAAS/API/1.0/REST/auth/system/login

After you configure the integration between Workspace ONE UEM with Workspace ONE Access, deactivate `/SAAS/API/1.0/REST/auth/system/login` as a login option.

Procedure

1 SSH into the Workspace ONE Access appliance as the root user.

2 To deactivate the login, enter

```
$cd /usr/local/horizon/bin
$hznAdminTool configureBreakGlassLogin -systemLogin -disable
```

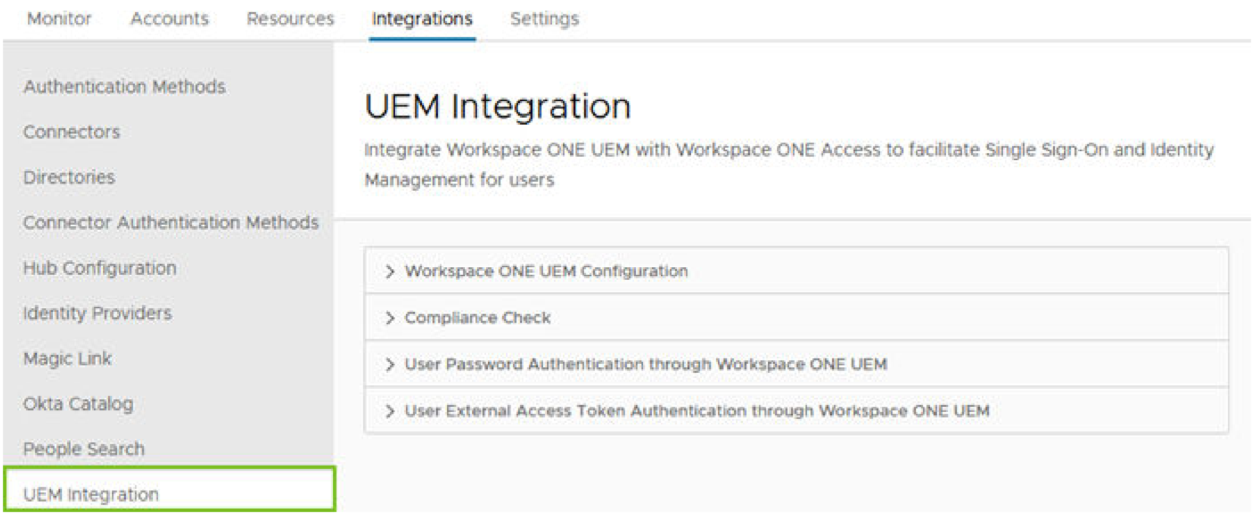
.

3 Restart the service on the appliance. Enter **`service horizon-workspace restart`**.

Repeat this process for all appliances in your environment.

Configure Workspace ONE UEM Integration in Workspace ONE Access

After you run the Getting Started wizard in the Workspace ONE UEM console to establish the trusted relationship between the two services, you go to the Workspace ONE Access console, to complete the setup.


Monitor
Accounts
Resources
Integrations
Settings
Authentication Methods
Connectors
Directories
Connector Authentication Methods
Hub Configuration
Identity Providers
Magic Link
Okta Catalog
People Search
UEM Integration
UEM Integration
Integrate Workspace ONE UEM with Workspace ONE Access to facilitate Single Sign-On and Identity Management for users
Workspace ONE UEM Configuration
Compliance Check
User Password Authentication through Workspace ONE UEM
User External Access Token Authentication through Workspace ONE UEM

Configuration Page	Description
Workspace ONE UEM Configuration	The Workspace ONE UEM settings created in the Getting Started wizard are populated to the UEM Integrations page in the Workspace ONE Access console. To complete the configuration, you can enable **Domain Mapping** and verify that the **App Catalog** setting is correct.
Compliance Check	You enable compliance checking in the Workspace ONE Access console Integrations > UEM Integration page and configure Device Compliance in the Integrations > Authentication Methods page to verify that Workspace ONE UEM managed devices adhere to Workspace ONE UEM compliance policies. When you configured Device Compliance authentication, you configure access policy rules to check the Workspace ONE UEM server for device compliance status when users sign in from their devices. See Enabling Compliance Checking for Workspace ONE UEM Managed Devices in Workspace ONE Access.

Configuration Page	Description
User Password Authentication through Workspace ONE UEM	Password Authentication with Workspace ONE UEM authenticates using AirWatch Cloud Connector through the Workspace ONE UEM service. When AirWatch Cloud Connector is used, you enable User Password Authentication through Workspace ONE UEM in the Workspace ONE Access console Integrations > UEM Integration page and configure Password (with Workspace ONE UEM) authentication in the Integrations > Authentication Methods page. You create access policies to apply to this authentication method. See Implementing Authentication with AirWatch Cloud Connector.
User External Access Token Authentication through Workspace ONE UEM	When users receive a new Dell® Windows 10+ device with out-of-box (OOBE) provisioning enabled in the Workspace ONE UEM Windows 10 Provisioning Service, you can enable **User External Access Token Authentication through Workspace ONE UEM** in the Workspace ONE Access console Integrations > UEM Integration page and configure Workspace ONE UEM External Access Token authentication in the Integrations > Authentication Methods page to manage Workspace ONE Intelligent Hub app logins.

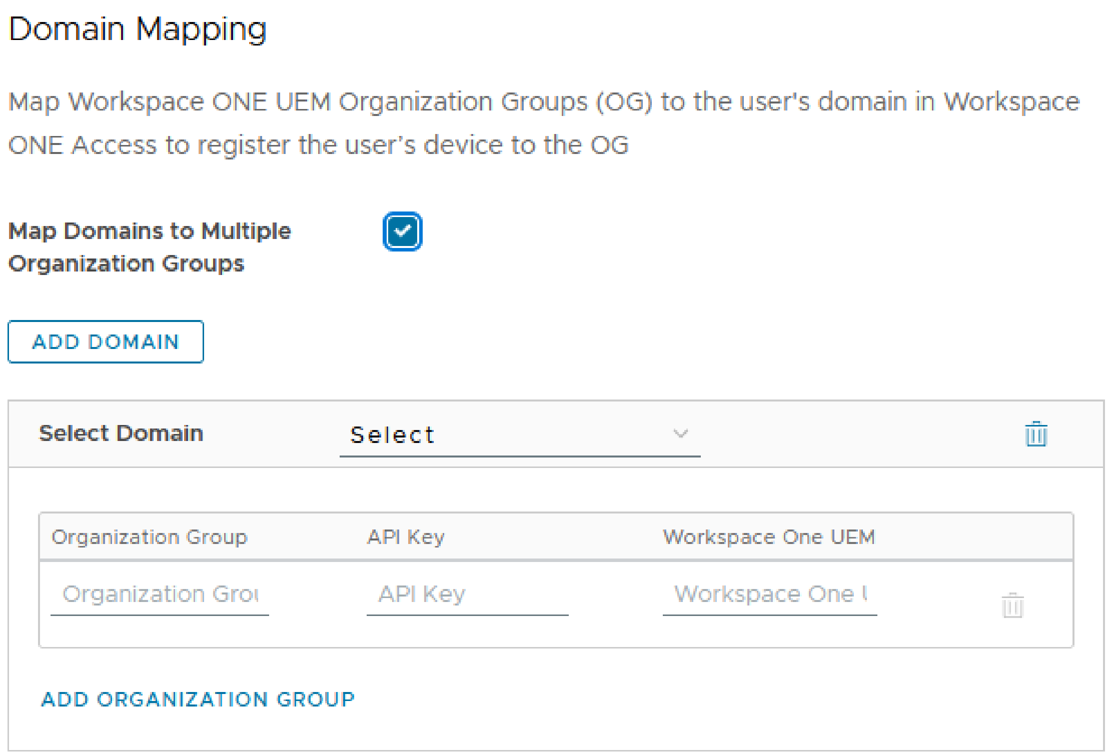
Enable Domain Mapping and Workspace ONE Intelligent Hub App Catalog

Enable **Domain Mapping** to map Workspace ONE UEM Organization Group (OG) to the user's domain in the Workspace ONE Access service to register that user's devices to the OG. See Mapping Workspace ONE Access Domains to Multiple Organization Groups in Workspace ONE UEM.

The **Fetch from Workspace ONE UEM** is automatically enabled in the **Catalog** section to include apps from the Workspace ONE UEM catalog. The Workspace ONE Intelligent Hub app catalog displays web and virtual apps configured in the Workspace ONE Access console and native apps and web links configured in the Workspace ONE UEM console. The Device Service URL for new device enrollment with UEM is automatically configured.

1 In the Workspace ONE Access console **Integrations > UEM Integration** page, scroll down to the **Domain Mapping** section.

2 Enable **Map Domains to Multiple Organization Groups**.



Domain Mapping

Map Workspace ONE UEM Organization Groups (OG) to the user's domain in Workspace ONE Access to register the user's device to the OG

Map Domains to Multiple Organization Groups ☑

ADD DOMAIN

Select Domain: Select

Organization Group	API Key	Workspace One UEM
Organization Grou	API Key	Workspace One U

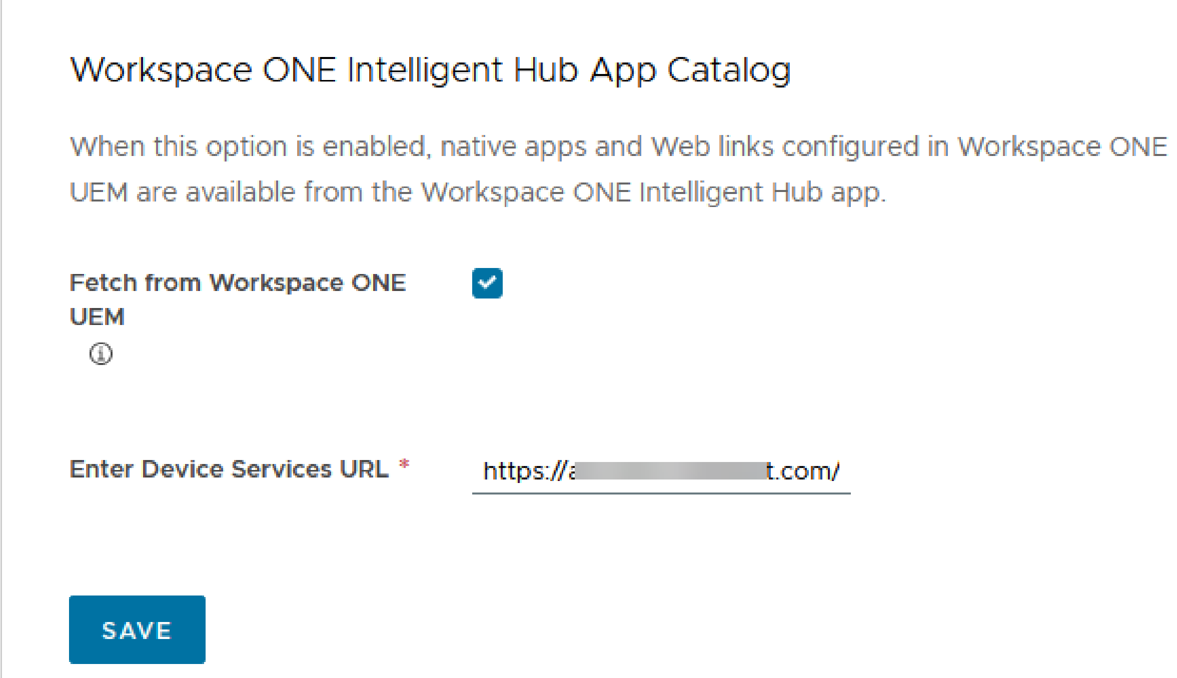
ADD ORGANIZATION GROUP

a Select a domain from the drop-down menu.

b Add the Workspace ONE UEM organization group for that domain, the API key, and the Workspace ONE UEM name.

Click **ADD ORGANIZATION GROUP** to add another organization group to the domain.

3 Verify that **Fetch from Workspace ONE UEM** is selected and the Device Services URL listed is correct.



Workspace ONE Intelligent Hub App Catalog

When this option is enabled, native apps and Web links configured in Workspace ONE UEM are available from the Workspace ONE Intelligent Hub app.

Fetch from Workspace ONE UEM ⓘ ☑

Enter Device Services URL * https://[redacted].com/

4 Click **Save** if you made any changes.

Mapping Workspace ONE Access Domains to Multiple Organization Groups in Workspace ONE UEM

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

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

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

The device organization groups must be identified when Workspace ONE UEM is integrated with Workspace ONE Access so that identity manager can locate the user and successfully register the device into the appropriate organization group.

When you configure the Workspace ONE UEM settings in the Workspace ONE Access service, you can enter device organization group IDs and the API keys to map multiple OG to a domain. When users sign into the Workspace ONE Intelligent Hub app from their devices, the user records are verified and the device is registered to the appropriate organization group in Workspace ONE UEM.

To learn more about how to configure multiple organization groups, see Deployment Strategies for Setting Up Multiple Workspace ONE UEM Organization Groups.

Note When Workspace ONE UEM is integrated with Workspace ONE Access and multiple Workspace ONE UEM organization groups are configured, the Active Directory Global Catalog option cannot be configured for use with the Workspace ONE Access service.

Map Organization Groups in Workspace ONE UEM to Workspace ONE Access Domains

Link domains configured in the Workspace ONE Access service to specific organization groups in Workspace ONE UEM to manage device registration through Workspace ONE UEM.

See Deployment Strategies for Setting Up Multiple Workspace ONE UEM Organization Groups to learn about different strategies to configuring organization groups for a domain.

Procedure

1. In the Workspace ONE Access console **Integrations > UEM Integration** page, navigate to the **Advanced Workspace ONE UEM** Configuration section.
2. Enable **Map Domains to Multiple Organization Groups**.
3. Select a domain from the drop-down menu next to the green +.
4. Configure the specific Workspace ONE organization group ID for that domain. Enter the organization group ID name, API key, and the Workspace ONE domain name.

   You can map multiple organization groups to the domain.
5. Click **Save**.

Deployment Strategies for Setting Up Multiple Workspace ONE UEM Organization Groups

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

When users sign into the Workspace ONE Intelligent Hub app from a device, a device registration event is triggered within Workspace ONE Access. A request is sent to Workspace ONE UEM to pull any applications that the user and device combination is entitled to. The request is sent using the REST API to locate the user within Workspace ONE UEM and to place the device in the appropriate organization group.

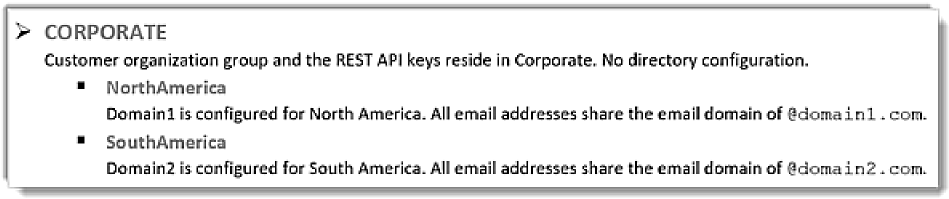
To manage organization groups in Workspace ONE Access, map Workspace ONE UEM organization groups to domains in the Workspace ONE Access service.

If Workspace ONE UEM organization groups are not mapped to domains in the Workspace ONE Access service, the Workspace ONE Intelligent Hub app attempts to locate the user at the organization group where the REST API key is created. That group is the **Customer** group.

Using Workspace ONE UEM Auto Discovery

Make sure that Auto Discovery is set up in the Workspace ONE UEM console. Set up Auto Discovery when a single directory is configured at a child group to the Customer Organization Group, or when multiple directories are configured below the Customer group with unique email domains.

Figure 1-1. Example 1



➢ CORPORATE

Customer organization group and the REST API keys reside in Corporate. No directory configuration.

- NorthAmerica

  Domain1 is configured for North America. All email addresses share the email domain of `@domain1.com`.
- SouthAmerica

  Domain2 is configured for South America. All email addresses share the email domain of `@domain2.com`.

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

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

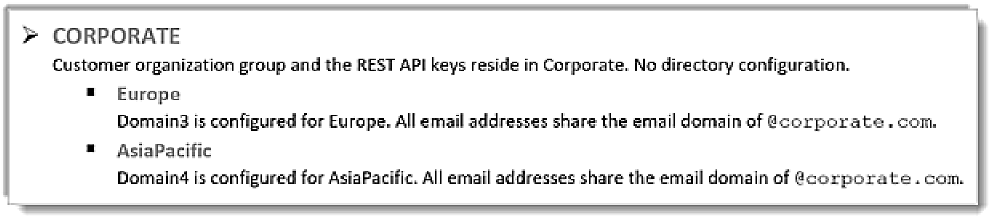
Using Workspace ONE UEM Organization Group Mapping to Workspace ONE Access Domains

Configure the Workspace ONE Access service to the Workspace ONE UEM organization group mapping when multiple directories are configured with the same email domain. You enable **Map Domains to Multiple Organization Groups** in the Integrations > UEM Integration page in the Workspace ONE Access console.

When the Map Domains to Multiple Organization Groups option is enabled, domains configured in Workspace ONE Access can be mapped to the Workspace ONE UEM organization group IDs. The admin REST API key is also required.

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

Figure 1-2. Example 2



➢ CORPORATE

Customer organization group and the REST API keys reside in Corporate. No directory configuration.

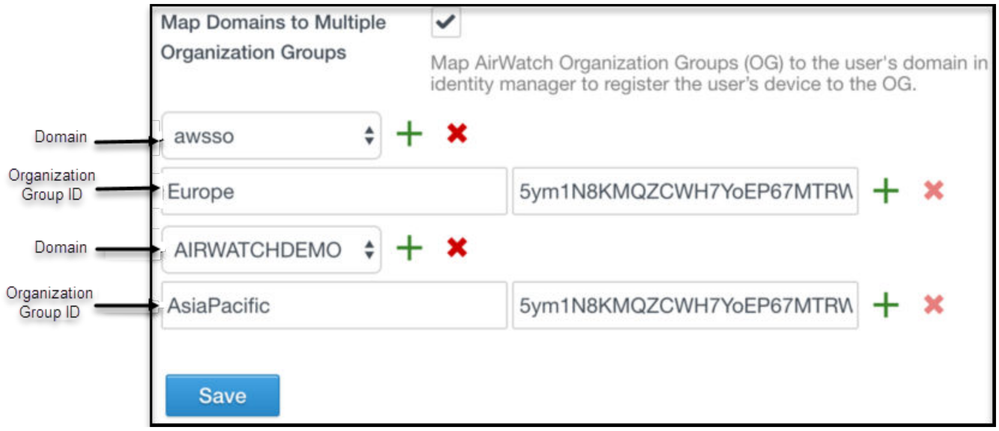
- Europe

  Domain3 is configured for Europe. All email addresses share the email domain of `@corporate.com`.
- AsiaPacific

  Domain4 is configured for AsiaPacific. All email addresses share the email domain of `@corporate.com`.

In the UEM Integration configuration page in the Workspace ONE Access console, configure a specific Workspace ONE UEM organization group ID for each domain.

Figure 1-3. Example 2 Organization Group Configuration



Map Domains to Multiple Organization Groups ☑

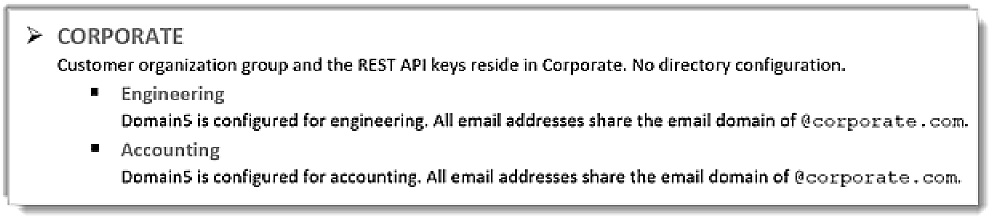
Map AirWatch Organization Groups (OG) to the user's domain in identity manager to register the user's device to the OG.

awsso	
Europe	5ym1N8KMQZCWH7YoEP67MTRW
AIRWATCHDEMO	
AsiaPacific	5ym1N8KMQZCWH7YoEP67MTRW

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

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

Figure 1-4. Example 3



➢ CORPORATE

Customer organization group and the REST API keys reside in Corporate. No directory configuration.

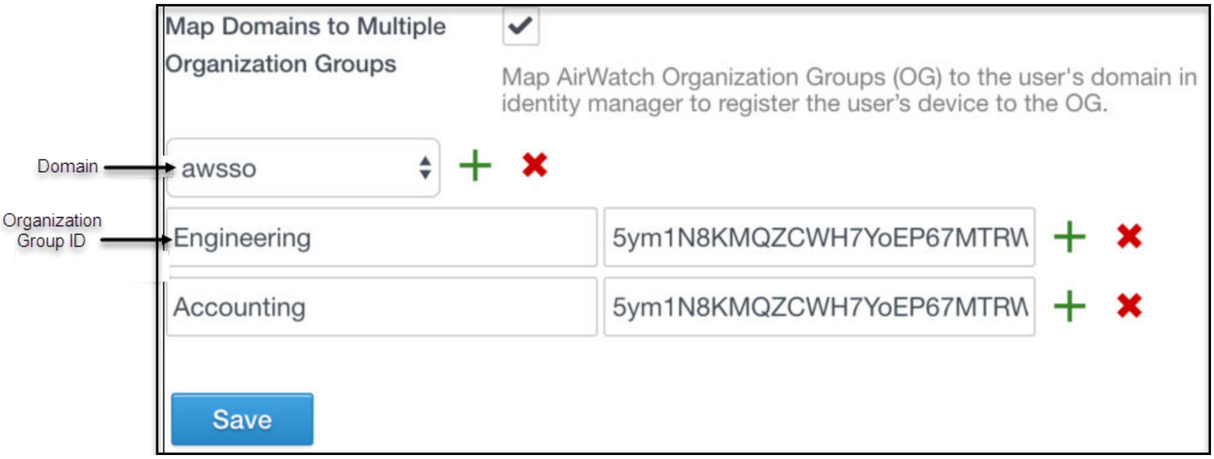
- Engineering

  Domain5 is configured for engineering. All email addresses share the email domain of `@corporate.com`.
- Accounting

  Domain5 is configured for accounting. All email addresses share the email domain of `@corporate.com`.

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

Figure 1-5. Organization Groups Where Directories Share the same Domain



Map Domains to Multiple Organization Groups ☑

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

Domain: awsso

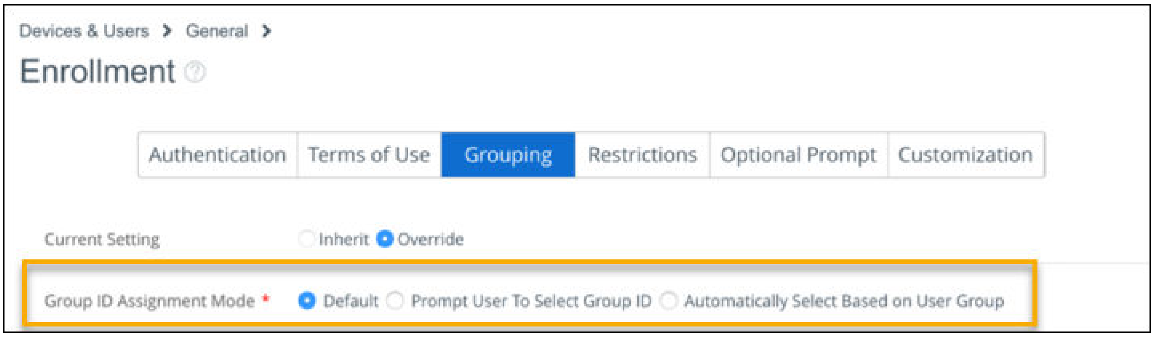
Organization Group ID:

Engineering	5ym1N8KMQZCWH7YoEP67MTRW
Accounting	5ym1N8KMQZCWH7YoEP67MTRW

Placing Devices in the Correct Organization Group

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

Figure 1-6. Workspace ONE UEM Group Enrollment for Devices



Devices & Users > General >

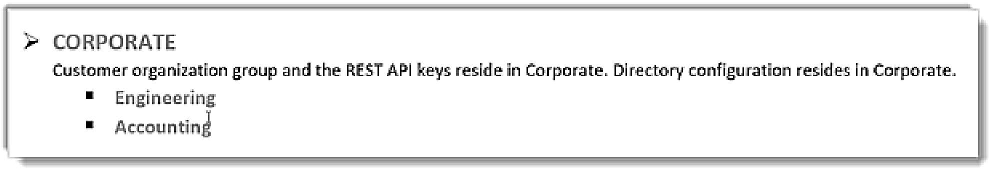
Enrollment

Current Setting ○ Inherit ● Override

Group ID Assignment Mode * ● Default ○ Prompt User To Select Group ID ○ Automatically Select Based on User Group

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

Figure 1-7. Example 4



➢ CORPORATE

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

- Engineering
- Accounting

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

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

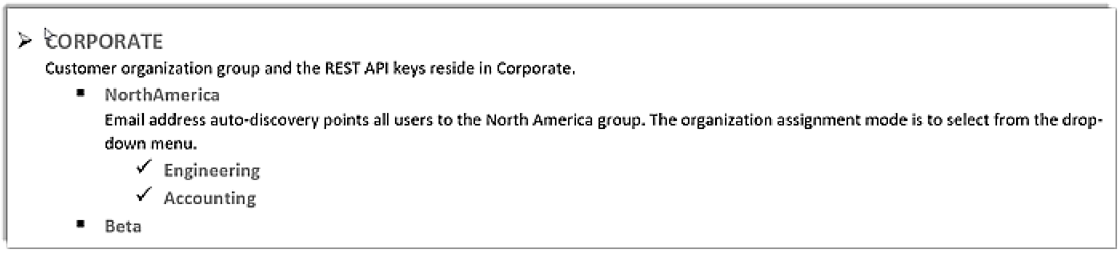
- If Prompt User to Select Group ID is selected, users are prompted to select which group to register their device into. For example 4, users see a drop-down menu within the Workspace ONE Intelligent Hub app with Engineering and Accounting as options.
- If Automatically Selected Based on User Group is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

Understanding the Concept of a Hidden Group

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

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

Figure 1-8. Example 5



- ➢ CORPORATE
  Customer organization group and the REST API keys reside in Corporate.
  - ▪ NorthAmerica
    Email address auto-discovery points all users to the North America group. The organization assignment mode is to select from the drop-down menu.
    - ✓ Engineering
    - ✓ Accounting
  - ▪ Beta

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

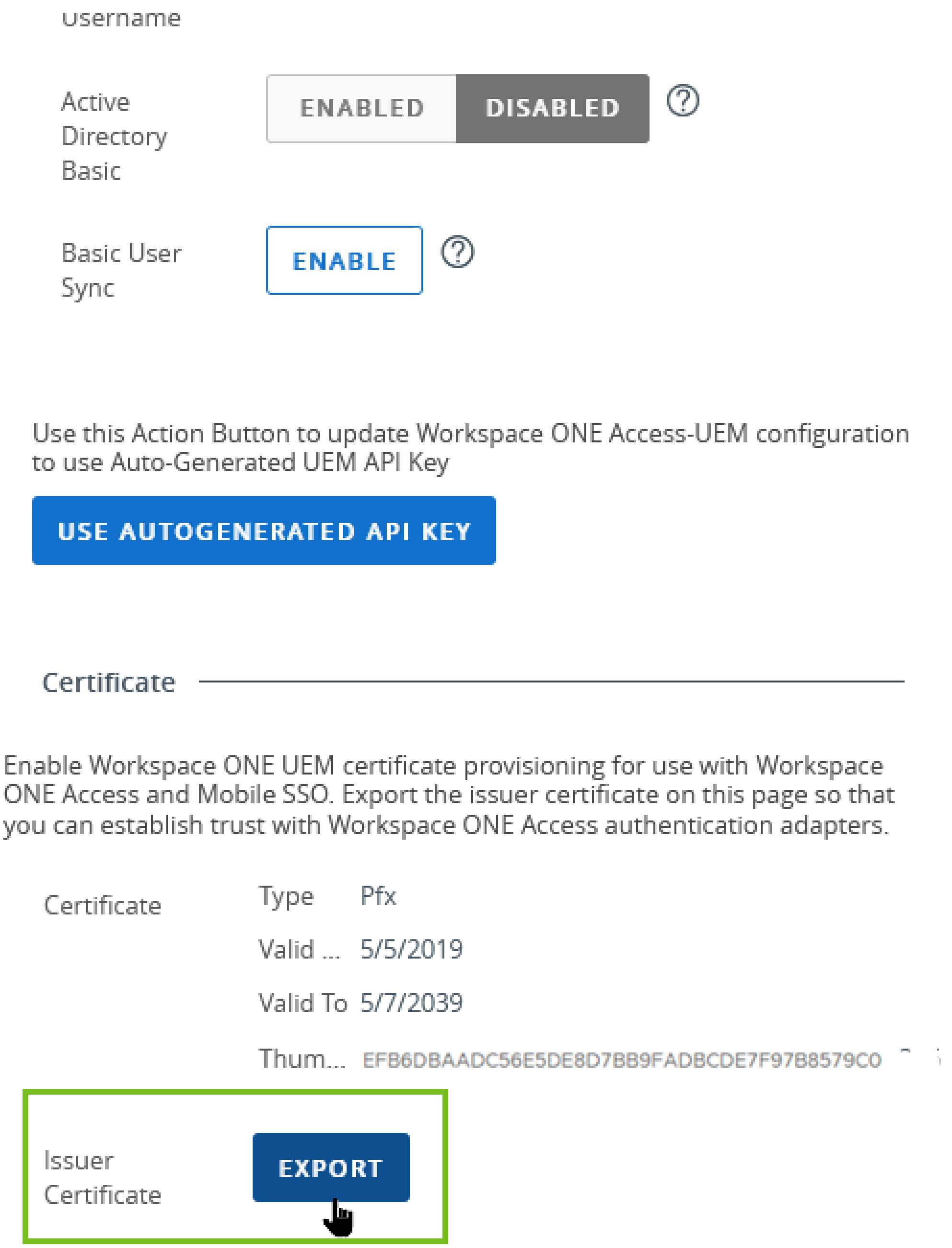
Maintaining Your Workspace ONE UEM Integration with Workspace ONE Access

When you change settings in the Workspace ONE UEM console that are integrated with the Workspace ONE Access service, you must also update the settings in the Workspace ONE Access console, Integrations > UEM Integrations page. Otherwise, Workspace ONE Access and Hub Services cannot communicate with Workspace ONE UEM.

Updating Workspace ONE Access Service after REST API Certificate Regenerated in Workspace ONE UEM

When the REST API certificate is regenerated in the Workspace ONE UEM console, you must manually upload and save the REST API certificate in the Workspace ONE Access console.

1 In the Workspace ONE UEM console **Settings > Enterprise Integration > Workspace ONE Access > Configuration** page, export the certificate and save the file.



Username

Active Directory Basic: ENABLED **DISABLED**

Basic User Sync: ENABLE

Use this Action Button to update Workspace ONE Access-UEM configuration to use Auto-Generated UEM API Key

Certificate

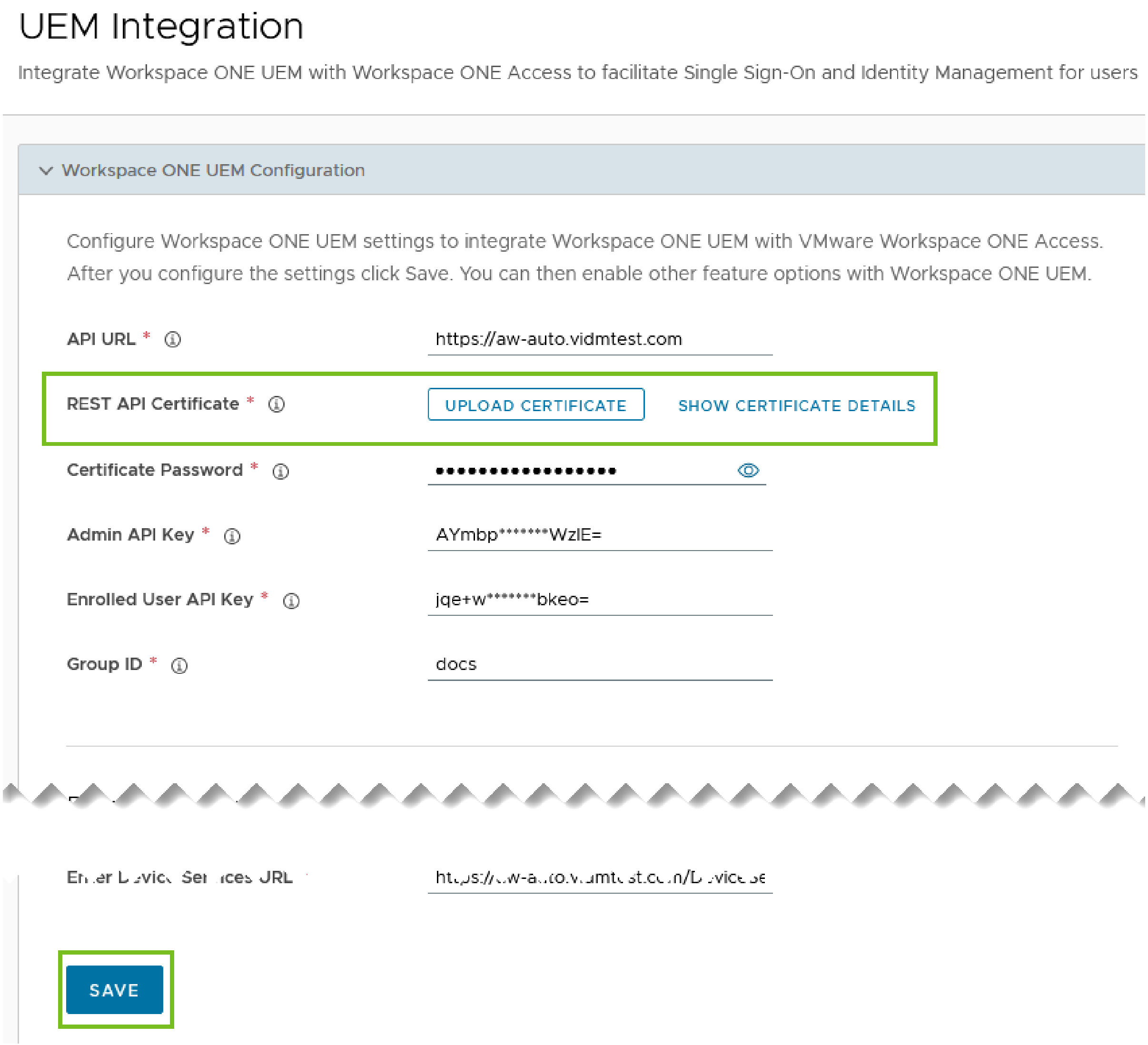
Enable Workspace ONE UEM certificate provisioning for use with Workspace ONE Access and Mobile SSO. Export the issuer certificate on this page so that you can establish trust with Workspace ONE Access authentication adapters.

Certificate	Type	Pfx
	Valid ...	5/5/2019
	Valid To	5/7/2039
	Thum...	EFB6DBAADC56E5DE8D7BB9FADBCDE7F97B8579C0

Issuer Certificate

2 In the Workspace ONE Access console **Integrations > UEM Integration** page **REST API Certificate** setting row, click **UPLOAD CERTIFICATE**. Navigate to the saved certificate and select the file to upload.

3 Scroll down to the **Workspace ONE Catalog** section and click **SAVE**.



UEM Integration

Integrate Workspace ONE UEM with Workspace ONE Access to facilitate Single Sign-On and Identity Management for users

Workspace ONE UEM Configuration

Configure Workspace ONE UEM settings to integrate Workspace ONE UEM with VMware Workspace ONE Access. After you configure the settings click Save. You can then enable other feature options with Workspace ONE UEM.

API URL *: https://aw-auto.vidmtest.com

REST API Certificate *: UPLOAD CERTIFICATE | SHOW CERTIFICATE DETAILS

Certificate Password *: •••••••••••••••••

Admin API Key *: AYmbp*******WzIE=

Enrolled User API Key *: jqe+w*******bkeo=

Group ID *: docs

Enter Device Services URL: https://aw-auto.vidmtest.com/DeviceSe

4 Verify that the thumbprint identifier is the same in Workspace ONE Access, Hub Services, and Workspace ONE UEM.

- In the Workspace ONE UEM console, go to the **Settings > Enterprise Integration > Workspace ONE Access > Configuration** page and scroll to the Certificate section to view the thumbprint identifier.
- In the Workspace ONE Access console, go to the **Integrations > UEM Integration** page, and in the Workspace ONE UEM Configuration section, click **SHOW CERTIFICATE DETAILS**. Verify that the thumbprint identifier is the same identifier as on the Workspace ONE UEM console.
- In the Hub Services console, go to **System Settings > API Certificate** and click **Show Details**. Verify that the thumbprint identifier is the same identifier as on the Workspace ONE UEM console.

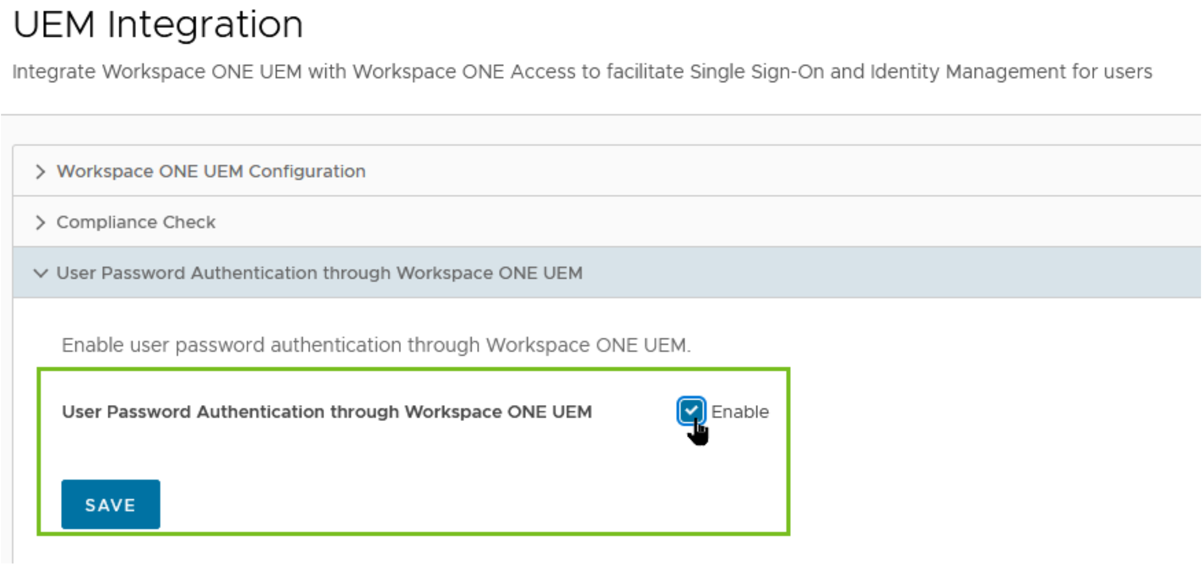
Updating the Connection after AirWatch Cloud Connector is Upgraded in Workspace ONE UEM

When you upgrade the AirWatch Cloud Connector software, make sure that you update the Workspace ONE UEM integration configuration in the Workspace ONE Access console to update the Password (with Workspace ONE UEM) authentication method configuration.

1 In the Workspace ONE Access **Settings** > **Enterprise Integration** > **Workspace ONE Access** > **Configuration** page, select **User Password Authentication through Workspace ONE UEM**

2 Deactivate and then reactivate the setting.

3 Click **SAVE**.



UEM Integration

Integrate Workspace ONE UEM with Workspace ONE Access to facilitate Single Sign-On and Identity Management for users

Enable user password authentication through Workspace ONE UEM.

User Password Authentication through Workspace ONE UEM ☑ Enable

> Workspace ONE UEM Configuration
> Compliance Check
User Password Authentication through Workspace ONE UEM
SAVE

4 Go to the **Integrations** > **Authentication Methods** page and select **Password (with Workspace ONE UEM)** to verify that the settings on the page were updated.

Configure Workspace ONE Access for Single Sign-On Authentication from Workspace ONE UEM Devices

2

When Workspace ONE UEM and Workspace ONE Access services are integrated, users from Workspace ONE UEM enrolled devices can log in to their Workspace ONE Intelligent Hub app to access their enabled apps without entering multiple passwords.

To set up single sign-on authentication for Workspace ONE UEM devices, complete the following tasks in the Workspace ONE Access console..

- Map Workspace ONE UEM directory user attributes to Workspace ONE Access directory user attributes and sync users to the Workspace ONE Access directory.
- Implement the password authentication method for AirWatch Cloud Connector and set up the access policy rules.
- Enable device compliance checking to verify that managed devices adhere to Workspace ONE UEM compliance policies and set up conditional access policies to include compliance checking rules.
- Enable and configure the external access token authentication method.

Read the following topics next:

- Syncing Workspace ONE UEM Users to Workspace ONE Access Directories
- Implementing Authentication with AirWatch Cloud Connector
- Enabling Compliance Checking for Workspace ONE UEM Managed Devices in Workspace ONE Access
- Configuring Access Policies in Workspace ONE Access to Manager User Access to Their Apps in Hub Catalog

Syncing Workspace ONE UEM Users to Workspace ONE Access Directories

When Workspace ONE Access and Workspace ONE UEM services are integrated, UEM user accounts are synchronized from the UEM console to the Workspace ONE Access console to enable Workspace ONE UEM users single sign-on access to the Workspace ONE Intelligent Hub app and their app resources without requiring reauthentication.

In the Workspace ONE UEM console, you can set up either Directory-based account access to user accounts, or you can create local basic user accounts that are not integrated to your UEM directory service. When you integrate with the Workspace ONE Access service, you select which type of user accounts to sync to the Workspace ONE Access service.

Important Make sure that the users and groups synced by the Workspace ONE UEM service to the Workspace ONE Access directory are unique. You should not sync the same user and groups via a Workspace ONE Access specific directory from the same source directory server (Active Directory or OpenLDAP). This is because the users/groups could share the same externalId. If duplicate user and groups are synced, it might cause directory sync to fail in the Workspace ONE Access Connector Directory Sync Service.

You can also use third-party identity providers such as Okta and Ping to provide single sign-on authentication to the Workspace ONE Intelligent Hub app. See Third-Party Identity Providers as an Application Source for more information.

Syncing Directory-Based Accounts from Your Workspace ONE UEM Directory Service

Directory-based account access is used when your organization's existing directory service is integrated with Workspace ONE UEM. The directory-based users are synchronized to the Workspace ONE Access directory.

In the Workspace ONE Access console, you create a directory and specify the connection details. You configure the user attribute mapping between the Workspace ONE UEM directory and the Workspace ONE Access directory. See the Directory Integration with Workspace ONE Access guide for detailed information about configuring a directory in the Workspace ONE Access service.

In the Workspace ONE UEM console, you configure the Workspace ONE Access settings to establish a connection between your organization group instance of the Workspace ONE UEM directory and Workspace ONE Access directory.

Synchronization of directory information between Workspace ONE UEM and Workspace ONE Access occurs on the same schedule as the Workspace ONE UEM directory sync. Users are also synced to the Workspace ONE Access service immediately when an administrator manually adds a user or from a bulk import.

Managing User Attributes Mapping

You can configure the user attribute mapping between the Workspace ONE UEM directory and the Workspace ONE Access directory.

The User Attributes page in the Workspace ONE Access console Settings page lists the default directory attributes that are mapped to Workspace ONE UEM directory attributes. Attributes that are required are marked with an asterisk. Users missing a required attribute in their profile are not synced to the Workspace ONE Access service.

Table 2-1. Default Workspace ONE UEM Directory Attributes Mapping

Workspace ONE Access User Attribute Name	Default Mapping to Workspace ONE UEM 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 Workspace ONE UEM Directory to Workspace ONE Access Directory

You configure the Workspace ONE Access settings in the Workspace ONE UEM console to establish a connection between your organization group instance of the Workspace ONE UEM directory and Workspace ONE Access. This connection is used to sync users and groups to a directory created in the Workspace ONE Access service.

You initially manually sync users and groups to the Workspace ONE Access directory. After the initial sync, the Workspace ONE UEM sync schedule determines when users and groups are synced with the Workspace ONE Access directory.

When you add or delete a user or a group on the Workspace ONE UEM server, the change is reflected on the Workspace ONE Access service immediately.

Prerequisites

- Workspace ONE Access local admin name and password.
- Identify attribute values to map from the Workspace ONE UEM directory. See Managing User Attributes Mapping.

Procedure

1 In the Workspace ONE UEM console, Groups & Settings, All Settings page, select your organization group and navigate to **System > Enterprise Integration > Workspace ONE Access > Configuration**.

2 In the Server section, click **Configure**.

Note The **Configure** 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 Workspace ONE Access settings.

Option	Description
URL	Enter your tenant VMware URL. For example, `https://myco.ws1a.com`.
Admin user name	Enter the Workspace ONE Access local admin user name.
Admin Password	Enter the Workspace ONE Access local admin user's password.

4 Click **Next**.

5 Enable custom mapping to configure the user attributes mapping from Workspace ONE UEM to the Workspace ONE Access service.

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

7 Click **Sync Now** to manually sync all users and groups to Workspace ONE Access service.

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

Results

A directory is created in the Workspace ONE Access service and the Workspace ONE UEM users and groups are synced to a directory in Workspace ONE Access.

What to do next

Review the Users and Groups page in the Workspace ONE Access console to verify that the user and group names are synced.

Syncing Workspace ONE UEM Local Basic User Accounts to Workspace ONE Access

To set up basic user account types to use single sign-on to the Intelligent Hub app, you enable the Local Basic User feature in the UEM console for your organization group.

The first synchronization to the Workspace ONE Access service after this feature is enabled creates a directory of type **Other** in the Workspace ONE Access service.

The directory name is **`UEMLocalDirectory_{groupid}`**. All basic users from the selected UEM organization group are added to that directory. When basic user accounts are added, changed, or deleted in the UEM console, the change is immediately synced to the UEMLocal Directory.

Enable Basic User Sync to Add Local Users to Workspace ONE Access Local UEM Directory

Sync basic user accounts to the Workspace ONE Access service. When basic accounts are synced, users can use the Workspace ONE Intelligent Hub app for single sign-on access to their app resources.

Prerequisites

Procedure

1 In the Workspace ONE UEM console Groups & Settings, All Settings page, select your Global > Customer-level organization group and navigate to **System > Enterprise Integration> Workspace ONE Access**.

2 Click **Configuration**.

The Workspace ONE Access page opens and your tenant URL and admin name are listed in the Server section.

3 Select **Enabled** for **Basic User Sync**.

4 In the Map Attribute section that displays, select the basic user attribute to sync to the Workspace ONE Access Local UEM directory.

5 Click **Save**.

Results

A directory named `UEMLocalDirectory_{your-groupid}` is created in the Workspace ONE Access service and basic users are synced to the directory.

Note If the sync to the Workspace ONE Access service fails for any reason, click **Sync Now** to start the sync again.

What to do next

Review the Users and Groups page in the Workspace ONE Access console to verify that the all basic users are synced.

Implementing Authentication with AirWatch Cloud Connector

The AirWatch Cloud Connector (ACC) in the Workspace ONE UEM service is integrated with VMware Workspace ONE Access for user password authentication in the Workspace ONE Intelligent Hub app.

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

To implement AirWatch Cloud Connector authentication for Workspace ONE Intelligent Hub, in the Workspace ONE Access console, you associate the Password (Workspace ONE UEM) authentication method to a built-in identity provider.

You can enable just-in-time support in Workspace ONE UEM to add new users to the 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 Workspace ONE UEM server to access Workspace ONE Intelligent Hub. Instead, new users sign in to their Workspace ONE Intelligent Hub portal, either from an iOS or Android device or from their desktop computer and enter their Active Directory user name and password. The VMware Workspace ONE Access service authenticates the Active Directory credentials through the AirWatch Cloud Connector and adds the user profile to the directory.

Managing Configuration of Password Authentication with Workspace ONE UEM in Workspace ONE Access

The Password (Workspace ONE UEM) authentication method authenticates using AirWatch Cloud Connector through the Workspace ONE UEM service. You enable **User Password Authentication through Workspace ONE UEM** in the Workspace ONE Access console Integrations > UEM Integration page and associate the authentication method to a built-in identity provider.

Important The Password Authentication with Workspace ONE UEM authentication method does not work when Workspace ONE UEM is unreachable or unavailable for any reason, including planned maintenance and unplanned outages.

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

Procedure

1 In the Workspace ONE Access console **Integrations > UEM Integrations** page, enable **Workspace ONE UEM Password Authentication** and click **Save**.

The AirWatch Cloud Connector configuration details are saved to the **Integrations > Authentication Methods > Password (with Workspace ONE UEM)** page.

2 In the **Integrations > Authentication Methods** page, select **Password (with Workspace ONE UEM)** and click **CONFIGURE**.

3 Set the **Number of authentication attempts** allowed. The other text boxes are pre-popuated with the configured Workspace ONE UEM values.

Option	Description
Enable Workspace ONE UEM Password Authentication	When enabled Workspace ONE UEM password authentication is available as an authentication method.
Workspace ONE UEM Admin Console URL	Prepopulated with the Workspace ONE UEM URL.
Workspace ONE UEM API Key	Prepopulated with the Workspace ONE UEM Admin API key.
Workspace ONE UEM Group ID	Prepopulated with the organization group ID.
Number of authentication attempts allowed	The maximum number of failed login attempts when using the Workspace ONE UEM password for authentication. No more login attempts are allowed after the failed logins reach this number. The Workspace ONE Access service tries to use the fallback authentication method if it is configured. The default is five attempts.

4 Click **SAVE**.

Important When the Workspace ONE UEM service details applicable to this authentication method change, make sure that you update the Workspace ONE UEM configuration in the Workspace ONE Access console. Otherwise this authentication method might fail.

What to do next

Enable Password (with Workspace ONE UEM) as an authentication method in a built-in identity provider.

Configure Built-in Identity Providers in Workspace ONE Access

You can configure multiple built-in identity providers and associate authentication methods that are configured in the Workspace ONE Access console, Integrations > Authentication Methods page.

Procedure

1 In the Workspace ONE Access console **Integrations > Identity Providers** page, click **Add** and select **Built-in IDP**.

Option	Description
Identity Provider Name	Enter the name for this built-in identity provider instance.
Users	Select the directories that include the users to authenticate.
Authentication Method	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.
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.

2 Click **SAVE**.

What to do next

Configure the default access policy rule to add the authentication policy to the rule. See the Managing User Authentication Methods in VMware Workspace ONE Access guide.

Enabling Compliance Checking for Workspace ONE UEM Managed Devices in Workspace ONE Access

When users enroll their devices in Workspace ONE UEM, 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 Workspace ONE UEM console. If the device goes out of compliance, corresponding actions configured in the UEM console are taken.

The Workspace ONE Access service includes an access policy option that can be configured to check the Workspace ONE UEM server for device compliance status when users sign in from the device. The compliance check ensures that users are blocked from signing into an application or using single sign-in to the user's portal if the device goes out-of-compliance. When the device is compliant again, the ability to sign in is restored.

The Workspace ONE Intelligent Hub app 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 UEM console unenrolls the device and removes the managed applications from the device. Unmanaged applications are not removed.

For more information about Workspace ONE UEM compliance policies, see the VMware Workspace ONE UEM Mobile Device Management guide, in the Workspace ONE UEM Documentation Center.

Important The Device Compliance authentication method does not work when Workspace ONE UEM is unreachable or unavailable for any reason, including planned maintenance and unplanned outages.

How to Enable Compliance Checking in Workspace ONE Access

In the Workspace ONE Access console, enable device compliance in the Integrations > Workspace ONE UEM configuration page and configure Device Compliance in the Authentication Methods page.

1 Go to the Workspace ONE Access console **Integrations > UEM Integration** > page, **Device Compliance Check** section and select **Enable**.

2 Click **Save**.

3 Go to the **Integrations > Authentication Methods** page, and select **Device Compliance (with Workspace ONE UEM)**

4 Set the maximum number of failed login attempts. The other text boxes are prepopulated with the configured Workspace ONE UEM values.

Option	Description
Enable Device Compliance Adapter	Select this check box to enable Workspace ONE UEM password authentication.
Workspace ONE UEM Admin Console URL	Pre-populated with the Workspace ONE UEM URL that you set up on the AirWatch configuration page.
Workspace ONE UEM API Key	Pre-populated with the Workspace ONE UEM 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.

5 Click **Save**.

Important When the Workspace ONE UEM service details applicable to this authentication method change, make sure that you update the Workspace ONE UEM configuration in the Workspace ONE Access console. Otherwise this authentication method might fail.

What to do Next

Associate the Device Compliance authentication method in the built-in identity provider and configure the default access policy to create rules to use device compliance with Workspace ONE UEM.

Configure Compliance Checking Rules in Workspace ONE Access

You can create an access policy rule that requires authentication and device compliance verification for devices managed by Workspace ONE UEM.

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

Prerequisites

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

Compliance checking enabled in the Workspace ONE Access Workspace ONE UEM page.

Procedure

1 In the Workspace ONE Access console **Resources > Policies** page, click **EDIT DEFAULT POLICY**.

2 Click **NEXT**.

3 Click **ADD POLICY RULE** to add a rule, or select a rule to edit.

Option	Description
If a user's network range is	Verify that the network range is correct. If adding a rule, select the network range.
and user accessing content from	Select the mobile device type.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy applies to all users.
Then perform this action	Select **Authenticate using...**.
then the user may authenticate using	Select the mobile device authentication method to apply. And then click + and in the drop-down menu select **Device Compliance (with Workspace ONE UEM)**.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

4 Click **Save**.

Configuring Access Policies in Workspace ONE Access to Manager User Access to Their Apps in Hub Catalog

To provide secure access to the users' Hub portal and to launch web and desktop applications, you configure access policies.

After you enable and configure the authentication methods in the built-in identity provider, create policy rules in the default access policy to manage access from mobile devices.

Policy rules map the requesting IP address to network ranges and designate the type of devices that users can use to sign in. The rule defines the authentication methods and the number of hours the authentication is valid.

When users attempt to sign in, the Workspace ONE Access service evaluates the default access policy rules to select which rule in the policy to apply. The authentication methods are applied in the order they are listed in the rule. The first identity provider instance that meets the authentication method and network range requirements of the rule is selected. The user authentication request is forwarded to the identity provider instance for authentication. If authentication fails, the next authentication method configured in the rule is applied.

You can create policies and assign them to applications that require restricted access. The access policy set can be configured to check the Workspace ONE UEM server for device compliance status when users sign in from a device. The compliance check ensures that users are blocked from signing in to an application or using single sign-in to their user portal if the device goes out-of-compliance. When the device is compliant again, the ability to sign in is restored.

Add Authentication Rules Workspace ONE Access Default Access Policy

To achieve the single sign-on experience when users access apps from the Workspace ONE Intelligent Hub app or from their Hub portal in the browser, the default access policy is configured with rules for each type of device that is used in your environment, Android, iOS, and macOS, and set the order in which the authentication methods are used for authentication.

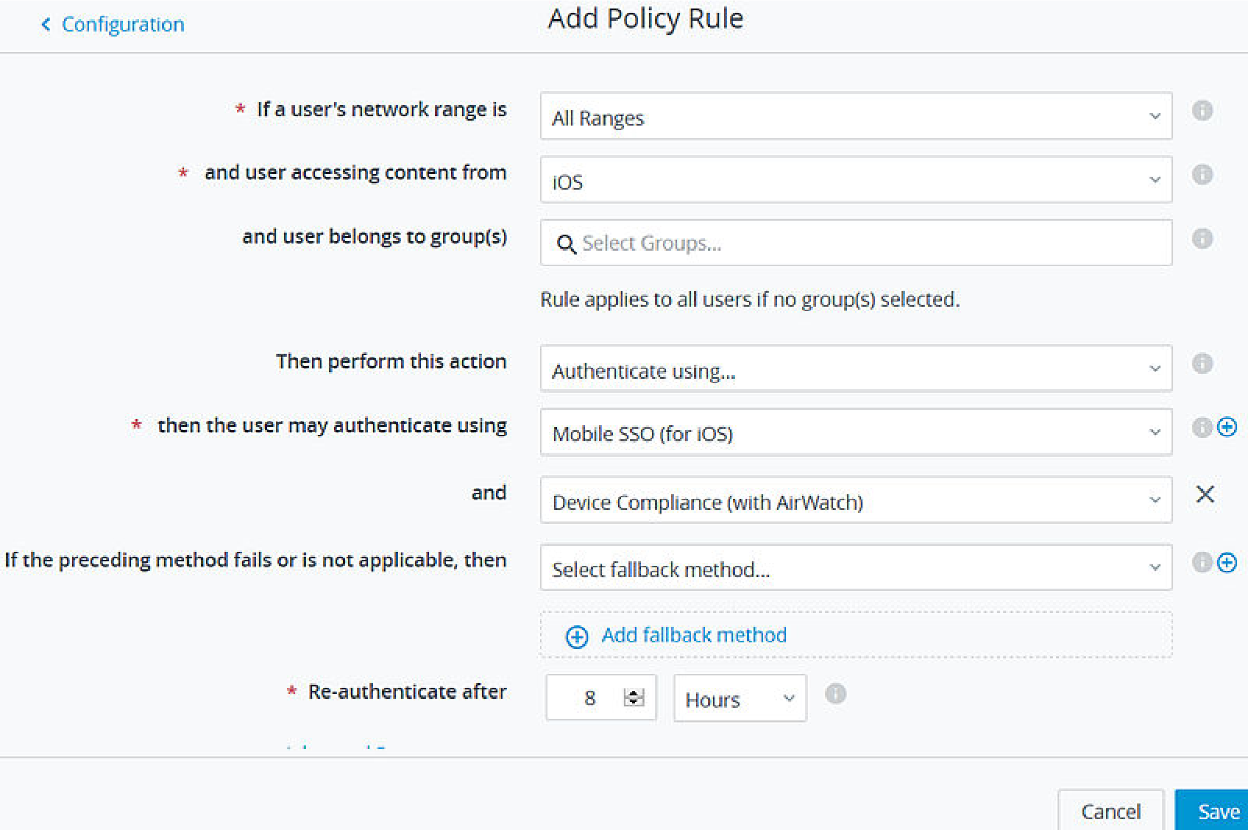
Prerequisites

- The authentication methods that your organization supports configured and enabled.
- Network ranges of defined IP addresses created and assigned to the identity providers.

You chain Device Compliance to the device authentication method to measure the health of the managed device, resulting in pass or fail based on Workspace ONE UEM defined criteria.

Create a rule for **each device type** that can be used to access the Workspace ONE Intelligent Hub app.

This example is for the rule to allow access from the device type **iOS** and with device compliance.



< Configuration

Add Policy Rule

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

Create policy rules that apply to all authentication method in every directory that is configured. If a directory uses an authentication method that is not configured in a policy rule, users in that directory cannot log in.

Procedure

1 In the Workspace ONE Access console **Resources > Policies** page, click **Edit Default Policy**.

2 You can change the policy name to be more specific. For example, Company Basic Access Policy.

The policy applies to all apps that are in the catalog, unless the app is assigned to a web-specific access policy.

3 Click **Next** to open the Configuration page.

4 Select the rule name to edit, or to add a policy rule, click **Add Policy Rule**.

Option	Description
If a user's network range is	Verify that the network range is correct, If adding a rule, select the network range.
and user accessing content from	Select the device type that this rule manages. When the Workspace ONE Intelligent Hub app is used to access Workspace ONE and resources, create the first rule with **Apps on Workspace ONE Intelligent Hub** configured as the device type.

Option	Description
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy rule applies to all users.
Then perform this action	Select **Authenticate using...**.
then the user may authenticate using	Configure the authentication method order. Select the authentication method to apply first. To require users to authenticate through two authentication methods, click + and in the drop-down menu select a second authentication method.
If the preceding methods fails or is not applicable, then	Configure fallback authentication methods as Password. This configuration provides the best experience to manage deices, while still providing a manual sign-in option for unmanaged devices.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

5 (Optional) In **Advanced Properties**, create a custom access denied error message that displays when user authentication fails. You can use up to 4000 characters, which are about 650 words. If you want to send users to another page, in the Custom Error Link URL text box, enter the URL link address. In the Custom Error Link text box, enter the text to describe the custom error link. This text is the link. If you leave this text box blank, the word Continue displays as the link.

6 Click **Next** to review the rules and then click **Save**.

What to do next

Create additional rules, if necessary.

After all the rules are created, order the rules in the list as to how they are applied.

The edited policy rules take effect immediately.

Configure a Policy in Workspace ONE Access to Restrict Access to Applications

If your organization deploys applications that contain sensitive data, you can restrict access to these applications to only MDM-managed devices. You can create application-specific policies to manage user access to specific Web and desktop applications.

Prerequisites

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

In the application-specific policy, create a rule for each device type in your deployment. Select the correct authentication method. However, because unmanaged devices cannot access the application, do not define a fallback authentication method.

If you plan to edit the default policy to control user access to the service as a whole, configure it before this policy before creating an application-specific policy.

Add web and desktop applications to the catalog. At least one application must be listed in the Catalog page before you can add an application-specific policy.

Procedure

1 In the Workspace ONE Access console **Resources > Policies** page, click **Add Policy**.

2 Add a policy name and description in the respective text boxes.

3 In the **Applies To** section, type the application in the Search text box, and select the applications to associate with this policy.

4 Click **Next**.

5 Click **Add Policy Rule** to add a rule.

Option	Description
If a user's network range is	Verify that the network range is correct. If adding a rule, select the network range.
and user accessing content from	Select the device type that this rule manages.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy rule applies to all users.
Then perform this action	Select **Authenticate using...**.
then the user may authenticate using	Configure the authentication method order. Select the authentication method to apply first. To require users to authenticate through two authentication methods, click + and in the drop-down menu select a second authentication method, such as **Device Compliance**.
If the preceding method fails or is not applicable, then	Do not configure a fallback method.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

6 Configure additional rules for other devices.

7 Click **Save**.

Implementing Mobile Single Sign-On Authentication for Workspace ONE UEM-Managed iOS Devices

3

The Mobile SSO for iOS authentication method is used for single sign-on authentication in Workspace ONE UEM-managed iOS devices. For iOS device authentication, Workspace ONE Access uses an identity provider that is built into the service to provide access to mobile SSO authentication. Mobile SSO (for iOS) authentication uses a Key Distribution Center (KDC) that is part of the Workspace ONE Access service.

For iOS Mobile SSO authentication, Workspace ONE Access makes use of a certificate that is deployed in a device profile to authenticate the user with Workspace ONE UEM. The iOS Mobile SSO certificate authentication relies on Kerberos to collect the certificate.

You configure the following for Mobile SSO for iOS authentication.

- Download the issuer certificate to configure Mobile SSO for iOS.
  - If you are using Workspace ONE UEM Certificate Authority, in the Workspace ONE UEM console, enable Certificates in the Enterprise Integrations > Workspace ONE Access page. 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 Workspace ONE UEM to use Active Directory Certificate Authority. Add the Certificate template in the Workspace ONE UEM console. Download the issuer certificate to configure Mobile SSO for iOS.
- Establish the Key Distribution Center (KDC) to use.
- Configure the Mobile SSO (iOS) authentication method in the Workspace ONE Access console.
- Configure the built-in identity provider and associate the Mobile SSO for iOS authentication method in the Workspace ONE Access console.
- Download the KDC certificate from the Workspace ONE Access console. You upload the certificate to the Apple iOS single sign-on device profile in Workspace ONE UEM.
- Configure the Apple iOS single sign-on device profile and enable single sign-in from the Workspace ONE UEM console.

In addition to configuring mobile SSO for iOS, you configure mobile device management for iOS devices in the Workspace ONE UEM console. See iOS Device Management documentation.

Supported Apple iOS Devices

iOS 9 or late is supported.

Read the following topics next:

- Using a Key Distribution Center for Authentication from iOS Devices When Authenticating with Workspace ONE Access
- Configuring Mobile SSO for iOS Authentication
- Configure Apple iOS Profile in Workspace ONE UEM Using Workspace ONE UEM Certificate Authority
- Configure Apple iOS Single Sign-On Profile in Workspace ONE UEM Using Active Directory Certificate Authority and Certificate Template
- Create Custom Lookup Value for iOS Mobile SSO Kerberos Principal Name
- Assign a Workspace ONE UEM Device Profile to Smart Groups

Using a Key Distribution Center for Authentication from iOS Devices When Authenticating with Workspace ONE Access

For iOS device authentication, 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. The iOS device authentication method uses a Key Distribution Center (KDC) without the use of a connector or a third-party system.

Workspace ONE Access Cloud tenants do not need to manage or configure the KDC.

For on premises deployments, use the Built-in KDC. The built-in KDC requires initializing KDC on the appliance and creating public DNS entries to allow the Kerberos clients to find the KDC. For more information about enabling the built-in KDC, see the Using the Built-in KDC for Workspace ONE Access article in the latest Workspace ONE Access on premise installation guide.

Using Workspace ONE UEM Certificate Authority for Kerberos Authentication

You can use the Workspace ONE UEM Certificate Authority instead of the Active Directory Certificate Authority to set up single sign-on with built-in Kerberos authentication to Workspace ONE UEM managed iOS 9 or later mobile devices. You can enable Workspace ONE UEM Certificate Authority in the Workspace ONE UEM console and export the CA issuer certificate for use in the Workspace ONE Access service.

The Workspace ONE UEM Certificate Authority is designed to follow Simple Certificate Enrollment Protocol (SCEP) and is used with Workspace ONE UEM managed devices that support SCEP. Workspace ONE Access integration with Workspace ONE UEM uses the Workspace ONE UEM Certificate Authority to issue certificates to iOS 9 or later mobile devices as part of the profile.

The Workspace ONE UEM Certificate Authority issuer root certificate is also the OCSP signing certificate.

Enable and Export the Workspace ONE UEM Certificate Authority

When Workspace ONE Access is enabled in Workspace ONE UEM, you can generate the Workspace ONE UEM issuer root certificate and export the certificate for use with the Mobile SSO for iOS authentication on managed iOS 9 or later mobile devices.

Procedure

1 In the Workspace ONE UEM console, navigate to **System > Enterprise Integration** > **Workspace ONE Access**.

  To enable Workspace ONE UEM 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**.

2 Click **Configuration**.

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 Workspace ONE Access console, configure Kerberos Authentication in the built-in identity provider and add the certificate authority issuer certificate.

Configure Active Directory Certificate Authority in Workspace ONE UEM

When you use Active Directory when you set up single sign-on authentication for Workspace ONE UEM managed iOS mobile devices, you set up a trust relationship between Active Directory and Workspace ONE UEM. After that, you enable the Mobile SSO for iOS authentication method in Workspace ONE Access.

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

Procedure

1 In the Workspace ONE UEM 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 host name 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 Workspace ONE UEM to request and issue certificates.

4 Click **Save**.

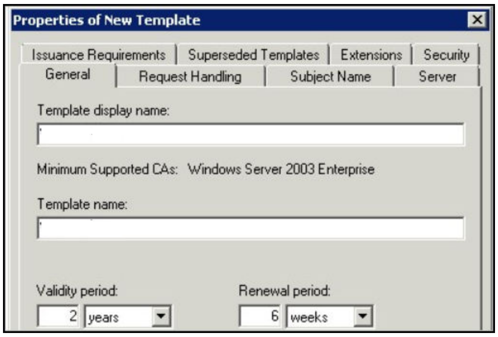
What to do next

Configure the Certificate Template in Workspace ONE UEM.

Configuring Workspace ONE UEM to Use Active Directory Certificate Authority

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

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



Template display name:

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name:

Validity period: 2 years

Renewal period: 6 weeks

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

- **General** tab. Enter the **Template display name** and the **Template name**. For example, `iOSKerberos`. This name is the display name that is shown in the Certificate Templates snap-in, Certificates snap-in, and Certification Authority snap-in.
- **Request Handling** tab. Enable **Allow private key to be exported**.
- **Subject Name** tab. Select **Supply in the request** radio button. Workspace ONE UEM supplies the subject name when the certificate is requested.
- **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 Workspace ONE UEM 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 Workspace ONE UEM configure the Certificate Authority and add the Certificate Template.

Add Certificate Template in Workspace ONE UEM

After you configure the certificate authority and certificate template for kerberos certificate distribution in the Active Directory CDertificate Services, you enable Workspace ONE UEM to request the certificate used for authentication and add the certificate authority to the Workspace ONE UEM console. You add the certificate template that associates the certificate authority used to generate the user's certificate.

Prerequisites

Configure the Certificate Authority in Workspace ONE UEM.

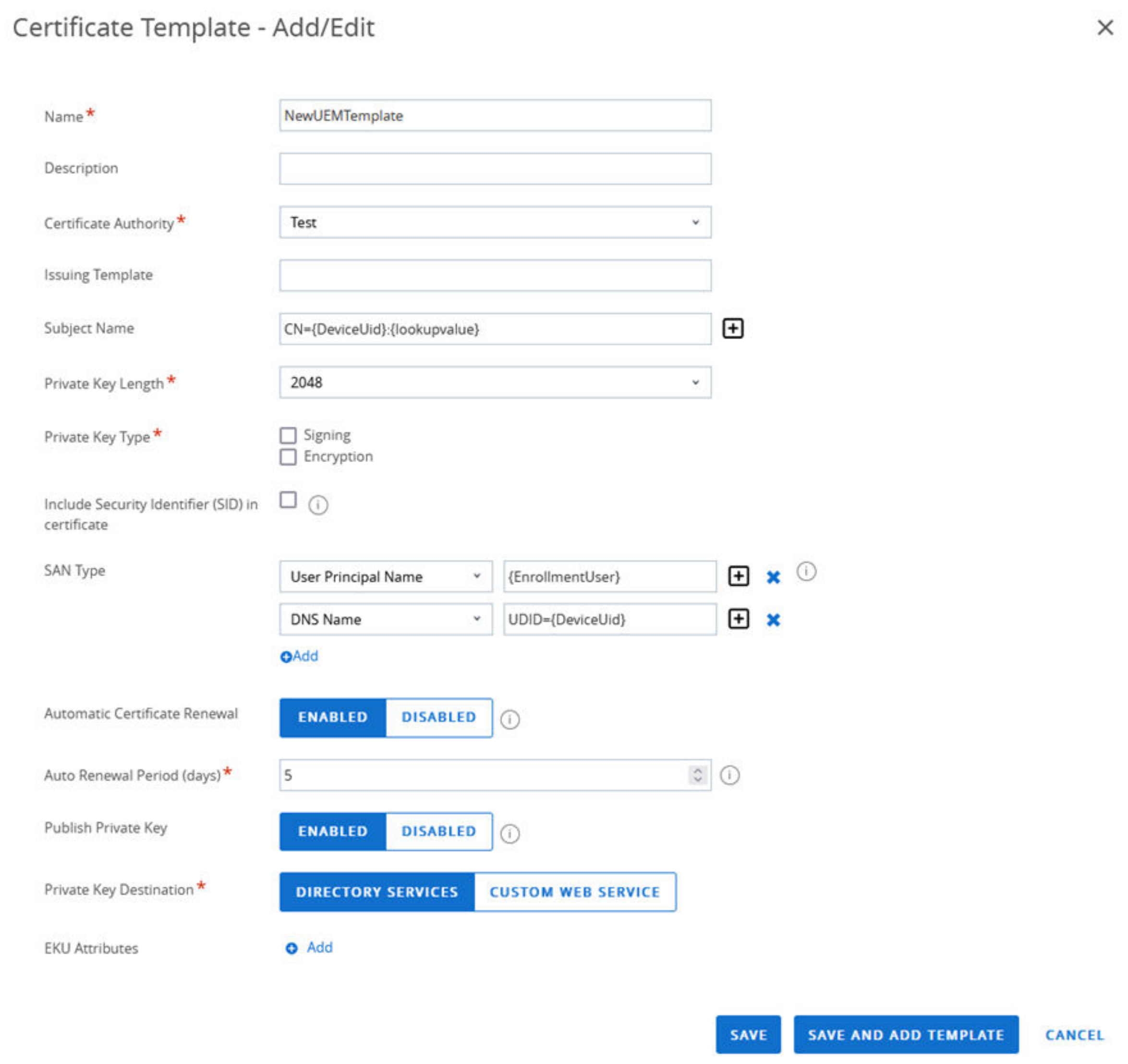
Procedure

1. In the Workspace ONE UEM 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 Workspace ONE UEM.
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	Enter the Subject name for the template. You can click **+** to select a lookup value from the list. Make sure that the value is entered after **CN=** in the text box. If you select the lookup type DeviceUid, enter a colon (:) after the value and select the lookup value from the list. For example, **CN={DeviceUid}:{lookupvalue}**, where the {} text box is the Workspace ONE UEM lookup value. Make sure to include the colon (:). The text entered in this text box is the Subject of the certificate, which can be used to determine who or what device 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 boxes for **Signing** and **Encryption**.
SAN Type	Click **+Add**. For the Subject Alternate Name, select **User Principal Name**. The value must be `{EnrollmentUser}`. When device compliance check is configured with Kerberos authentication, if you did not configure the DeviceUid as the Subject Name lookup value, add a second SAN type to include the device unique identifier (UDID). Select the SAN type **DNS Name**. The value must be **UDID={DeviceUid}**.
Automatic Certificate Renewal	Select the **Automatic Certificate Renewal** check box to renew certificates that use this template automatically prior to their expiration date.
Auto Renewal Period (days)	If you selected Automatic Certificate Renewal, enter the number of days before expiration that automatically reissues a certificate to the device.
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**.



Certificate Template - Add/Edit ×

Name*	NewUEMTemplate
Description	
Certificate Authority*	Test
Issuing Template	
Subject Name	CN={DeviceUid}:{lookupvalue}
Private Key Length*	2048
Private Key Type*	□ Signing □ Encryption
Include Security Identifier (SID) in certificate	□ ⓘ

SAN Type	User Principal Name – {EnrollmentUser}
	DNS Name – UDID={DeviceUid}
	Add

Automatic Certificate Renewal	ENABLED DISABLED ⓘ
Auto Renewal Period (days)*	5 ⓘ
Publish Private Key	ENABLED DISABLED ⓘ
Private Key Destination*	DIRECTORY SERVICES CUSTOM WEB SERVICE
EKU Attributes	Add

What to do next

In the Workspace ONE Access console, configure the built-in identity provider with the Mobile SSO for iOS authentication method.

Configuring Mobile SSO for iOS Authentication

You can use one of multiple methods to configure mobile SSO for iOS authentication, depending on your deployment and your preferred method for the deployment to perform iOS single sign-on. After you configure a Mobile SSO for iOS authentication method, you must use VMware Workspace ONE Access to create a conditional access policy with a Mobile SSO for iOS rule.

Configure Mobile SSO for iOS Authentication in Workspace ONE Access

You configure the Mobile SSO for iOS authentication method from the Authentication Methods page in the Workspace ONE Access console. Select the Mobile SSO (for iOS) authentication method in the built-in identity provider.

Prerequisites

- Certificate authority PEM or DER file used to issue certificates to users in the Workspace ONE UEM tenant.
- For revocation checking, the OCSP responder's signing certificate.
- For KDC service for Workspace ONE Access on premises, the built-in KDC service must be initialized. See Using the Built-in KDC for Workspace ONE Access.in the Workspace ONE Access installation guide.

Procedure

1 In the Workspace ONE Access console **Integrations > Authentication Methods** page, select **Mobile SSO (for iOS)**.

2 Click **CONFIGURE** and configure the Mobile SSO (iOS) authentication settings.

Option	Description
Enable KDC Authentication	To enable users to sign in using iOS devices that support Kerberos authentication, select this check box.
Realm	For tenant deployments in the cloud , the realm value is read-only. The realm name displayed is the identity manager realm name for your tenant. If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays.
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 certificates that are included are added to the list.
Enable OCSP	To use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate, select the check box.
Send OCSP Nonce	If you want the unique identifier of the OCSP request to be sent in the response, select this check box.
OCSP Responder's Signing Certificate	Upload the OCSP certificate for the responder. When you are using the Workspace ONE UEM Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the Workspace ONE UEM certificate here as well.
OCSP Responder's Signing Certificate Subject DN	The uploaded OCSP certificate file is listed here.
Cancel Message	Create a custom sign-in message that displays when authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials`.

Option	Description
Enable Cancel Link	When authentication is taking too long, give users the ability to click **Cancel** to stop the authentication attempt and cancel the sign-in. When the Cancel link is enabled, the word Cancel appears at the end of the authentication error message that displays.
Enterprise Device Management Server URL	Enter the Mobile Device Management (MDM) server URL to redirect users when access is denied because the device is not enrolled into Workspace ONE UEM for MDM management. This URL displays in the authentication failure error message. If you do not enter a URL here, the generic Access Denied message displays.

3 Click **SAVE**.

What to do next

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

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

Configure Built-in Identity Provider for Mobile SSO iOS Authentication

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

Prerequisites

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

Procedure

1 In the Workspace ONE Access, **Integrations > Identity Providers**, click **Add** and select **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 Method	The authentication methods that are configured on the service are displayed. Select the check box for the iOS authentication method to associate to this built-in identity provider. Add any other authentication methods. For Device Compliance (with Workspace ONE UEM) and Password (Workspace ONE UEM Connector), make sure that the option is enabled in the Workspace ONE UEM configuration page.

2 In the KDC Certificate Export section, click **Download Certificate**. Save this certificate to a file that can be access from the Workspace ONE UEM console.

   You upload this certificate when you configure the iOS device profile in Workspace ONE UEM.

3 Click **SAVE**.

What to do next

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

Create a Conditional Access Policy Rule

You must edit the Workspace ONE Access default access policy to add the iOS Mobile SSO authentication method that you configured to the rules.

When users attempt to sign in from their iOS devices, Workspace ONE Access service evaluates the default access policy rules to select the rule that applies to iOS Mobile SSO authentication. The authentication policy you create determines which authentication method Workspace ONE Access implements, based on the network range, device type, and user group.

Procedure

1 In the Workspace ONE Access console **Resources > Policies** page, click **Edit Default Policy** and then click **Next**.

2 Add a new policy rule, click **Add Policy Rule**.

Option	Description
If a user's network range is	Select the network range for this policy rule.
and user accessing content from	Select **iOS**.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If you do not select a group, the access policy applies to all users.
Then perform this action	Select **Authenticate using...**.
then the user may authenticate using	Select **Mobile SSO (for iOS)**.
If the preceding methods fails or is not applicable, then	Configure additional fallback authentication methods. You can add Device Compliance to check the Workspace ONE UEM server for device compliance status when users sign in from their devices. See Configure Compliance Checking Rules in Workspace ONE Access.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

3 (Optional) In Advanced Properties, create a custom access denied error message that displays when user authentication fails. You can use up to 4000 characters, which are about 650 words. If you want to send users to another page, in the **Custom Error Link URL** text box, enter the URL link address. In the **Custom Error Link text** text box, enter the text to describe the custom error link. This text is the link. If you leave this text box blank, the word `Continue` displays as the link.

4 Click **Save**.

5 Drag and drop this rule before the Web Browser rule in the list of default access policy rules.

6 Click **Next** to review the rules and then click **Save**.

What to do next

Go to the Workspace ONE UEM console and configure the iOS device profile and add the KDC server issuer certificate from Workspace ONE Access. See Configure Apple iOS Profile in Workspace ONE UEM Using Workspace ONE UEM Certificate Authority.

Configure Apple iOS Profile in Workspace ONE UEM Using Workspace ONE UEM Certificate Authority

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

Prerequisites

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

Procedure

1 In the Workspace ONE UEM 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}**.
Realm	For tenant deployments in the cloud, enter the VMware Identity Manager realm name for your tenant. The text in this parameter must be capitalized. For example, **`VMWAREIDENTITY.COM`**. For on premises deployments, enter the realm name you used when you initialized KDC in the VMware Identity Manager machine. 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. For tenant deployments in the cloud, enter the VMware Workspace ONE Access server URL as **`https://<tenant>.vmwareidentity.<region>`**. For on premises deployments, enter the VMware Workspace ONE Access server URL as **`https://myco.example.com`**.
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`**. To add additional applications, continue to enter bundle IDs or select bundle IDs from the drop-down menu. A bundle ID appears in the drop-down menu after an application is uploaded to the UEM console. For example: com.air-watch.secure.browser. The applications listed must support SAML authentication.

10 Click **Save & Publish**.

Results

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

What to do next

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

Configure Apple iOS Single Sign-On Profile in Workspace ONE UEM Using Active Directory Certificate Authority and Certificate Template

To allow iOS devices to connect to the Workspace ONE Access Identity Provider, first configure the single sign-on profile for iOS devices then assign the profile to a smart group. This profile contains the information necessary for the device to connect to the identity provider and the certificate that the device used to authenticate.

Prerequisites

- Mobile SSO for iOS is configured in Workspace ONE Access.
- Mobile iOS authentication configured in the Workspace ONE Access default access policy.
- iOS Kerberos certificate authority file saved to a computer that can be accessed from the Workspace ONE UEM admin console.
- Your Certificate Authority and Certificate Template is properly configured in Workspace ONE UEM.
- List of URLs and application bundle IDs that use Mobile SSO for iOS authentication on iOS devices.

Procedure

1 In the Workspace ONE UEM 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 Workspace ONE UEM.

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 **Integrations > Identity Providers > Built-in IDP** 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}**. If your Active Directory includes employee user names that are configured with the same value for FirstName and LastName, create a custom attribute in the Workspace ONE UEM console Lookup Fields page. See Create Custom Lookup Value for iOS Mobile SSO Kerberos Principal Name.
Realm	For tenant deployments in the cloud, enter the Workspace ONE Access realm name for your tenant. Make sure that you enter the realm name in the same case as the realm name for your tenant. **Note** Kerberos realm names are case sensitive. The recommend format is to create realm names in all upper case. Realm names that differ in the case are not equivalent. For example, `WORKSPACEONEACCESS.COM` is not the same realm name as `workspaceoneaccess.com`. For on premises deployments, enter the realm name you used when you initialized KDC in the Workspace ONE Access 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.

Option	Description
URL Prefixes	Enter the URL prefixes that must match to use this account for Kerberos authentication over HTTP. For tenant deployments in the cloud, enter the Workspace ONE Access server URL as `https://<tenant>.workspaceoneaccess.<region>`. For on premises deployments, enter the Workspace ONE Access server URL as `https://myco.example.com`.
Application Bundle ID	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**.

What to do next

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

Create Custom Lookup Value for iOS Mobile SSO Kerberos Principal Name

If your Active Directory includes multiple employee user names configured with the same FirstName and LastName, you must create a custom attribute in the **Devices & Users > General > Lookup Fields** page in the Workspace ONE UEM console to use as the Kerberos Principal Name in the iOS SSO profile configured in the Workspace ONE UEM console.

Prerequisites

To learn more about lookup fields in the Workspace ONE UEM console, see Devices & Users / General / Lookup Fields.

Procedure

1 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings**.

2 In the **Devices & Users** section, select **General** and then click **Lookup Fields**.

3 Click **ADD CUSTOM FIELD** and configure the following.

Option	Description
Option	**Description**
Standard Lookup Field	In the drop-down menu, select **User Principal Name**.
Name	Enter a name for the custom look up field. For example, **`KerberosSPN`**
Description	Enter the description of this custom field, for example, **`Custom Kerberos User Principal Name lookup`**

Option	Description
Allow Inheritance	Select **Enable**.
Custom type	Select **Regex Lookup**.
Regular Expression	Enter `^[^@]+`.

4. Click **SAVE**.

   The custom lookup name is listed in the Lookup table page.

5. To add the custom lookup name to the iOS profile, in the Workspace ONE UEM console, navigate to the iOS Resources >Profiles page and select the iOS device profile to edit. In the Single Sign-On page **Kerberos Principal Name** text box, enter the custom lookup name that you created.

6. Select **SAVE & PUBLISH**.

   See the Workspace ONE UEM documentation, Configure an iOS Profile > Single Sign-On Profile for iOS.

Assign a Workspace ONE UEM Device Profile to Smart Groups

After you create a device profile in Workspace ONE UEM, you assign the profile to a smart group.

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

Procedure

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

Results

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

Accessing Other Documents

4

As you configure Workspace ONE integration, you might need to access additional documentation from these documentation centers.

- VMware Workspace ONE Document Center
  - Hub Services documentation
  - Workspace ONE Integrations
  - Workspace ONE Intelligence
- VMware Workspace ONE UEM Document Center
  - AirWatch Cloud Connector
  - VMware Workspace ONE UEM Mobile Device Management documentation
  - VMware Workspace ONE UEM Mobile Application Management documentation
  - iOS Device Management documentation
  - Android Platform documentation
- VMware Workspace ONE Access Documentation Center
  - Workspace ONE Access Administration Guide
  - Managing User Authentication Methods in VMware Workspace ONE Access
  - Setting Up Resources in Workspace ONE Access
  - Integrations - Workspace ONE UEM, Okta, Android Mobile Single Sign-on
  - Configuring AirWatch Provisioning app in Workspace ONE Access