(Legacy) VMware Workspace ONE Access Administration Guide

Legacy Admin Console-Based Documentation (prior to April 2022)

FEB 2022

VMware Workspace ONE Access

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

https://docs.vmware.com/

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

Contents

Working in VMware Workspace ONE Access Console

1

The VMware Workspace ONE® Access ™ console provides you with a centralized management console with which you can manage users and groups, set up and manage authentication and access policies, and add resources to the catalog and manage entitlements to those resources. You can also configure Workspace ONE UEM integration. Note that Workspace ONE Access was formerly known as VMware Identity Manager.

The key tasks you perform from the Workspace ONE Access console is manage user authentication and access policies and entitle users to resources. Other tasks support this key task by providing you with more detailed control over which users or groups are entitled to which resources under which conditions.

When Workspace ONE Hub Services is integrated with Workspace ONE Access, end users can access their work resources from their user web portal in a browser or from the Workspace ONE Intelligent Hub App on their devices. You can access the Hub Services console from the Workspace ONE Access console to set up how employees use Workspace ONE Intelligent Hub to access apps, receive notifications, and search for people.

Note For documentation about configuring and managing user authentication and access policies, see the *Managing Workspace ONE Access User Authentication Methods* guide.

This chapter includes the following topics:

Navigating in the Workspace ONE Access Console

The tasks in the Workspace ONE Access console are organized by tabs.

If you have administrator privileges, you can log in to the Workspace ONE Access console from your user portal page. To open the console pages, click your profile on the right and select Administration Console.

To access the Workspace ONE Access console directly, enter the Workspace ONE Access URL as `https://<exampleFQDN.com>/SAAS/admin`. When the login page displays, select the domain, if requested and log in with your Active Directory user name and password, or select System Domain and log in as the Workspace Access admin.

Tab	Description
Dashboard	The User Engagement dashboard can be used to monitor user activity and resources used. This dashboard displays information about who signed in, which applications are being used, and how often they are being used. For on premises deployment, a System Diagnostics dashboard displays a detailed overview of the health of the service in your environment and other information about the services. You can also manage the configuration of the appliance, including configuring SSL certificates for the appliance, change the services admin and system passwords. You can create reports to track users' and groups' activities, resource and device use, and audit events by user.
Users and Groups	In the Users and Groups tab, you manage and monitor users and groups imported from your Active Directory or LDAP directory, create local users and groups, and entitle the users and groups to resources. The password restriction policy for local users is managed in the User and Groups Settings page.
Catalog	The Catalog is the repository for all the resources that you can entitle to users. In the Catalog tab, you add Web applications and manage existing resources. In the Virtual Apps Collection page, you manage Horizon, Citrix, Horizon Cloud, and ThinApp desktops and application integrations. You group applications into categories and can access information about each resource. On the Catalog Settings page, you download SAML certificates and manage resource configurations. From the Catalog > Hub Configuration page, you access the Hub Service console. From the Hub Services console, you can design and set up how users use Workspace ONE Intelligent Hub to access the catalog, receive notifications, search for people they work with, and use support services.
Identity & Access Management	The Identity and Access Management tab is where you set up and manage the directory service, authentication methods, access policies, and preferences. You can configure Okta and Workspace ONE UEM settings to integrate with Workspace ONE Access.
Roles	In the Roles tab, you manage administrator roles. Users can be assigned as admins to the three pre-defined administrator roles and you can create custom administrator roles that give limited permissions to specific services in the Workspace ONE Access console.
Appliance Settings	For the on premises deployments, the Appliance Settings tab is displayed. You manage the license settings and configure SMTP settings.

Supported Web Browsers to Access the Workspace ONE Access Console

The Workspace ONE Access console is a web-based application you use to manage the Workspace ONE Access service. You can access the Workspace ONE Access console from the latest versions of Mozilla Firefox, Google Chrome, Safari, and Microsoft Edge.

Workspace ONE Intelligent Hub for End Users

End users can access entitled resources from the Workspace ONE Intelligent Hub app on their devices or from the Intelligent Hub portal in web browsers. The Intelligent Hub portal is the default interface used when users access and use their entitled resources with a browser.

When Workspace ONE UEM is integrated with Workspace ONE Access, end users can see all applications that they are entitled to. Native applications that are internally developed or publicly available in app stores can be made available to your end users from the Hub portal.

Workspace ONE Access Identity and Access Management Settings Overview

The Identity and Access Management tab in the Workspace ONE Access console is where you can set up and manage the authentication methods, access policies, directory service, and integrate with Workspace ONE UEM.

The following is a description of the setup settings in the Identity and Access Management tab.

Table 1-1. Identity and Access Management Set Up Settings

Setting	Description
Setup > Connectors	The Connectors page lists the connectors that are deployed inside your enterprise network. The Workspace ONE Access connector is an on-premises component of Workspace ONE Access that integrates with your on-premises infrastructure. The following enterprise services can be installed on a connector. ■ Directory Sync service that syncs users from Active Directory or LDAP directories to the Workspace ONE Access service. ■ User Auth service that provides connector-based authentication methods, including Password (cloud deployment, RSA SecurID (cloud deployment), and RADUS (cloud deployment). ■ Kerberos Auth service that provides Kerberos authentication for internal users.
Setup > Custom Branding	In the Custom Branding page, you can customize the appearance of the Workspace ONE Access console header and sign-in screen. **Note** You customize the look and add a logo that displays in the Workspace ONE Intelligent Hub app or Hub portal view from the Hub Services console, Branding page.
Setup > User Attributes	The User Attributes page lists the default user attributes that sync in the directory. You can add other attributes that you can map to Active Directory attributes. See the *Directory Integration with VMware Workspace ONE Access* guide.
Setup > Auto Discovery	For on-premises deployment, when Workspace ONE Access and Workspace ONE UEM are integrated, you can integrate the Windows Autodiscovery service that you deployed in your Workspace ONE UEM configuration with the Workspace ONE Access service. For more details about setting up auto discovery in Workspace ONE UEM in on-premises deployments, see the Workspace ONE UEM documentation Auto discovery Service Installation Guide. For cloud deployments, you can register your email domain to use the auto-discovery service to make it easier for users to access their apps portal using Workspace ONE Intelligent Hub. End users can enter their email addresses instead of the organization's URL when they access their apps portal through Workspace ONE Intelligent Hub.
Setup > Okta	On this page, you can enter your Okta tenant information to connect Workspace ONE Access to the Okta tenant and retrieve apps from Okta. See Integrating VMware Workspace ONE with Okta for configuration information.

Table 1-1. Identity and Access Management Set Up Settings (continued)

Setting	Description
Setup > VMware Workspace ONE UEM	On this page, you can set up integration with Workspace ONE UEM. You can enable the catalog settings with UEM, enable compliance check to verify that managed devices adhere to Workspace ONE UEM compliance policies, and enable user password authentication through the AirWatch Cloud Connector (ACC). See Guide to Deploying VMware Workspace ONE with Workspace ONE Access guide on the Workspace ONE Documentation page.
Setup > Preferences	The Preferences page displays features that the admin can enable. This page includes the following preferences. ■ Enable Show that the System Domain on Login Page . ■ Enable persistent cookies. The persistent cookie stores users' sign-in session details so that users do not need to reenter their user credentials when accessing their managed resources from their iOS or Android mobile devices. See the Managing User Authentication Methods guide. ■ Enable Hide Domain Drop-Down Menu, when you do not want to require users to select their domain before they log in. ■ Select the User Sign-in Unique Identifier option to display the identifier-based login page. See Chapter 5 Managing the User Login Experience in Workspace ONE Access. ■ Customize the Sign-in Input Prompt can be used to customize the prompt in the user text box on the sign-in screen. ■ Enable Sync Group Members to the Directory when Adding Groups to sync the members in the groups from Active Directory. When this is disabled, names are synced, but members of the group are not. ■ Enable User Sign-in Unique Identifier to hide the domain request page.
Setup > Terms of Use	On this page, you can set up Workspace ONE terms of use and ensure that end users accept these terms of use before using the Workspace ONE Intelligent Hub portal.

The following is a description of the settings to use to manage the services in the Identity and Access Management tab.

Table 1-2. Identity and Access Management Manage Settings

Setting	Description
Manage > Directories	The Directories page lists directories that you created. You create one or more directories and then sync those directories with your enterprise directory deployment. On this page, you can see the number of groups and users that are synced to the directory and the last sync time. You can click Sync Now, to start the directory sync. When you click a directory name, you can edit the sync settings, navigate the Identity Providers page, and view the sync log. From the directories sync settings page, you can manage the following. ■ Schedule the sync frequency. ■ View the list of domains associated with this directory. ■ Change the mapped attributes list. ■ Update the user and groups list that syncs. ■ Set the safeguard targets. See the *Directory Integration with VMware Workspace ONE Access* guide.
Manage > Identity Providers	You can configure and manage the following identity provider types on this page. ■ Workspace ONE Access identity provider for Kerberos authentication ■ Built-in identity provider for User Auth authentication methods and authentication methods managed by Workspace ONE Access ■ Third-party identity providers See the *Managing Workspace ONE Access User Authentication Methods* guide.
Manage > Password Recovery Assistant	On the Password Recovery Assistant page, you can change the default behavior when "Forgot password" is clicked in the sign-in screen by the end user.
Manage > Authentication Methods	The Authentication Methods page is used to configure cloud authentication methods associated to the Workspace ONE Access service. These authentication methods are then associated with the built-in identity providers. See Managing Authentication Methods for Identity Providers for configuration information.
Manage > Policies	The Policies page lists the default access policy and any other Web application access policies you created. You also configure the network ranges to use from this page. Policies are a set of rules that specify criteria that must be met for users to access their Workspace ONE Intelligent Hub portal or to launch Web applications that are enabled for them. You can edit the default policy. If Web applications are added to the catalog, you can add new policies to manage access to these Web applications. See Managing Access Policies for more information about access policies.
Manage > Enterprise Authentication Methods	The User Auth service and Kerberos Auth service authentication methods are configured and managed from this page. See Managing User Authentication Methods in VMware Workspace ONE Access.

Join or Leave the Customer Experience Improvement Program for Workspace ONE Access (On Premises Only)

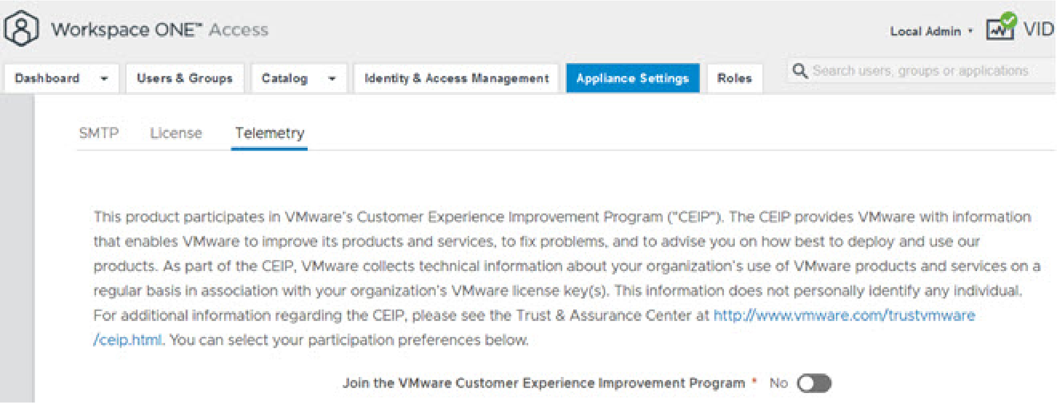
This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by

VMware are set forth at the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. To join or leave the CEIP for this product, follow this procedure.

Note If your network is configured to access the Internet through HTTP proxy, to send the data collected through CEIP to VMware you must adjust the proxy settings in VMware Workspace ONE Access. See Setting Proxy Server Settings in the *Installing and Configuring VMware Workspace ONE Access* guide.

Procedure

1 In the Workspace ONE Access console, click the **Appliance Settings** tab, then select **Telemetry**.



This product participates in VMware's Customer Experience Improvement Program ("CEIP"). The CEIP provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual. For additional information regarding the CEIP, please see the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You can select your participation preferences below.

Join the VMware Customer Experience Improvement Program * No

2 Select the **Join the VMware Customer Experience Improvement Program** check box to join the CEIP program or deselect the check box to leave the CEIP program.

3 Click **Save**.

Managing Administrator Roles in Workspace ONE Access 2

Workspace ONE Access uses role-based access control to manage administrator roles. With roles-based access control, you create functional roles that control admin access to tasks in the Workspace ONE Access console, and assign the roles to one or more users and groups.

Three predefined administrator roles are built in to the Workspace ONE Access service. You can assign these predefined roles to users and groups in your service. You cannot modify or delete these roles.

You can also create custom administrator roles that give limited permissions to specific services in the Workspace ONE Access console. Within the service, specific operations can be selected as the type of action that can be performed in the role.

This chapter includes the following topics:

About the Roles-Based Access Roles in Workspace ONE Access

The three predefined administrator roles that can be granted in the Workspace ONE Access server are super administrator, read-only administrator, and directory administrator.

- The super administrator role can access and manage all features and functions in the Workspace ONE Access services.

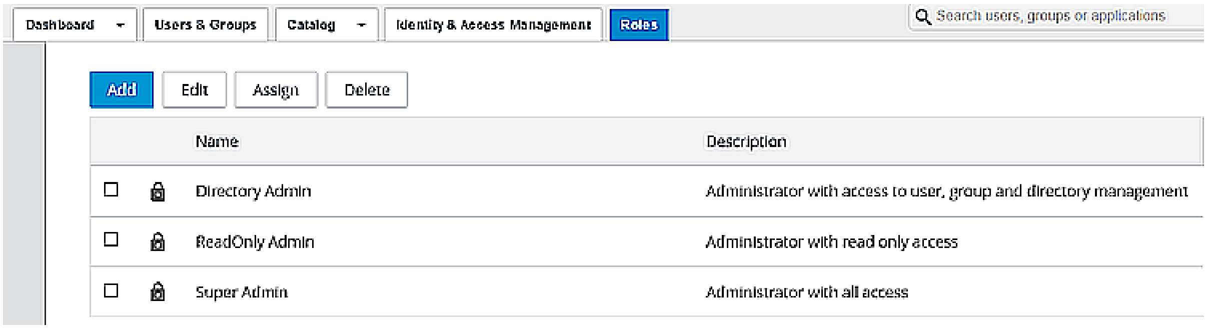
The first super administrator is the local administrator user that Workspace ONE Access creates when you first set up the service. The service creates the administrator in the System Domain of the System Directory. You can assign other users to the super administrator role in the System Directory. As a best practice, grant the super administrator role to a select few.

- The read-only administrator role can view the details in the Workspace ONE Access console pages, including the dashboard and the reports, but cannot make changes. All administrator roles are automatically assigned the read-only role.

  Note Some Workspace ONE Access console pages are not enabled to be viewed by an admin entitled to only the read-only role. When read-only admins try to view these pages, they are redirected to the dashboard.

- The directory administrator role can manage users, groups, and directories. The directory administrator can manage directory integration for both enterprise directories and local directories within your organization. The directory administrator can also manage local users and groups.

Figure 2-1. Roles Tab in Workspace ONE Access Console


Dashboard
Users & Groups
Catalog
Identity & Access Management
Roles
Search users, groups or applications
Add
Edit
Assign
Delete

	Name	Description
□	Directory Admin	Administrator with access to user, group and directory management
□	ReadOnly Admin	Administrator with read only access
□	Super Admin	Administrator with all access

You can assign these predefined roles to users and groups in your service. You cannot modify or delete these roles.

You can also create custom administrator roles that give limited permissions to specific services in the Workspace ONE Access console. Within the service, specific operations can be selected as the type of action that can be performed in the role.

Multiple roles can be assigned to the same user and groups. When a user is assigned more than one role, the behavior of the roles applied is additive. For example, if an administrator is assigned two roles, one with write access to policy management and the other without, that administrator has access to modify policies.

Role-based access control can be set up to manage the following services in the administrator console.

Service Type	Service Description
Catalog	The Catalog is the repository of all the Workspace ONE resources that can be entitled to users. The Catalog service can manage the following types of actions. ■ Web Applications ■ App sources ■ Third-party applications ■ ThinApp Virtual Apps Collection ■ Virtual Apps Collection which includes Horizon, Horizon Cloud, and Citrix-based applications. **Note** A super admin is required to initiate the getting started flow in the Virtual Apps Collection page in the Catalog. After the initial getting started flow, admin roles with the Catalog service can manage ThinApp packages and Desktop applications.
Directory Management	The Directory Management service can manage the following types of actions either for the organization or for specific directories in your organization. ■ Enterprise Directory. The admin can add, edit, and delete directories in the service. Editing a directory includes managing directory settings, including sync settings. ■ Local Directory. The admin can create, edit, and delete local directories. Editing a directory includes managing settings and creating, editing, and deleting local users and groups. When the Directory Management service is included in a role, the Identity & Access Management service must also be configured in the role.
Users and Groups	The Users and Groups service can manage the following types of action in your total organization or for specific domains in your organization. ■ Groups ■ Users ■ Password resets for local users
Entitlements	The Entitlement service can assign users to web and virtual applications. The following types of entitlement actions can be managed. For each of these actions, you can configure the role to assign users and groups to all the resources in your organization or to specific applications. You can also entitle applications to users and groups within specific domains. ■ Web entitlements ■ Third-party entitlements
Roles Administration	The Roles Administration service can manage the assignment of the admin role to users. When you create a role with the Roles Administration service, you must configure the User and Groups service and select the Manage Users and Manage Groups actions. Administrators who are assigned this role can promote users and groups to the administrator role and can remove the administrator role from users or groups.
Identity & Access Management	The Identity & Access Management service can manage the settings in the Identity & Access Management tab. To manage the directory settings, the Directory Management service is also required. **Note** Administrators with the Identity and Access Management role can integrate Workspace ONE Access with Workspace ONE UEM and create the directory from the Workspace ONE UEM console.

When you add a role, you select the service and define which actions can be performed in the service. In some of the services, you can select to manage all resources for the selected action or some resources.

Manage Read-Only Access

Read-only Access is granted with each role that is assigned to an administrator. You can also assign users and groups to the read-only role from the ReadOnly Admin roles page.

The read-only administrator role gives users admin access to view the Workspace ONE Access console, but unless an administrator is assigned another role with additional access, they can only view the content in the Workspace ONE Access console.

When you assign the read-only role as a separate role, you can remove the role from the ReadOnly Admin role Assign page or from the user or group profile page.

Add an Administrator Role in Workspace ONE Access

With role-based access control, you can create a role to manage one action or many actions.

When you create a role, you can add one or more services to the role. You name the role, select the type of services and the specific actions within the service that the role can manage.

- When you create a role with the Directory Management service, the Identity and Access Management service must also be configured in the role.
- When you create a role with the Roles Administration service, the User and Groups service must also be configured with the actions to manager users and to manage groups selected.

Prerequisites

To create a role in the Workspace ONE Access service, you must be a super admin who can access and manage all features and functions in the Workspace ONE Access services, or an admin assigned the role that is configured with the Roles Administration service.

Procedure

1. In the console **Roles** tab, click **Add**.
2. In the **Role Name** text box, enter a descriptive role name and add a description.

   Each role name in your environment must be unique.
3. Click **Next**.
4. Select the service to be managed by this role.
5. In the **Actions** drop-down menu, select the type of actions that can be managed.
6. Select **All** resources to manage all resources within the action, or select **Some** and then select the condition that can be managed from the Conditions drop-down menu.
7. To add additional actions to be managed by this role, click **+** and complete the configuration action.

8 Click **Save**.

   The Services page displays the configuration you set up.

9 If you want to add another service to this role, select the service and complete the configuration steps 5–8.

10 When finished, click **Save** on the Configuration page.

What to do next

Assign this role to users to make them administrators of this service.

Assign Users and Groups to a Workspace ONE Access Administrator Role

A Workspace ONE Access super administrator or a role that includes the role administrator service and the users and groups service can assign a role to users and groups to elevate them to administrators of that role.

Prerequisites

- Before adding an administrator role to a user who is synced from the Workspace ONE UEM directory, make sure that the user profile is configured with an **Admin User Promote** account in the Workspace ONE UEM console.

  When users with the Admin User Promote account sync to Workspace ONE Access, they are recognized as administrators and can be assigned a role in Workspace ONE Access. If an admin is not in this account in the UEM console, when the Workspace ONE UEM directory syncs with the Workspace ONE Access directory, the admin role is removed from the user profile.

Procedure

1 In the Workspace ONE Access console **Roles** tab, select the role and click **Assign**.

2 Enter a name in the search box and select the user or group.

   Only groups with fewer than 500 users in the group can be promoted to an administrator role.

3 Click **Save**.

   The users or groups become administrators for the role. The user profile page is updated to show the role.

Removing Workspace ONE Access Administrator Roles

An Administrator role in Workspace ONE Access can be revoked from the specific role’s Assign page. You can revoke all roles that are assigned to a user from the user’s profile page.

You can remove the group from the role, to revoke the role for all members of the group. You cannot remove a role from a specific member of the group. To remove only the user from the role, you remove the user from the group.

Remove Workspace ONE Access Administrator Role from Individual Users

A super administrator or a role administrator can remove an administrator user from a role in the Workspace ONE Access service.

You can begin from the user's profile page in the Users and Groups tab to revoke the role. When you begin from the profile page, you click the link to remove the role and are redirected to the Roles page.

Note Administrator roles can be revoked directly from the role's Assign page.

Procedure

1 In the Workspace ONE Access console **Users and Groups** tab, select **Users** and then the user name.

  The Profile page, Roles row lists all the roles assigned to this user.

2 In the **Roles** row, click **here**.

  You are redirected to the Roles page.

3 Select the role and click **Assign**.

4 Click **X** next to the name.

5 Click **Save**.

  The user is removed from the role and the role is removed from the user profile.

Results

Remove a Group from a Workspace ONE Access Admin Role

When you remove a group from a role, access is revoked for all members of the group. The Roles section of the user and the group profile pages is updated to remove the role.

Individual member of a group cannot be removed from a role. To remove a member of a group from a role, remove the user from the group.

If a user in the group was directly assigned to the role, when the group is removed from the role, the administrator role is maintained for the user.

Note Group administrator roles can be revoked directly from the role's Assign page.

Procedure

1 In the console **Users and Groups** tab, select **Groups** and then the group name.

The Profile page, Roles row lists all the roles assigned to this group.

2 In the **Roles** row, click **here**.

You are redirected to the Roles page.

3 Select the role and click **Assign**.

4 Click **X** next to the group name.

5 Click **Save**.

The group is removed from the role. The role is removed from the group profile and from each member profile.

Example: Example of Removing Groups from a Role

Group A, which includes User1, User2, and User3, is assigned to the Directory Admin role. The Group A, User1, User2, and User3 profiles are updated to reflect the Directory Admin role in their profile pages.

User2, also is directly assigned to the Directory Admin role.

You revoke access to Group A. Group A, User1, and User3 are removed from the role and the role is removed from these profile pages.

Because User2 was directly assigned to the Directory Admin role, User2 is still assigned to the Directory Admin role.

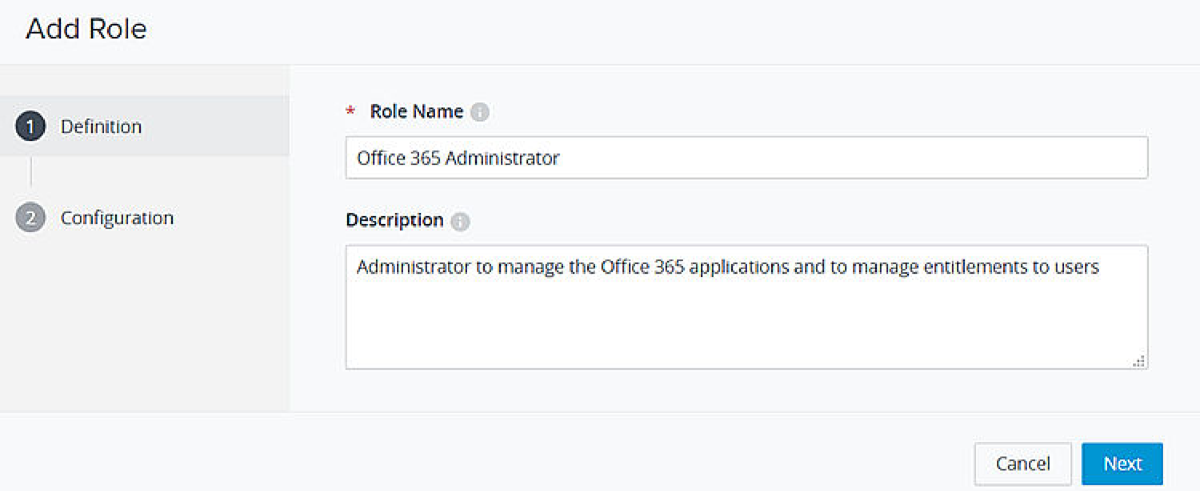
Example 1. Create an Admin Role in Workspace ONE Access to Manage Office 365 Application and Entitlements

With role-based access control in Workspace ONE Access, you can grant administrator access to users and groups, enabling them to manage specific applications.

For example, the super administrator can delegate the day-to-day duties to manage the Office 365 application in Workspace ONE to another administrator. You create an administrator role to manage Office 365 in Workspace ONE and to manage the entitlements to the application.

Procedure

1 In the console Roles page, click **Add**. Create a descriptive role name and describe the purpose of the role. Click **Next**.



Add Role

1 Definition

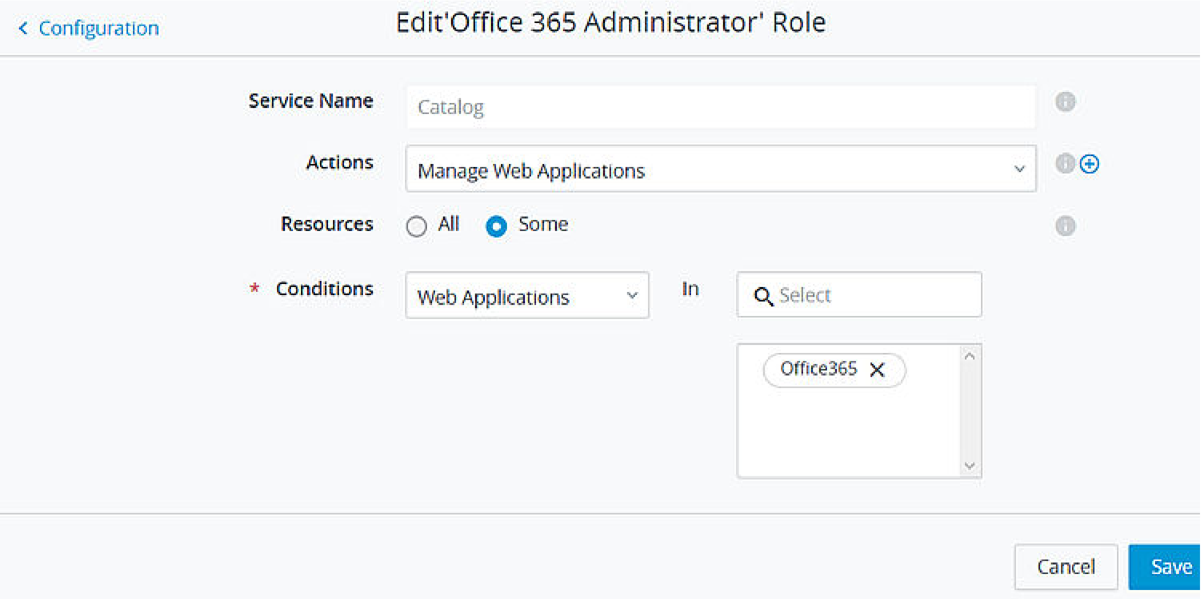
2 Configuration

* Role Name: Office 365 Administrator

Description: Administrator to manage the Office 365 applications and to manage entitlements to users

2 In the Configuration page, select the Catalog service. For **Actions**, select **Manage Web Applications**. For **Resources**, select **Some**. For **Conditions**, select **Web Applications** and enter **Office 365** in the search box. **Save** the configuration.

You can add other applications to manage. For example, search for SalesForce and add it to the list of web applications to be managed in this role.



< Configuration

Edit'Office 365 Administrator' Role

Service Name: Catalog

Actions: Manage Web Applications

Resources: ○ All ● Some

* Conditions: Web Applications In Select

Office365 ✕

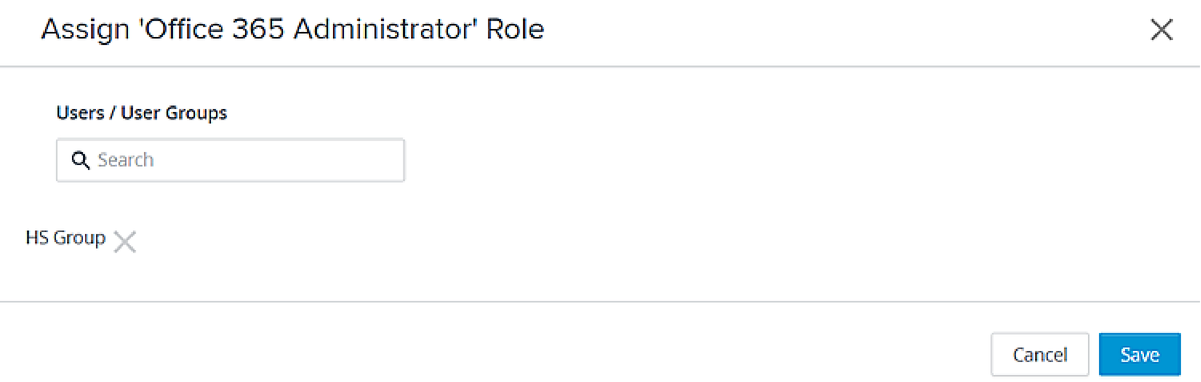
3 Again, on the Configuration page, select the **Entitlements** service. For **Actions**, select **Manage Web Entitlements**. For **Resources**, select **Some**. For **Conditions**, select **Applications** and in the search box, enter **Office 365** to select the same application. **Save** the configuration.

If you added another application in the Catalog Service, make sure that you add it here, if you want the admin to manage the entitlements.

4 On the Configuration page, click **Save** again.

The role to manage the Office 365 application is created and is listed on the Roles page.

5 Select the role you created and click **Assign**. In the **Search** text box, enter the users or group names who should be granted access. Select the user or group and click **Save**.



Assign 'Office 365 Administrator' Role

Users / User Groups

Search

HS Group

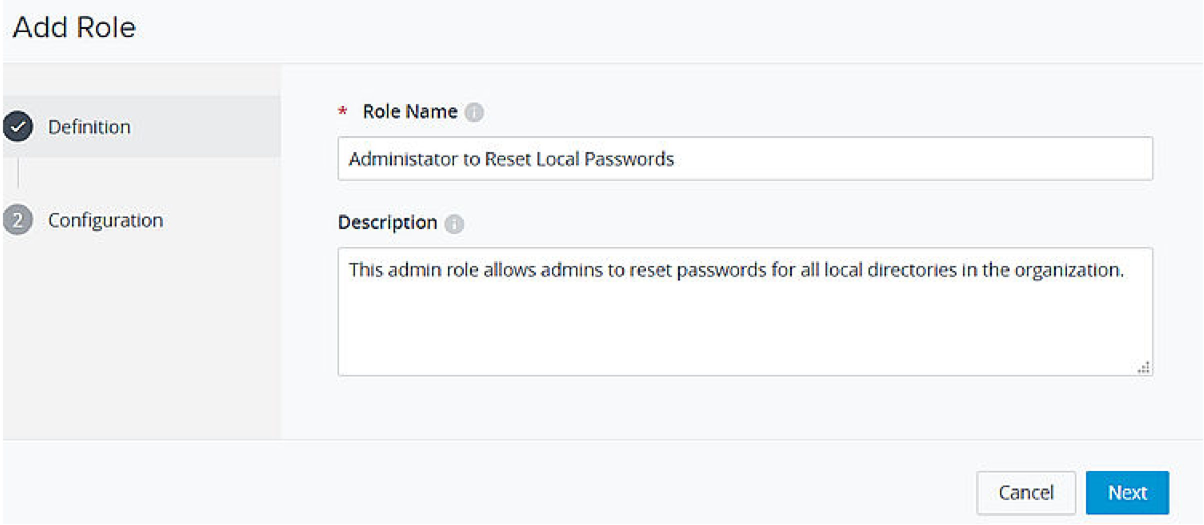
The user or group is now the administrator for this role. The profile page is updated to show the assigned administrator role.

Example 2. Create an Admin Role in Workspace ONE Access to Manage Password Reset in a Local Directory

You can create a simple administrator role in Workspace ONE Access to manage password resets for specific domains.

Procedure

1 In the Workspace ONE Access console Roles page, click **Add**, enter a descriptive role name, and describe the purpose of the role. Click **Next**.

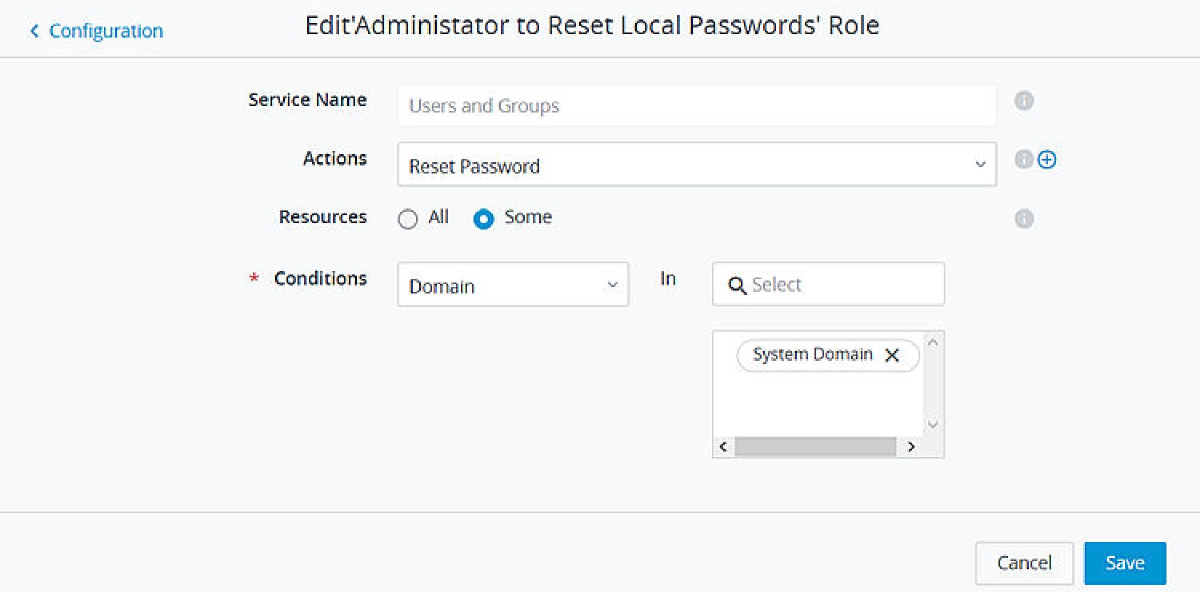


Add Role

* Role Name: Administator to Reset Local Passwords

Description: This admin role allows admins to reset passwords for all local directories in the organization.

2 In the Configuration page, select the **User and Groups** service. For **Actions**, select **Reset Password**. For Resources, select **Some**. For **Conditions**, select the local domain and enter the local directory name in the search box to select the local directory. **Save** the configuration.



< Configuration

Edit'Administator to Reset Local Passwords' Role

Service Name: Users and Groups

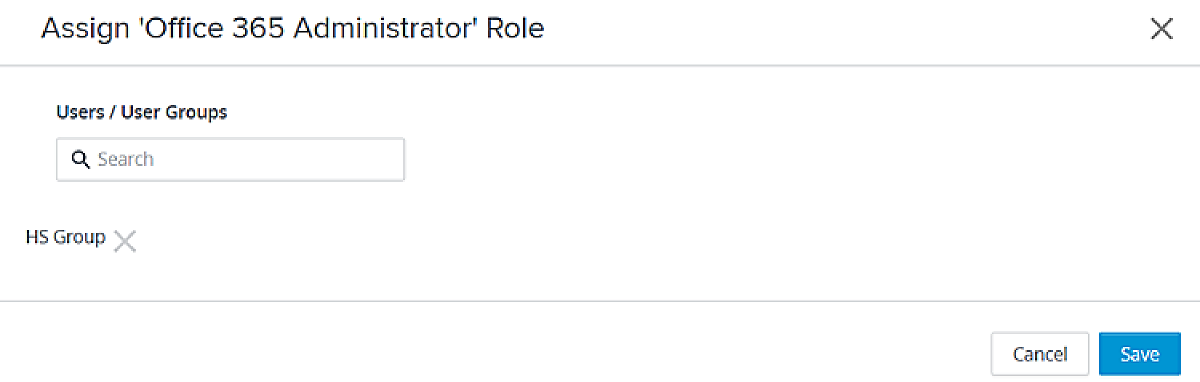
Actions: Reset Password

Resources: ○ All ● Some

* Conditions: Domain In Select

System Domain ✕

3 Select the role you created and click **Assign**. In the **Search** text box, enter the user or user group name. Select the user or group and click **Save**.



Assign 'Office 365 Administrator' Role

Users / User Groups

Search

HS Group ✕

The users or group is now the administrator for this role. The profile page is updated to show the assigned administrator role.

Using Local Directories in Workspace ONE Access

3

A local directory is one of the types of directories that you can create in the Workspace ONE Access service. A local directory enables you to provision local users in the service and provide them access to specific applications, without having to add them to your enterprise directory. A local directory is not connected to an enterprise directory and users and groups are not synced from an enterprise directory. Instead, you create local users directly in the local directory.

A default local directory, named System Directory, is available in the service. You can also create other local directories.

System Directory

The System Directory is a local directory that is automatically created in the service when it is first set up. This directory uses a domain called System Domain. You cannot change the directory or domain name of the System Directory or add new domains to it. You cannot delete the System Directory or the System Domain.

For Workspace ONE Access cloud deployments, a local administrator user is created in the System Domain of the System Directory when the tenant is first set up. The credentials you receive when you get a new tenant belong to this local administrator user.

The local administrator user that is created when you first set up the Workspace ONE Access appliance is created in the System Domain of the System Directory.

The System Directory is typically used to set up a few local administrator users to manage the service. To provision end users and additional administrators and entitle them to applications, creating a new local directory is recommended.

Local Directories

Besides the System Directory, other local directories can be created. Each local directory can have one or more domains. When you create local users, you specify the directory and domain for users.

You can select user attributes that are required for the local users. User attributes such as userName, lastName, firstName, and email are specified at the global level in the Workspace ONE Access service and are required. Global user attributes apply to all directories in the service. At the local directory level, you can select other attributes that are required for the directory. Selecting other attributes allows you create a custom set of attributes for each local directory.

Creating local directories with customized mapped attributes is useful in scenarios such as the following.

- You can create a local directory for a specific type of user that is not part of your enterprise directory. For example, you can create a local directory for partners, and provide partners access to only the specific applications they need.
- If you want different user attributes or authentication methods for different sets of users, you can create different local directories. For example, you can create a local directory for distributors that has user attributes such as region and market size, and another local directory for suppliers that has user attributes such as product category and supplier type.

Identity Provider for System Directory and Local Directories

By default, the System Directory is associated with an identity provider named System Identity Provider. The Password (Local Directory) authentication method is enabled on this identity provider. The default_access_policy_set policy rule sets up this password authentication for the ALL RANGES network range for the Web Browser device type. You can configure additional authentication methods to the policy rules.

When you create a new local directory, this local directory is not associated with an identity provider. After creating the local directory, create a new built-in identity provider of type Embedded. Associate the local directory with the identity provider and enable the Password (Local Directory) authentication method. Multiple local directories can be associated with the same identity provider.

The Workspace ONE Access connector is not required for either the System Directory or for local directories you create.

Password Management for Local Directory Users

By default, all users configured in local directories can change their password in the user portal or from the Intelligent Hub app. You can set a password policy for local users. You can also reset local user passwords as needed.

Users click their name in the top-right corner to change their passwords when they are logged into their user portal . They select **Account** from the drop-down menu and click the **Change Password** link. In the Intelligent Hub app users can change their passwords by clicking their profile and selecting **Change Password**.

For information on setting password policies and resetting local user passwords, see Managing Passwords in Workspace ONE Access.

This chapter includes the following topics:

- Creating a Local Directory in Workspace ONE Access
- Changing Local Directory Settings in Workspace ONE Access
- Deleting a Local Directory in Workspace ONE Access
- Configuring Authentication Method for System Admin Users in Workspace ONE Access

Creating a Local Directory in Workspace ONE Access

To create a local directory in the Workspace ONE Access service, you specify the user attributes for the directory, create the directory, and identify it with an identity provider.

Set User Attributes at the Global Level Workspace ONE Access

Before you create a local directory in Workspace ONE Access, review the global user attributes on the User Attributes page and add custom attributes, if necessary.

User attributes, such as firstName, lastName, email and domain, are part of a user's profile. In the Workspace ONE Access service, user attributes are defined at the global level and apply to all directories in the service, including local directories. At the local directory level, you can override whether an attribute is required or optional for users in that local directory, but you cannot add custom attributes. If an attribute is required, you must provide a value for it when you create a user.

The following words cannot be used when you create custom attributes.

Table 3-1. Words that cannot be used as Custom Attribute Names

active	addresses	costCenter
department	displayName	division
emails	employeeNumber	entitlements
externalId	groups	id
ims	locale	manager
meta	name	nickName
organization	password	phoneNumber
photos	preferredLanguage	profileUrl

Table 3-1. Words that cannot be used as Custom Attribute Names (continued)

roles	timezone	title
userName	userType	x509Certificate

Note The ability to override user attributes at the directory level only applies to local directories, not to Active Directory or LDAP directories.

Procedure

1 In the Workspace ONE Access console, click the **Identity & Access Management** tab.

2 Click **Setup**, then click the **User Attributes** tab.

3 Review the list of user attributes and add additional attributes, if necessary.

   Note Although this page lets you select which attributes are required, it is recommended that you make the selection for local directories at the local directory level. If an attribute is marked required on this page, it applies to all directories in the service, including Active Directory or LDAP directories.

4 Click **Save**.

What to do next

Create the local directory.

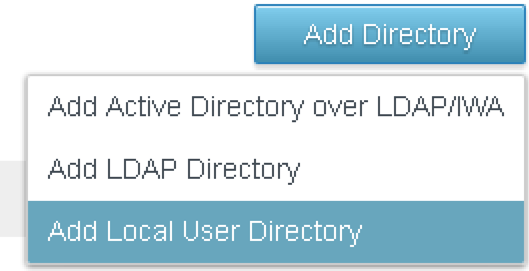
Create a Local Directory Workspace ONE Access

After you review and set global user attributes, create the local directory in Workspace ONE Access.

Procedure

1 In the Workspace ONE Access console, click the **Identity & Access Management** tab, then click the **Directories** tab

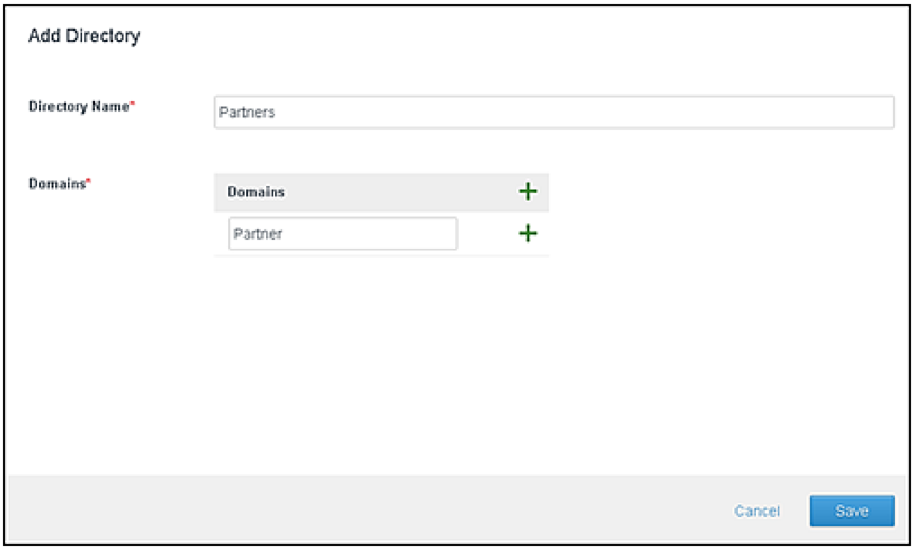
2 Click **Add Directory** and select **Add Local User Directory** from the drop-down menu.



3 In the Add Directory page, enter a directory name and specify at least one domain name.

The domain name must be unique across all directories in the service.

For example:



Add Directory

Directory Name*: Partners

Domains*: Partner

4 Click **Save**.

5 In the Directories page, click the new directory.

6 Click the **User Attributes** tab.

All the attributes from the Identity & Access Management > Setup > User Attributes page are listed for the local directory. Attributes that are marked required on that page are listed as required in the local directory page too.

7 Customize the attributes for the local directory.

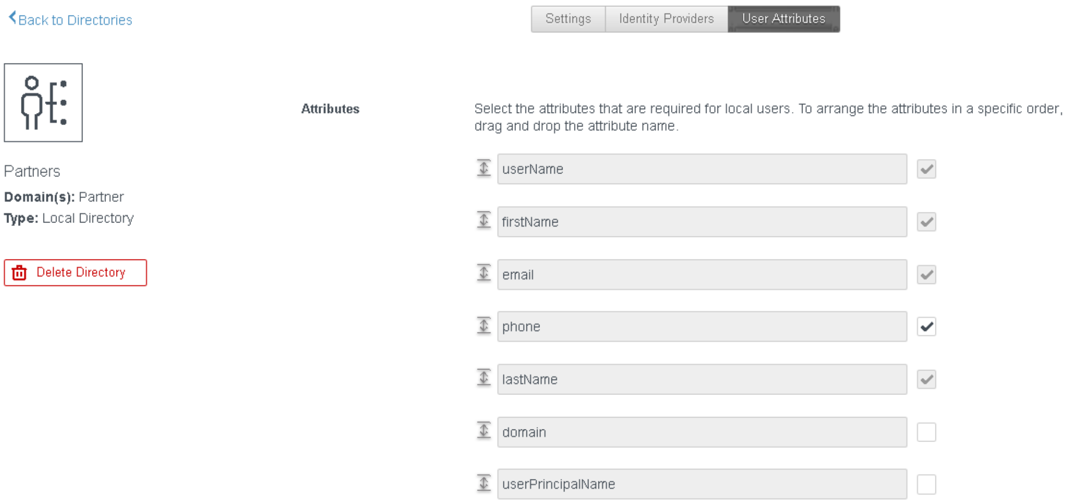
You can specify which attributes are required and which attributes are optional. You can also change the order in which the attributes appear.

Important The attributes userName, firstName, lastName, and email are always required for local directories.

- To make an attribute required, select the check box next to the attribute name.
- To make an attribute optional, deselect the check box next to the attribute name.
- To change the order of the attributes, click and drag the attribute to the new position.

If an attribute is required, when you create a user you must specify a value for the attribute.

For example:



Partners
Domain(s): Partner
Type: Local Directory

Attributes

Select the attributes that are required for local users. To arrange the attributes in a specific order, drag and drop the attribute name.

- userName ☑
- firstName ☑
- email ☑
- phone ☑
- lastName ☑
- domain □
- userPrincipalName □

8 Click **Save**.

What to do next

Associate the local directory with the identity provider you want to use to authenticate users in the directory.

Associate the Local Directory with an Identity Provider in Workspace ONE Access

Associate the local directory with an identity provider in Workspace ONE Access so that users in the directory can be authenticated. Add a new built-it identity provider of type Embedded and enable the Password (Local Directory) authentication method on it.

Prerequisites

The Password (Local Directory) authentication method must be configured in the Identity & Access Management > Authentication Methods page.

Network ranges of defined IP addresses that local users can use set up.

Procedure

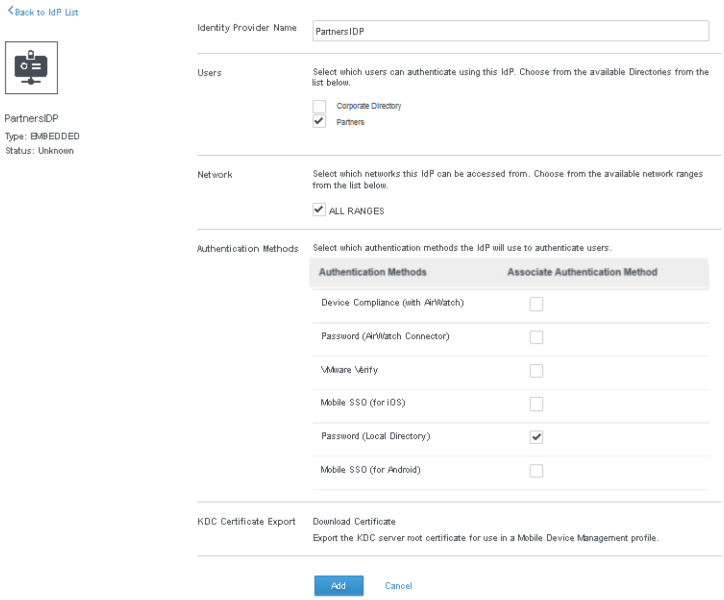
1 In the **Identity & Access Management** tab, click the **Identity Providers** tab.

2 Click **Add Identity Provider** and select **Create Built-in IDP**.

3 Enter the following information.

Option	Description
Identity Provider Name	Enter a name for the identity provider. For example, Local Users.
Users	Select the local directory you created.
Network	Select the networks from which this identity provider can be accessed.

Option	Description
Authentication Methods	Select **Password (Local Directory)**.
KDC Certificate Export	You do not need to download the certificate unless you are configuring mobile SSO for Workspace ONE UEM-managed iOS devices.



PartnersIDP
Type: EMBEDDED
Status: Unknown

Identity Provider Name: PartnersIDP

Users: Select which users can authenticate using this IdP. Choose from the available Directories from the list below.

□ Corporate Directory
☑ Partners

Network: Select which networks this IdP can be accessed from. Choose from the available network ranges from the list below.

☑ ALL RANGES

Authentication Methods: Select which authentication methods the IdP will use to authenticate users.

Authentication Methods	Associate Authentication Method
Device Compliance (with AirWatch)	□
Password (AirWatch Connector)	□
VMware Verify	□
Mobile SSO (for iOS)	□
Password (Local Directory)	☑
Mobile SSO (for Android)	□

KDC Certificate Export: Download Certificate
Export the KDC server root certificate for use in a Mobile Device Management profile.

4 Click **Add**.

Results

The identity provider is created and associated with the local directory. Later, you can configure other authentication methods on the identity provider.

You can use the same identity provider for multiple local directories.

What to do next

Create local users and groups. You create local users and groups in the **Users & Groups** tab in the identity manager console. See Chapter 6 Managing Users and Groups in Workspace ONE Access for more information.

Changing Local Directory Settings in Workspace ONE Access

After you create a local directory in Workspace ONE Access service, you can modify its settings at any time.

You can change the following settings.

- Change the directory name.
- Add, delete, or rename domains.
  - Domain names must be unique across all directories in the service.

  - When you change a domain name, the users that were associated with the old domain are associated with the new domain.
  - The directory must have at least one domain.
  - You cannot add a domain to the System Directory or delete the System Domain.
- Add new user attributes or make an existing attribute required or optional.
  - If the local directory does not have any users yet, you can add new attributes as either optional or required, and change existing attributes to required or optional.
  - If you have already created users in the local directory, you can add new attributes as optional attributes only, and change existing attributes from required to optional. You cannot make an optional attribute required after users have been created.
  - The attributes userName, firstName, lastName, and email are always required for local directories.
  - As user attributes are defined at the global level in the Workspace ONE Access service, any new attributes you add will appear in all directories in the service.
- Change the order in which attributes appear.

Procedure

1. Click the **Identity & Access Management** tab.
2. In the Directories page, click the directory you want to edit.
3. Edit the local directory settings.

Option	Action
Change the directory name	a In the **Settings** tab, edit the directory name. b Click **Save**.
Add, delete, or rename a domain	a In the **Settings** tab, edit the **Domains** list. b To add a domain, click the green plus icon. c To delete a domain, click the red delete icon. d To rename a domain, edit the domain name in the text box.
Add user attributes to the directory	a Click the **Identity & Access Management** tab, then click **Setup**. b Click the **User Attributes** tab. c Add attributes in the **Add other attributes to use** list, and click **Save**.

Option	Action
Make an attribute required or optional for the directory	a In the **Identity & Access Management** tab, click the **Directories** tab. b Click the local directory name and click the **User Attributes** tab. c Select the check box next to an attribute to make it a required attribute, or deselect the check box to make it an optional attribute. d Click **Save**.
Change the order of the attributes	a In the **Identity & Access Management** tab, click the **Directories** tab. b Click the local directory name and click the **User Attributes** tab. c Click and drag the attributes to the new position. d Click **Save**.

Deleting a Local Directory in Workspace ONE Access

You can delete a local directory that you created in the Workspace ONE Access service. You cannot delete the System Directory, which is created by default when you first set up the service.

Caution When you delete a directory, all users in the directory are also deleted from the service.

Procedure

1 Click the **Identity & Access Management** tab, then click the **Directories** tab.

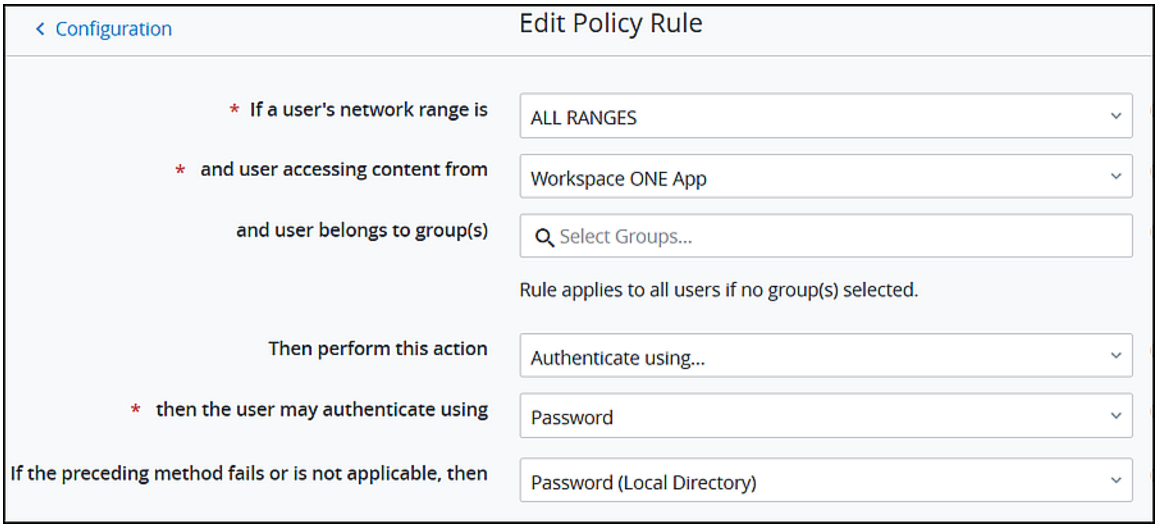
2 Click the directory you want to delete.

3 In the directory page, click **Delete Directory**.

Configuring Authentication Method for System Admin Users in Workspace ONE Access

The default authentication method that admin users enter to log in from the System directory is Password (Local Directory). The default access policy includes a policy rule configured with Password (Local Directory) as a fallback method so that admins can log in to the Workspace ONE Access console and to the portal.

When you create access policies for specific Web and desktop applications that the system admin role is entitled to, configure a rule in the policies to include Password (Local Directory) as a fallback authentication method. Otherwise, an admin cannot log in to the application.



Edit Policy Rule

* If a user's network range is	ALL RANGES
* and user accessing content from	Workspace ONE App
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	Password
If the preceding method fails or is not applicable, then	Password (Local Directory)

How Just-in-Time User Provisioning Works in Workspace ONE Access

4

Just-in-Time provisioning provides another way of provisioning users in the Workspace ONE Access service. Instead of syncing users from an Active Directory or other LDAP directory instance, with Just-in-Time provisioning users are created and updated dynamically when they log in through SAML SSO or OpenID Connect SSO.

Note An OpenID Connect identity provider only can be configured for Workspace ONE Access cloud tenants.

In this scenario, Workspace ONE Access acts as the service provider (SP).

Just-in-Time configuration can only be configured for third-party identity providers. It is not available for the connector. The third-party identity provider manages all user creation and management either through SAML assertions or OpenID Connect claims.

Just-in-Time Directory

The third-party identity provider must have a Just-in-Time directory associated with it in the service.

When you enable Just-in-Time provisioning for an identity provider, you create a Just-in-Time directory and specify one or more domains for it. Users belonging to those domains are provisioned to the directory. If multiple domains are configured for the directory, a domain attribute must be included in the configuration. If a single domain is configured for the directory, a domain attribute is not required, but if specified, its value must match the domain name.

Only one directory, of type Just-in-Time, can be associated with an identity provider that has Just-in-Time provisioning enabled.

User Creation and Management

If Just-in-Time user provisioning is enabled, when a user goes to the Workspace ONE Access service login page and selects a domain, the page redirects the user to the correct identity provider. The user logs in, is authenticated, and the identity provider redirects the user back to the Workspace ONE Access service. The data required to provision the user is in the SSO response and is used to create the user in the Workspace ONE Access service. Only the data for the user attributes that are mapped in the Workspace ONE Access directory are used to provision the user. The user is also added to groups based on the attributes and receives the entitlements that are set for those groups.

On subsequent logins, if there are any changes in user data, the user data is updated in the service.

Just-in-Time provisioned users cannot be deleted. To delete users, you must delete the Just-in-Time directory.

All user management is handled through the identity provider response. You cannot create or update these users directly from the service. Just-in-Time users cannot be synced from Active Directory or other LDAP directories.

This chapter includes the following topics:

Create Local Groups in Workspace ONE Access

Users provisioned through Just-in-Time provisioning in the Workspace ONE Access service are added to groups based on their user attributes and derive their resources entitlements from the groups to which they belong.

Before you configure Just-in-Time provisioning, ensure that you have local groups in the service. Create one or more local groups, based on your needs. For each group, set the rules for group membership and add entitlements.

Note Reference to local groups is synonymous with system domain groups.

Procedure

1. In the Workspace ONE Access console, click the **Users & Groups** tab.
2. Click **Create Group**, provide a name and description for the group, and click **Add**.
3. In the Groups page, click the new group.

4 Set up users for the group.

   a In the left pane, select **Users in This Group**.

   b Click **Modify Users in This Group** and set the rules for group membership.

5 Add entitlements to the group.

   a In the left pane, select **Entitlements**.

   b Click **Add Entitlements** and select the applications and the deployment method for each application.

   c Click **Save**.

Review User Attributes for Just-in-Time Provisioning in Workspace ONE Access

Review the user attributes that are set for all Workspace ONE Access directories in the User Attributes page and modify them, if necessary. When a user is provisioned through Just-in-Time provisioning, the data in the SAML assertion or the OpenID Connect token is used to create the user. Only those SAM attributes or OpenID Connect claims that match the attributes listed in the User Attributes page are used.

Note An OpenID Connect identity provider is only for Workspace ONE Access cloud tenants.

Important If an attribute is marked required in the User Attributes page, the SAML assertion or OpenID Connect token must include the attribute, otherwise login fails.

When you make changes to the user attributes, consider the effect on other directories and configurations in your tenant. The User Attributes page applies to all directories in your tenant.

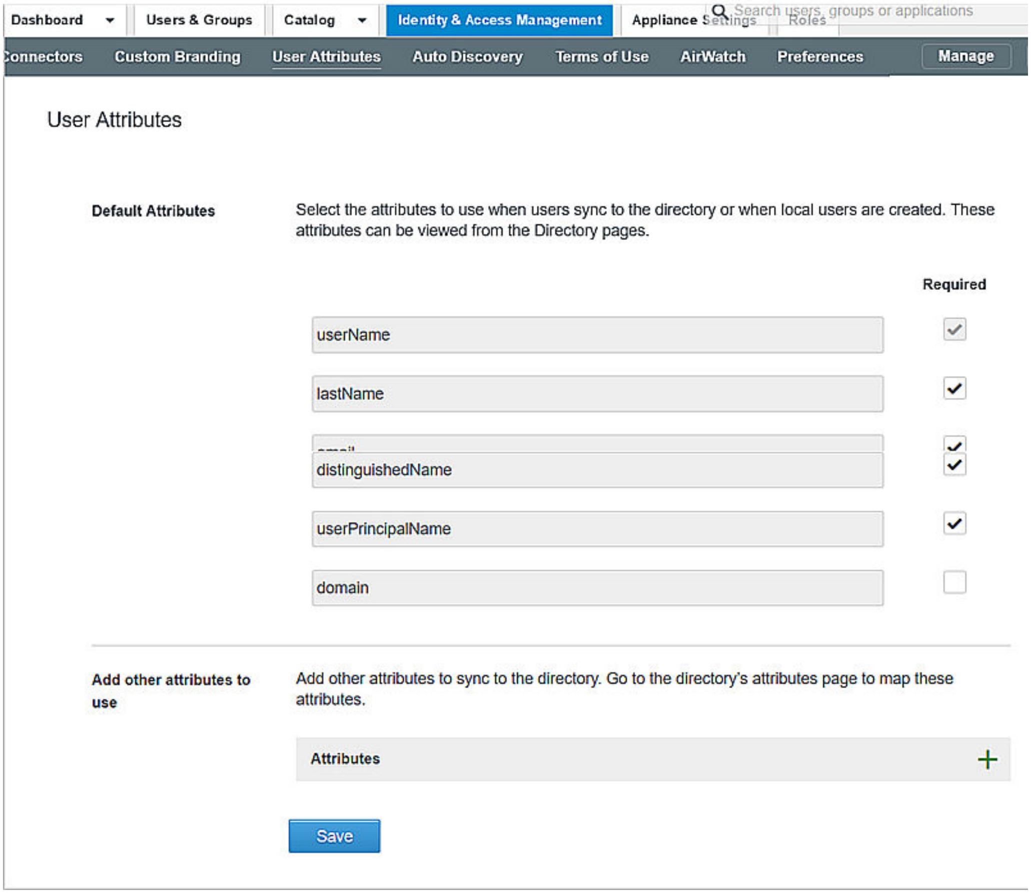
Note You do not have to mark the `domain` attribute required.

Procedure

1 In the administration console, click the **Identity & Access Management** tab.

2 Click **Setup** and click **User Attributes**.

3 Review the attributes and make changes, if necessary.



User Attributes

Default Attributes

Select the attributes to use when users sync to the directory or when local users are created. These attributes can be viewed from the Directory pages.

	Required
userName	☑
lastName	☑
email	☑
distinguishedName	☑
userPrincipalName	☑
domain	☐

Add other attributes to use

Add other attributes to sync to the directory. Go to the directory's attributes page to map these attributes.

Requirements to Use SAML Assertions for Just-in-Time Provisioning in Workspace ONE Access

When Just-in-Time user provisioning is enabled for a SAML third-party identity provider, users are created or updated in the Workspace ONE Access service during login based on SAML assertions. SAML assertions sent by the identity provider must contain certain attributes.

- The SAML assertion must include the `userName` attribute.
- The SAML assertion must include all the attributes that are marked as required in the User Attributes page in the Workspace ONE Access service.

  To view or edit the user attributes in the Workspace ONE Access console, in the **Identity & Access Management** tab, click **Setup** and then click **User Attributes**.

  Important Ensure that the keys in the SAML assertion match the attribute names exactly, including the case.

- If you are configuring multiple domains for the Just-in-Time directory, the SAML assertion must include the `domain` attribute. The value of the attribute must match one of the domains configured for the directory. If the value does not match or a domain is not specified, login fails.
- If you are configuring a single domain for the Just-in-Time directory, specifying the `domain` attribute in the SAML assertion is optional.

  If you specify the `domain` attribute, ensure that its value matches the domain configured for the directory. If the SAML assertion does not contain a domain attribute, the user is associated with the domain that is configured for the directory.
- If you want user name changes to be updated, include the `ExternalId` attribute in the SAML assertion. The user is identified by the `ExternalId`. If on a subsequent login, the SAML assertion contains a different user name, the user is still identified correctly, login succeeds, and the user name is updated in the Workspace ONE Access service.

Attributes from the SAML assertion are used to create or update users as follows.

- Attributes that are listed as required or optional in the User Attribute page in the Workspace ONE Access service are used.
- SAML attributes that do not match any attributes in the User Attributes page are ignored.
- SAML attributes without a value are ignored.

Requirements to Use OpenID Connect Claims for Just-in-Time Provisioning in Workspace ONE Access (Cloud Only)

When Just-in-Time provisioning is enabled for an OpenID Connect third-party identity provider, users are created in Workspace ONE Access and updated dynamically when they log in, based on the token sent by the identity provider.

The OpenID Connect token must include the following attributes (claims) in the response to Workspace ONE Access.

- Domain Attribute. If you are configuring multiple domains for the Just-in-Time directory, the OpenID Connect token must include the domain attribute. The value of the attribute must match one of the domains configured for the directory. If the value does not match or a domain is not specified, login fails.
- The OpenID Connect token must include all the attributes that are marked as required in the User Attributes page in the Workspace ONE Access service.

  To view or edit the user attributes in the Workspace ONE Access console, in the Identity & Access Management tab, click **Setup** and then click **User Attributes**.

The required attributes from the User Attributes page are configured in the OpenID Connect configuration under User Attribute Mapping. After successful authentication, attributes from the OpenID Connect scope ID token are used to create or update a JIT user's information.

- Attributes that are configured on the OpenID Connect identity provider configuration under User Attribute Mapping are used.
- Attributes that do not match any attributes in the User Attributes page are ignored.
- Attributes without a value are ignored.

Configuring Just-in-Time User Provisioning in Workspace ONE Access

You configure Just-in-Time user provisioning for a third-party identity provider while creating or updating the identity provider in the Workspace ONE Access service.

When you enable Just-in-Time provisioning, you create a new Just-in-Time directory and specify one or more domains for it. Users belonging to these domains are added to the directory.

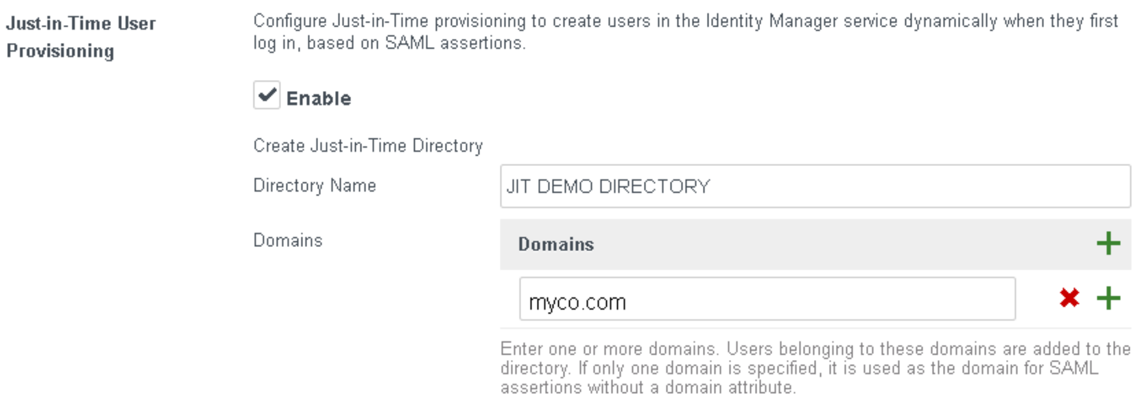
You must specify at least one domain. The domain name must be unique across all the directories in the Workspace ONE Access service. If you specify multiple domains, SAML assertions must include the domain attribute. If you specify a single domain, it is used as the domain for SAML assertions without a domain attribute. If a domain attribute is specified, its value must match one of the domains otherwise login fails.

Procedure

1. Log in to the Workspace ONE Access console.
2. Click the **Identity & Access Management** tab, then click **Identity Providers**.
3. Click **Add Identity Provider** or select an identity provider.
4. In the **Just-in-Time User Provisioning** section, click **Enable**.
5. Specify the following information.
   - A name for the new Just-in-Time directory.
   - One or more domains.

     Important The domain names must be unique across all directories in the tenant.

   For example:



Just-in-Time User Provisioning

Configure Just-in-Time provisioning to create users in the Identity Manager service dynamically when they first log in, based on SAML assertions.

☑ Enable

Create Just-in-Time Directory

Directory Name: JIT DEMO DIRECTORY

Domains: myco.com

Enter one or more domains. Users belonging to these domains are added to the directory. If only one domain is specified, it is used as the domain for SAML assertions without a domain attribute.

6 Complete the rest of the page and click **Add** or **Save**.

Deleting a Just-in-Time Directory in Workspace ONE Access

A Just-in-Time directory in the Workspace ONE Access service is the directory associated with a third-party identity provider that has Just-in-Time user provisioning enabled. When you delete the directory, all users in the directory are deleted and the Just-in-time configuration is disabled. Because a Just-in-Time identity provider can only have a single directory, when you delete the directory, the identity provider can no longer be used.

To enable Just-in-Time configuration for the identity provider again, you create a new directory.

Procedure

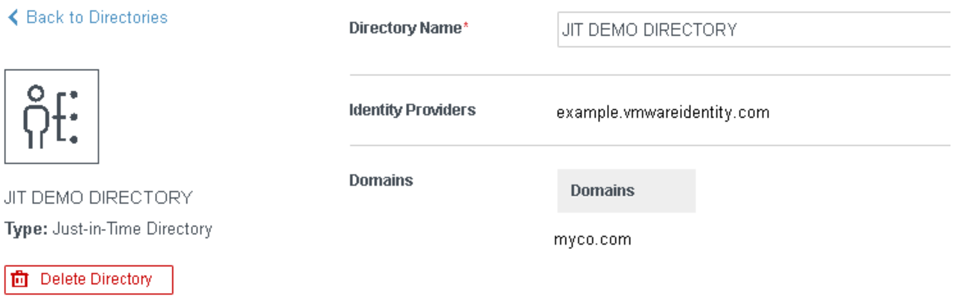
1 In the Workspace ONE Access console, click the **Identity & Access Management** tab.

2 In the Directories page, locate the directory you want to delete.

You can identify Just-in-Time directories by looking at the directory type in the **Type** column.

3 Click the directory name.

4 Click **Delete Directory**.



JIT DEMO DIRECTORY

Type: Just-in-Time Directory

Directory Name*: JIT DEMO DIRECTORY

Identity Providers: example.vmwareidentity.com

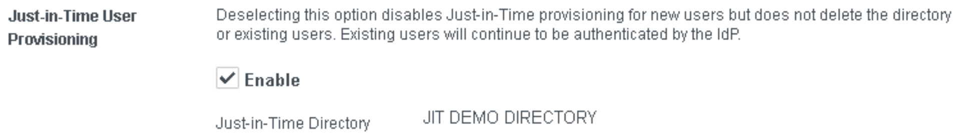
Domains: myco.com

Disabling Just-in-Time User Provisioning in Workspace ONE Access

You can disable Just-in-Time user provisioning in the Workspace ONE Access service. When the Just-in-Time option is disabled, new users are not created, and existing user data is not updated during login. Existing users continue to be authenticated by the identity provider.

Procedure

1. In the Workspace ONE Access console, click the **Identity & Access Management** tab, then click **Identity Providers**.
2. Click the identity provider you want to edit.
3. In the **Just-in-Time User Provisioning** section, deselect the **Enable** checkbox.



Just-in-Time User Provisioning

Deselecting this option disables Just-in-Time provisioning for new users but does not delete the directory or existing users. Existing users will continue to be authenticated by the IdP.

☑ **Enable**

Just-in-Time Directory JIT DEMO DIRECTORY

Just-in-Time Error Messages in Workspace ONE Access

Administrators or end users might see errors related to Workspace ONE Access service Just-in-Time provisioning. For example, if a required attribute is missing in the SAML assertion, an error occurs, and the user is unable to log in.

The following errors can appear in the Workspace ONE Access console.

Error Message	Solution
`If JIT User provisioning is enabled, at least one directory must be associated with identity provider.`	There is no directory associated with the identity provider. An identity provider with the Just-in-Time provisioning option enabled must have a Just-in-Time directory associated with it. 1 In the **Identity & Access Management** tab in the Workspace ONE Access console, click **Identity Providers** and click the identity provider. 2 In the **Just-in-Time User Provisioning** section, specify a directory name and one or more domains. 3 Click **Save**. A Just-in-Time directory is created.

The following errors can appear on the log-in page:

Error Message	Solution
`User attribute is missing: name.`	A required user attribute is missing in the SAML assertion sent by the third-party identity provider. All attributes that are marked required in the User Attributes page must be included in the SAML assertion. Modify the third-party identity provider settings to send the correct SAML assertions.
`Domain is missing and cannot be inferred.`	The SAML assertion does not include the domain attribute and the domain cannot be determined. A domain attribute is required in the following cases: ■ If multiple domains are configured for the Just-in-Time directory. ■ If domain is marked as a required attribute in the User Attributes page. If a domain attribute is specified, its value must match one of the domains specified for the directory. Modify the third-party identity provider settings to send the correct SAML assertions.
`Attribute name: name, value: value.`	The attribute in the SAML assertion does not match any of the attributes in the User Attributes page in the tenant and will be ignored.
`Failed to create or update a JIT user.`	The user could not be created in the service. Possible causes include the following: ■ A required attribute is missing in the SAML assertion. Review the attributes in the User Attributes page and ensure that the SAML assertion includes all the attributes that are marked required. ■ The domain for the user could not be determined. Specify the domain attribute in the SAML assertion and ensure that its value matches one of the domains configured for the Just-in-Time directory.

Managing the User Login Experience in Workspace ONE Access

5

Users are identified uniquely by both their user name and domain when they log in to Workspace ONE Access. The default experience for users who log in to the Hub portal from Workspace ONE Access is to select the domain to which they belong on the first login page that displays.

Because users select their domain first, users that have the same user name but in different domains can log in successfully. For example, you can have a user jane in domain eng.example.com and another user jane in domain sales.example.com.

Workspace ONE Access displays the authentication page based on the access policy rules configured for that domain.

Note Users are not prompted to select a domain when authentication methods based on certificate authentication are configured. The authentication methods include Mobile SSO (iOS), Mobile SSO (Android), and Certificate (Cloud Deployment).

This chapter includes the following topics:

Selecting a Domain When Logging In with Workspace ONE Access

The setting **Show the System Domain on Login Page** is enabled by default in the Identity & Access Management > Setup > Preferences page. Users are presented with the domain drop-down selection menu that lists all Active Directory domains integrated with the Workspace ONE Access server and the local System domain.

If you deselect the Show the System Domain on Login Page setting, the System Domain entry is removed from the domain drop-down menu. When the Workspace ONE Access service contains a single Active Directory domain, users do not see the drop-down menu. They are prompted for their credentials to log in.

When the system domain is not displayed in a drop-down menu and the system domain admin user login is required, the option to use to log in depends on whether you are deployed on-premises or as a cloud tenant.

- For on-premises deployments, you must enable the break-glass URL on the appliance to access the `<yourFQDN>/SAAS/login/0` URL. See Chapter 12 Workspace ONE Access Security Settings Guidelines (On Premises only).
- For cloud tenant deployments, you can use the break-glass URL `<yourFQDN>/SAAS/login/0` to enter system domain admin credentials.

Login Experience in Workspace ONE Access Using Unique Identifier

When you do not want to require users to select their domain before they log in to Workspace ONE Access, you can hide the domain request page. You then select a unique identifier to distinguish users across your organization.

When users log in, a page displays prompting them to enter their unique identifier. Workspace ONE Access attempts to find the user in the internal database. When the Workspace ONE Access service looks up the identifier, the information found includes the domain that the user belongs to. The authentication page that displays is based on the access policy rules for that domain.

The unique identifier can be the user name, email address, UPN, or employee ID. You select the identifier to use from the Identity & Access Management > Preferences page. The unique identifier attribute must be mapped in the User Attributes page and synced from Active Directory.

If multiple users are found that match the identifier and no unique user can be determined, an error message displays. If no user is found, the local user login page is displayed to avoid possible user name enumeration attacks.

Set Up Unique Identifier-Based Log In in Workspace ONE Access

When users use a user name and password authentication method to log in using Workspace ONE Access, you can enable the unique identifier option to display the identifier-based login pages. Users are asked to enter their unique identifier and then are asked to enter the appropriate authentication based on the configured access policy rules.

The authentication methods that support unique identifier-based login include the Password authentication methods, RSA SecurID, and RADIUS.

Prerequisites

- Select the unique identifier user attribute to use in the Identity & Access Management > User Attributes page. Make sure that attribute is used only to identify unique objects.
- Make sure that the selected attributes sync to the directory.
- Verify that the default access policy rules for the user domains reflect the type of authentication to use when the identifier-based login is available.

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, click **Preferences**.

2 If you are setting up unique identifier-based login in a single domain environment, enable **Show the System Domain on Login Page**.

Enabling this functionality is required only when one domain is configured.

3 To hide the domain selection login page, select the **Enable** check box.

4 Select the unique identifier to use from the drop-down menu. The options are **userName** or **email** for cloud tenants. The on premises service also includes **userPrincipalName** and **employeeID** unique identifiers options.

5 In the **Customize the Sign-in Input Prompt** text box, enter the prompt to display in the user text box on the sign-in screen.

If this text box is blank, the sign-in unique identifier value is displayed.

6 Click **Save**.

Requiring Terms of Use to Access the Workspace ONE Catalog

In the Workspace ONE Access service, you can write your organization's own Workspace ONE terms of use and ensure the end user accepts this terms of use before using Workspace ONE.

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

The Terms of Use feature include the following configuration options.

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

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

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

Set Up and Enable Terms of Use in Workspace ONE Access

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

Prerequisites

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

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Setup > Terms of Use**.

2 Click **Add Terms of Use**.

3 Enter a descriptive name for the terms of use.

4 Select **Any**, if the terms of use policy is for all users. To use terms up use policies by device type, select **Selected Devices Platforms** and select the device types that display this terms of use policy.

5 By default, the language of the terms of use that is displayed first is based on the browser language preference settings. Enter the terms of use content for the default language in the text box.

6 Click **Save**.

To add a terms of use policy in another language, click **Add Language** and select another language. The Terms of Use content text box is refreshed and you can add the text in the text box.

You can drag the language name to establish the order that the terms of use are displayed.

7 To begin using the terms of use, click **Enable Terms of Use** on the page that displays.

What to do next

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

View Status of Terms of Use Acceptance in Workspace ONE Access

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

Procedure

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

   A status page displays the action taken, either accepted or declined, with the user name, device ID, version of the policy viewed, platform used, and the date.
3. Click **Cancel** to close the view.

Configure Workspace ONE Access to Display the Login Pages in an iFrame

When an iframe is used to display apps that require authentication from Workspace ONE Access, you must configure the Workspace ONE Access service to display the login pages in the iframe.

In the Identity & Access Management Preferences page, you add the trusted URL addresses that can display the Workspace ONE Access login pages. When users log in to the app, Workspace ONE Access sends an X-Frame-Options HTTP response header that instructs the browser to grant the URL you specify to load itself in the iframe.

Workspace ONE Access **Specification for Using iFrames**

- If you are using 19.03 or later versions of the Workspace ONE Access connector, all authentication methods are supported.
- This feature can be used with Workspace ONE Access 20.01 or later and with Workspace ONE Access Cloud deployments.

Procedure

1. In the Workspace ONE Access console, Identity & Access Management tab, click **Preferences**.
2. In the **URL address from which rendering VMware Workspace ONE Access login pages in iframe is allowed** text box, enter the URL address, including the port number that can display the Workspace ONE Access login page. Enter as **`http://example.com:portnumber`**.

   Click **+** to add additional addresses that can be used.
3. Click **Save**.

4 Test each of the URL addresses you configured to confirm that the log in page displays correctly and you can log in.

To display the login page in the Safari browser, users must disable Prevent Cross-Site Tracking in the Safari browser Privacy & Security settings on their devices.

The login page does not display in the Firefox or Chrome browsers when the page is accessed from an iOS device.

Managing Users and Groups in Workspace ONE Access

6

The users and groups in the Workspace ONE Access service are imported from your enterprise directory or are created as local users and groups in the Workspace ONE Access console.

Users in the Workspace ONE Access service can be users that are synced from your enterprise directory, local users that you provision in the Workspace ONE Access console, or users added with just-in-time provisioning.

Users imported from your enterprise directory are updated in the Workspace ONE Access directory according to your server synchronization schedule. You cannot edit or delete users that sync from Active Directory.

You can create local users and groups. Local users are added to a local directory on the service. You manage the local user attribute mapping and password policies. You can create local groups to manage resource entitlements for users.

Users added with just-in-time provisioning are added and updated dynamically when the user logs in based on SAML assertions sent by the identity provider. All user management is handled through SAML assertions. To use just-in-time provisioning, see Chapter 4 How Just-in-Time User Provisioning Works in Workspace ONE Access

Groups in the Workspace ONE Access service can be groups that are synced from your enterprise directory and local groups that you create in the Workspace ONE Access console. Active Directory group names sync to the directory according to your sync schedule. The users in these groups are not synced to the directory until a group is entitled to resources or a group is added to the access policy rules. You cannot edit or delete groups that sync from Active Directory.

In the Workspace ONE Access console, the Users & Groups pages provides a user-and-group-centric view of the service. You can manage users and groups and monitor resource entitlements, group affiliations, and phone numbers. For local users, you also can manage the password policy.

This chapter includes the following topics:

Managing Users

In the Workspace ONE Access service, users are identified uniquely by both their name and domain. This allows you to have multiple users with the same name in different Active Directory domains. User names must be unique within a domain.

Before you set up the directory in the Workspace ONE Access you specify which default user attributes are required and add additional attributes that you want to map to Active Directory attributes. The attributes and filters you select in Active Directory to map to these attributes determine which Active Directory users sync in the directory. See the Directory Integration with Workspace ONE Access publication for more information about integrating Active Directory with Workspace ONE Access.

The Workspace ONE Access service supports having multiple users with the same name in different Active Directory domains. User names must be unique within a domain. For example, you can have a user jane in domain eng.example.com and another user jane in domain sales.example.com.

Users are identified uniquely by both their user name and domain. The userName attribute in Workspace ONE Access is used for user names and is typically mapped to the sAMAccountName attribute in Active Directory. The domain attribute is used for domains and is typically mapped to the canonicalName attribute in Active Directory.

During directory sync, users that have the same user name but different domains are synced successfully. If there is a user name conflict within a domain, the first user is synced and an error occurs for subsequent users with the same user name.

Tip If you have an existing Workspace ONE Access directory in which the user domain is incorrect or missing, check the domain settings and sync the directory again. See Selecting Users and Groups to Sync.

In the Workspace ONE Access console, you can identify users uniquely by both their user name and domain. For example:

- In the Dashboard tab Users and Groups column, users are listed as user (domain). For example, jane (sales.example.com).
- In the Users & Groups tab, Users page, the DOMAIN column indicates the domain to which the user belongs.
- Reports that display user information, such as the Resource Entitlements report, include a DOMAIN column.

When end users log in to the user portal, on the login page they select the domain to which they belong. If multiple users have the same user name, each can log in successfully using the appropriate domain.

Note This information applies to users synced from Active Directory. If you use a third-party identity provider and configured Just-in-Time user provisioning, see Just-In-Time Provisioning for information. Just-in-Time user provisioning also supports multiple users with the same user name in different domains.

Select Users from Active Directory to Add to the Workspace ONE Access Directory

Active Directory users are added when the user profiles are synced from Active Directory to the Workspace ONE Access directory.

Because members of groups are not synced until the group has entitlements, add all users who need to access the Workspace ONE Access service when you initially set up .

Prerequisites

Active Directory attributes mapped to user attributes in the Identity & Access Management > Setup > Users Attributes page. See the Directory Integration with Workspace ONE Access publication for more information about integrating Active Directory with Workspace ONE Access.

Procedure

1 In the Workspace ONE Access console, Identity & Access Management tab, click **Manager > Directories**.

2 Select the directory where you want to update the user filters.

3 Click **Sync Settings** and select **Users**.

4 In the **Specify the user DNs** row, click **+** and enter the user DNs.

   Enter user DNs that are under the Base DN configured for the Active Directory. If a user DN is outside the BaseDN, users from that DN are synced but cannot log in.

5 Click **Save**.

Reviewing User Profile Information in Workspace ONE Access

The Users page in the Workspace ONE Access console shows the users that are enabled to sign into Workspace ONE.

Select a user name to see detailed user information.

The user profile page displays the personal data associated with the user and the assigned role, either User or Admin. User information that syncs from an external directory can also include the principal name, distinguished name, and external ID data. A local user's profile page displays the available user attributes for users in the local user's directory.

The data in the user profile page for users that sync from your external directory cannot be edited. You can change the role of the user.

The user profile page also includes links to Groups, VMware Verify, and Apps. The Groups page shows the groups that the user is a member of. VMware Verify lists the devices that have been configured to authenticate with VMware Verify. The Apps page lists the applications that the user is entitled to use.

Managing Groups in Workspace ONE Access

In the Workspace ONE Access service, groups are identified uniquely by both the group name and domain.

When new groups are added to the directory from Active Directory, the group names are synced to the directory. Users that are members of the group can sync to the directory under the following conditions.

- The group is entitled to an application in Workspace ONE.
- The group name is added to an access policy.
- The users in the group are manually synced from the Group > Users profile page.

Note If some users need to authenticate before a group syncs to the directory, you can add the individual user to the directory's Sync Settings > Users page .

The Workspace ONE Access service supports having multiple groups with the same name in different Active Directory domains. Group names must be unique within a domain. For example, you can have a group called ALL_USERS in the domain eng.example.com and another group called ALL_USERS in the domain sales.example.com.

During directory sync, groups that have the same name but different domains are synced successfully. If there is a group name conflict within a domain, the first group is synced and an error occurs for subsequent groups with the same name.

In the Workspace ONE Access console User & Groups tab Groups page, Active Directory groups are listed by their group name and domain. In this list, you can distinguish between groups that have the same name. Groups that are created locally in the Workspace ONE Access service are listed by the group name. The domain is listed as Local Users.

Syncing Active Directory Groups to the Workspace ONE Access Directory

When a group distinguished name is mapped from your enterprise directory to the Workspace ONE Access directory, the group names are added to the directory. The group members are not synced to the directory.

The Groups page in the Workspace ONE Access console displays the group names that are synced. The Users in Group column shows the number of members that have been synced. If members are not yet synced, the Users in Group column displays **Not Synced**.

Group members are synced to the directory when the group is entitled to an application in the Catalog or when the group is added to a rule in an access policy in Workspace ONE Access. To sync members of groups when groups are added from Active Directory, you can enable **Sync Group Members to the Directory When Adding Group** in the Identity & Access Management > Preferences page.

Create Local Groups and Configure Group Rules in Workspace ONE Access

You can create groups, add members to groups, and create group rules in the Workspace ONE Access service. You then can populate the groups based on rules you define.

Use groups to entitle more than one user to the same resources at the same time, instead of entitling each user individually. A user can belong to multiple groups. For example, if you create a Sales group and a Management group, a sales manager can belong to both groups.

You can specify which policy settings apply to the members of a group. Users in groups are defined by the rules you set for a user attribute. If a user's attribute value changes from the defined group rule value, the user is removed from the group.

Procedure

1. In the Workspace ONE Access console, Users & Groups tab, click **Groups**.
2. Click **Add Group**.
3. Enter a group name and description of the group. Click **Next**.
4. Add users to the group. To add users to the group, enter a few letters of the user name. As you enter text, names that match are displayed.
5. Select the user name and click **+Add user**.

   Continue to add members to the group.
6. After the users are added to the group, click **Next**.
7. In the Group Rules page, select how group membership is granted. In the drop-down menu, select either **any** or **all**.

Option	Action
Any	Grants group membership when any of the conditions for group membership are met. This action works like an OR condition. For example, if you select **Any** for the rules **Group Is Sales** and **Group Is Marketing**, sales and marketing staff are granted membership to this group.
All	Grants group membership when all the conditions for group membership are met. Using All works like an AND condition. For example, if you select **All of the following** for the rules **Group Is Sales** and **Email Starts With 'western_region'**, only sales staff in the western region are granted membership to this group. Sales staff in other regions is not granted membership.

8 Configure one or more rules for your group. You can nest rules.

Option	Description
Attribute	Select one of these attributes from the first column drop-down menu. Select Group to add an existing group to the group you are creating. You can add other types of attributes to manage which users in the groups are members of the group you create.
Attribute Rules	The following rules are available depending on the attribute you selected. - Select **is** to select a group or directory to associate with this group. Enter a name in the text box. As you type, a list of the available groups or directories appears. - Select **is not** to select a group or directory to exclude. Enter a name in the text box. As you type, a list of the available groups or directories appears. - Select **matches** to grant group membership to entries that exactly match the criteria you enter. For example, your organization might have a business travel department that shares a central phone number. If you want to grant access to a travel booking application for all employees who share that phone number, you create a rule such as Phone matches (555) 555-1000. - Select **does not match** to grant group membership to all directory server entries except those that match the criteria you enter. For example, if one of your departments shares a central phone number, you can exclude that department from access to a social networking application by creating a rule such as Phone does not match (555) 555-2000. Directory server entries with other phone numbers have access to the application. - Select **starts with** to grant group membership for directory server entries that start with the criteria you enter. For example, the organization's email addresses might begin with the departmental name, such as sales_username@example.com. If you want to grant access to an application to everyone n your sales staff, you can create a rule, such as email starts with sales_. - Select **does not start with** to grant group membership to all directory server entries except those that begin with the criteria you enter. For example, if the email addresses of your human resources department are in the format hr_username@example.com, you can deny access to an application by setting up a rule, such as email does not start with hr_. Directory server entries with other email addresses have access to the application.
Using Attribute Any or All	(Optional) To include the attributes Any or All as part of the group rule, add this rule last. - Select **Any** for group membership to be granted when any of the conditions for group membership are met for this rule. Using Any is a way to nest rules. For example, you can create a rule that says All of the following: Group is Sales; Group is California. For Group is California, Any of the following: Phone starts with 415; Phone starts with 510. The group member must belong to your California sales staff and have a phone number that starts with either 415 or 510. - Select **All** for all the conditions to be met for this rule. This is a way to nest rules. For example, you can create a rule that says Any of the following: Group Is Managers; Group is Customer Service. For Group is

Option	Description
	Customer Service, all the following: Email starts with cs_; Phone starts with 555. The group members can be either managers or customer service representatives, but customer service representatives must have an email that starts with cs and a phone number that starts with 555.

9 (Optional) To exclude specific users, enter a user name in the text box and click **Exclude user**.

10 Click **Next** and review the group information. Click **Create Group**.

What to do next

Add the resources that the group is entitled to use.

Edit Group Rules in Workspace ONE Access

You can edit group rules to change the group name, add and remove users, and change the group rules in the Workspace ONE Access service.

Procedure

1 In the console, click **Users & Groups > Groups**.

2 Click the group name to edit.

3 Click **Edit Users in Group**.

4 Click through the pages to make the changes to the name, users in the group, and rules.

5 Click **Save**.

Add Resources to Groups in Workspace ONE Access

The most effective way to entitle users to resources in the Workspace ONE Access service is to add the entitlements to a group. All members of the group can access the applications that are entitled to the group.

Prerequisites

Applications are added to the Catalog page.

Procedure

1 In the Workspace ONE Access console, click **Users & Groups > Groups**.

The page displays a list of the groups.

2 To add resources to a group, click the group name.

3 Click the **Apps** tab and then click **Add Entitlement**.

4 Select the type of application to entitle from the drop-down menu.

The application types shown in the drop-down is based on the types of applications that are added to the catalog.

5 Select the applications to entitle to the group. You can search for a specific application or you can select the box next to **Applications** to select all displayed applications.

   If an application is already entitled to the group, the application is not listed.

6 Click **Save**.

   The sync is run in the background. When the sync is finished, users in the group are synced to the directory and are entitled to the applications.

Sync Members of a Group Manually to Workspace ONE Access Directory

You can sync the members of a group to the Workspace ONE Access directory before the group is entitled to applications or configured in a policy rule.

Procedure

1 In the Workspace ONE Access console Users and Groups tab select **Groups**.

2 Click the group name to sync.

3 Open the **Users** tab and click **Sync Users**.

Create Local Users in Workspace ONE Access

You can create local users in the Workspace ONE Access service to add and manage users who are not provisioned in your enterprise directory. You can create different local directories and customize the attribute mapping for each directory.

You create a directory and select attributes and create custom attributes for that local directory. The required user attributes userName, lastName, firstName, and email are specified at the global level in the Identity & Access Management > User Attributes page. In the local directory user attribute list, you can select other required attributes and create custom attributes to have custom sets of attributes for different local directories. See the Directory Integration with Workspace ONE Access guide.

Create local users when you want to let users access your applications but do not want to add them to your enterprise directory.

- You can create a local directory for a specific type of user that is not part of your enterprise directory. For example, you can create a local directory for partners, who are not usually part of your enterprise directory, and provide them access to only the specific applications they need.
- You can create multiple local directories if you want different user attributes or authentication methods for different sets of users. For example, you can create a local directory for distributors that has user attributes labeled region and market size. You create another local directory for suppliers that has user attribute labeled product category.

You configure the authentication method local users use to sign in to your enterprise Web site. A password policy is enforced for the local user password. You can define the password restrictions and password management rules.

After you provision a user, an email message is sent with information about how to sign in to enable their account. When they sign in, they create a password and their account is enabled.

Add Local Users in Workspace ONE Access

You create one local user at a time in the Workspace ONE Access service. When you add the user, you select the local directory that is configured with the local user attributes to use and the domain that the user signs in to.

In addition to adding user information, you select the user role, either as user or admin. The admin role allows the user to access the administration console to manage the Workspace ONE Access services.

Prerequisites

- Local directory created
- Domain identified for local users
- User attributes that are required selected in the local directory User Attributes page
- Password policies configured
- SMTP server configured in the Appliance Settings tab to send an email notification to newly created local users

Procedure

1. In the Workspace ONE Access console Users & Groups tab, click **Add User**.
2. In the **Add a user page**, select the local directory for this user.

   The page expands to display the user attributes to configure.
3. Select the domain that this user is assigned to and complete the required user information.
4. If this user role is as an admin, in the User text box, select **Admin**.
5. Click **Add**.

Results

The local user is created. An email is sent to the user asking them to sign in to enable their account and create a password. The link in the email expires according to the value set in the Password Policy page. The default is seven days. If the link expires, you can click Rest Password to resend the email notification.

A user is added to existing groups based on the group attribute rules that are configured.

What to do next

Go the local user account to review the profile, add the user to groups, and entitle the user to the resources to use.

If you created an admin user in the system directory who is entitled to resources that are managed by a specific access policy, make sure that the application policy rules include Password (Local Directory) as a fallback authentication method. If Password (Local Directory) is not configured, the admin cannot sign in to the app.

Disable or Enable Local Users in Workspace ONE Access

In the Workspace ONE Access service, you can disable local users to prevent users from signing in and accessing their Hub portal and entitled resources rather than deleting them.

Procedure

1 In the Workspace ONE Access console, click **Users & Groups**.

2 In the Users page, Select the user.

3 Depending on the status of the local user, do one of the following.

   a To disable the account, deselect the **Enable** check box

   b To enable the account, select **Enable**.

Results

Disabled users cannot sign in to the portal or to resources they were entitled to. If they are working in an entitled resource when the local user is disabled, the local user can access the resource until the session times out.

Delete Local Users in Workspace ONE Access

You can delete local users from the Workspace ONE Access service.

Procedure

1 In the Workspace ONE Access console, click **Users & Groups**.

2 Select the user to delete.

   The User Profile page appears.

3 Click **Delete User**.

4 In the confirmation box, click **OK.**

   The user is removed from the Users list.

Results

Deleted users cannot sign in to the portal or to resources they were entitled to.

Managing Passwords in Workspace ONE Access

You can create a password policy to manage local user passwords in Workspace ONE Access. Local users can change their password according to the password policy rules.

Local users can change their password from the Workspace ONE Intelligent Hub portal in the Account Settings Profile page drop-down menu by their name.

Configure Password Policy for Local Users in Workspace ONE Access

You create a password policy to manage local user passwords in Workspace ONE Access.The local user password policy is a set of rules and restrictions on the format and expiration of the local user passwords. The password policy applies only to local users that you created from the Workspace ONE Access console.

The password policy can include password restrictions, a maximum lifetime of a password, and for password resets, the maximum lifetime of the temporary password. You can also set up the lockout policy

The default password policy requires six characters. The password restrictions can include a combination of uppercase, lowercase, numerical, and special characters to require strong passwords be set.

You can configure an account lockout policy to prevent unauthorized access to an account. The policy settings determine the number of failed sign-in attempts within a specific duration of time that activates the user account lockout. An account is locked out for the number of minutes defined in the policy. The default configuration is five failed sign-in attempts in 15 minutes. When a user attempts to sign in a sixth time within 15 minutes and fails, the account is locked out for 15 minutes.

Procedure

1 In the Workspace ONE Access console, select **Users & Groups > Settings**

2 Click **Password Policy** to edit the password restriction parameters.

Option	Description
Minimum length for passwords	Six characters is the minimum length, but you can require more than six characters. The minimum length must be no less than the combined minimum of alphabetic, numeric, and special character requirements.
Lowercase characters	Minimum number of lowercase characters. Lowercase a-z
Uppercase characters	Minimum number of uppercase characters. Uppercase A-Z
Numerical characters (0-9)	Minimum number of numerical characters. Base 10 digits (0-9)
Special characters	Minimum number of non-alphanumeric characters, for example & # % $!
Consecutive identical characters	Maximum number of identical adjacent characters. For example, if you enter 1, the following password is allowed: p@s$word, but this password is not allowed: p@$$word.

Option	Description
Password history	Number of the previous passwords that cannot be selected. For example, if a user cannot reuse any of the last six passwords, type 6. To disable this feature, set the value to 0.
Number of characters from previous password allowed	Enforce a minimum number of characters that can be reused in a new password. For example, if 0 is set, users cannot use any of the same characters from the previous password. If this text box is left blank, this rule is not applied.

3 In the **Password Management** section, edit the password lifetime parameters.

Option	Description
Temporary password lifetime	Number of hours a password reset or forgot password link is valid. ■ The default lifetime value is 24 hours for new Workspace ONE Access tenants deployed after February 24, 2022. ■ Workspace ONE Access tenants deployed before February 24, 2022 might have inherited the old default of 168 hours or have an admin-modified lifetime value to be greater than 24 hours. For security purposes, you should minimize the temporary password lifetime to only the number of hours that your organization deems necessary.
Password lifetime	Maximum number of days that a password can exist before the user must change it.
Password reminder	Number of days before a password expiration that the password expiry notice is sent.
Password reminder notification frequency	After the first password expiry notice is sent, how frequently reminders are sent.

Each box must have a value to set up the password lifetime policy. To not setup a password lifetime policy, enter 0.

4 Define the account lockout policy in the Account Lockout section.

Option	Description
Failed password attempts	The number of incorrect passwords that can be entered. Default is 5. If you set the default to 0, accounts are never locked out for failed password attempts.
Failed authentication attempts interval	The number of minutes in which failed sign-in attempts are counted. The default is 15 minutes.
Account lockout duration	After the failed authentication attempts interval is reached, an account is locked out for the number of minutes set here. The account is automatically unlocked when the time is up. The default is 15 minutes. If you set the minutes to 0, a user's account is not locked out. Users can continue to retry to log in.

5 Click **Save**.

Sync Workspace ONE Access Directory to Correct Domain Information

If you have an existing Workspace ONE Access directory in which the user domain is incorrect or missing, you must check the domain settings and sync the directory again. Checking the domain settings is required so that users or groups that have the same name in different Active Directory domains are synced to the Workspace ONE Access directory successfully and users can log in.

Procedure

1. In the Workspace ONE Access console, go to the **Identity & Access Management > Directories** page.
2. Select the directory to sync, then click **Sync Settings** and click the **Mapped Attributes** tab.
3. In the Mapped Attributes page, verify that the Workspace ONE Access attribute **domain** is mapped to the correct attribute name in Active Directory.

   The domain attribute is typically mapped to the canonicalName attribute in Active Directory. The domain attribute is not marked Required.
4. Click **Save & Sync** to sync the directory.

Managing the Catalog in Workspace ONE Access

7

The Workspace ONE Access catalog is the repository for the resources that you entitle to users. Before you can entitle a particular resource to users, you must populate the catalog with that resource.

The method you use to populate the catalog depends on the type of resource. You can integrate the following types of resources.

- Web applications
- VMware Horizon Cloud Service applications and desktops
- VMware Horizon® desktop and application pools
- Citrix-published resources
- VMware ThinApp® packaged applications

See the Setting Up Resources guide for information about setting up the resources.

In the Workspace ONE Access console Catalog section, you also configure global settings that are applicable to all resources in the catalog and configure other settings specific to web and virtual applications.

- The Catalog > Settings global options include the following.
  - Disable the launcher preference prompt for virtual . See Global Settings to Disable Prompt for Downloading Helper Applications.
  - Create clients to enable access to remote apps. See Creating Clients in Workspace ONE Access for Remote Application Access
  - Enable the People Search feature. See Set Up People Search in Workspace ONE Access.
- The Settings page accessible from the Web Apps, Virtual Apps, or Virtual Apps Collection page include the following.
  - Global Approvals option to manage access to apps that require approvals. See Enabling Application Approval for Resource Usage.
  - SAML Metadata page with the SAML-signing certificate that can be downloaded to send to relying apps to allow logins from Workspace ONE Access. You can generate a certificate signing request from this page when a external signing certificate is required. See Working with SAML Signing Certificates in Workspace ONE Access.

- Application Sources page to configure third-party identity providers as the application source. See Add an Application Source to Workspace ONE Access Catalog.

When Workspace ONE Access is integrated with Workspace ONE UEM, you navigate to the Hub Services console from Catalog > Hub Configuration to customize how the catalog displays in the Workspace ONE Intelligent Hub app on devices and in the Hub web browser view. See the Workspace ONE Hub Services documentation.

This chapter includes the following topics:

Global Settings to Disable Prompt for Downloading Helper Applications

Horizon desktops, Citrix published apps, and ThinApp resources require the following helper applications be installed on the users' computers or device.

- Horizon desktops use Horizon Client.
- Citrix-published apps require Citrix Receiver.

Users are asked to download helper applications to their desktop or device the first time they launch applications from these resources types. You can completely disable this prompt from displaying each time the resource is launched from the Catalog > Settings > Global Settings page.

Disabling the prompt from display is a good option when computers or devices are managed, and you know the helper applications are on the user's local image.

Procedure

1. In the Catalog tab, select **Settings > Global Settings**.
2. Select the operating systems that should not ask to launch the helper applications.
3. Click **Save**.

Creating Clients in Workspace ONE Access for Remote Application Access

You can create a single client to enable a single application to register with Workspace ONE Access to allow user access to a specific application enabled in the Catalog > Settings page.

You can also create a template to enable a group of clients to register dynamically with Workspace ONE Access service to allow access to specified applications.

The initial user authentication request follows the authentication flow defined in the OIDC spec.

Managing Access Token Time to Live

The access token provides temporary secure access to the application. Access tokens have a limited lifetime. When you create the client credentials, the access token is configured with a time to live (TTL). The time configured is the maximum time that the access token is valid for use within an application.

If users frequently use an application, such as Workspace ONE, you can configure the client credentials not to require these users to have to log in every time the access token expires.

Enable Issue Refresh Token so that when the access token expires, the application uses the refresh token to request a new access token. The refresh token is configured with a TTL. New access tokens can be requested until the refresh token expires. When the refresh token expires, the user must log in to the application.

You can configure how long a refresh token can be idle before it cannot be used again. If the refresh token is not used by the refresh token idle TTL, users must log in to the application again.

Example: How Access Token Time to Live Works

The access token time-to-live (TTL) settings in the client credentials are configured as follows.

- Access Token TTL is set to nine hours
- Refresh Token TTL is set to three months
- Refresh Token Idle TTL is set to seven days

If the user uses the application every day, the user does not need to log in again for three months, based on the Refresh Token TTL setting. However, if the user is idle and does not use the application for seven days, the user would need to log in after seven days, based on the Refresh Token idle TTL setting.

Set up Remote Access to a Single Catalog Resource

You can create a client to enable a single application to register with Workspace ONE Access services to allow user access to a specific application.

Registering the details of the application identifies the application as a trusted client for the OAuth service.

You register the client ID, client secret, and a redirect URI with Workspace ONE Access service.

Procedure

1 In the Workspace ONE Access console Catalog tab, select **Settings > Remote App Access**.

2 On the Clients page, click **Create Client**.

3 On the Create Client page, enter the following information about the application.

Label	Description
Access Type	Options are User Access Token or Service Client Token. Set to **Service Client Token**. This indicates that the application accesses the APIs on its own behalf, not on behalf of a user.
Client ID	Enter a unique client identifier for the application to use to authenticate to Workspace ONE Access. The client id must not match any client id in your tenant. The following characters can be used, alphanumeric (A-Z, a-z, 0-9) period (.), underscore (_), and hyphen (-) and at sign (@).
Application	Select Identity Manager.
Scope	Select the information that the token contains. When you select NAAPS, OpenID is also selected.
Redirect URI	Enter the registered redirect URI. You can use a comma separated list to add more than one redirect URL.
Advanced Section	Click **Advanced**.
Shared Secret	Click **Generate Shared Secret** to generate a secret that is shared between this service and the application resource service. Copy and save the client secret to configure in the application setup. The client secret must be kept confidential. If a deployed app cannot keep the secret confidential, then the secret is not used. The shared secret is not used with Web browser-based applications.
Issue Refresh Token	To use refresh tokens, leave this option enabled.
Token Type	Select Bearer. This attribute tells the application what type of access token it was given. For Workspace ONE Access, the tokens are bearer tokens.
Access Token TTL	The access token expires in the number of seconds set in **Access Token Time-To-Live**. If Issue Refresh Token is enabled, when the access token expires, the application uses the refresh token to request a new access token.
Refresh Token TTL	Set the Refresh Token time to live. New access tokens can be requested until the refresh token expires.
Idle Token TTL	Configure how long a refresh token can be idle before it cannot be used again.
User Grant	Do not check **Prompt users for access**.

4 Click **Add**.

Results

The client configuration is displayed on the OAuth2 Client page.

What to do next

In the resource application, configure the Client ID and the generated shared secret. See the application documentation.

Create Remote Access Template

You can create a template to enable a group of clients to register dynamically with the Workspace ONE Access service to allow users access to a specific application.

Procedure

1 In the Workspace ONE Access console Catalog tab, select **Settings > Remote App Access**.

2 Click **Templates**.

3 Click **Create Template**.

4 On the Create Template page, enter the following information about the application.

Label	Description
Template ID	Enter a unique name that identifies this template.
Application	Select Identity Manager
Scope	Select the information that the token contains. When you select NAAPS, OpenID is also selected.
Redirect URI	Enter the registered redirect URI.
Advanced Section	Click **Advanced**.
Token Type	Select Bearer. This attribute tells the application what type of access token it was given. For Workspace ONE Access, the tokens are bearer tokens.
Token Length	Leave the default setting, 32 Bytes.
Issue Refresh Token	To use refresh tokens, leave this option enabled.
Access Token TTL	Set the access token time to live length. The access token expires based on the TTL set in **Access Token Time-To-Live**. If Issue Refresh Token is enabled, when the access token expires, the application uses the refresh token to request a new access token.
Refresh Token TTL	Set the Refresh Token time to live. New access tokens can be requested until the refresh token expires.
Idle Token Time-to-Live (TTL)	Configure how long a refresh token can be idle before it cannot be used again.
User Grant	Do not check Prompt users for access.

5 Click **Add**.

What to do next

In the resource application, set up the Workspace ONE Access service URL as the site that supports integrated authentication.

Enabling Application Approval for Resource Usage

You enable Approvals from the Catalog Web Apps Settings page and configure licensing in the application to manage access to applications that require approval from your organization.

When the licensing option is configured, users view the application in their Workspace ONE catalog and request use of the application. The application icon displays a pending notification

Workspace ONE Access sends the approval request message to the organization's configured approval REST endpoint URL. The server workflow process reviews the request and sends back an approved or denied message to Workspace ONE Access. When an application is approved Pending is changed to Added and the application displays in the user's Workspace ONE launcher page.

Two approval engines are available.

- REST API. The REST API approval engine uses an external approval tool that routes through your Webserver REST API to perform the request and approval responses. You enter your REST API URL in the Workspace ONE Access service and configure your REST APIs with the Workspace ONE Access OAuth client credential values and the call out request and response action.
- REST API via Connector. The REST API via Connector approval engine routes the callback calls through the connector using the Websocket-based communication channel. You configure your REST API endpoint with the call out request and response action.

You can view the Workspace ONE Access resource usage and resource entitlements reports to see the number of approved applications being used.

Set up the REST API Approval Engine

You can register your callout REST URI to integrate your application management system with Workspace ONE Access.

Prerequisites

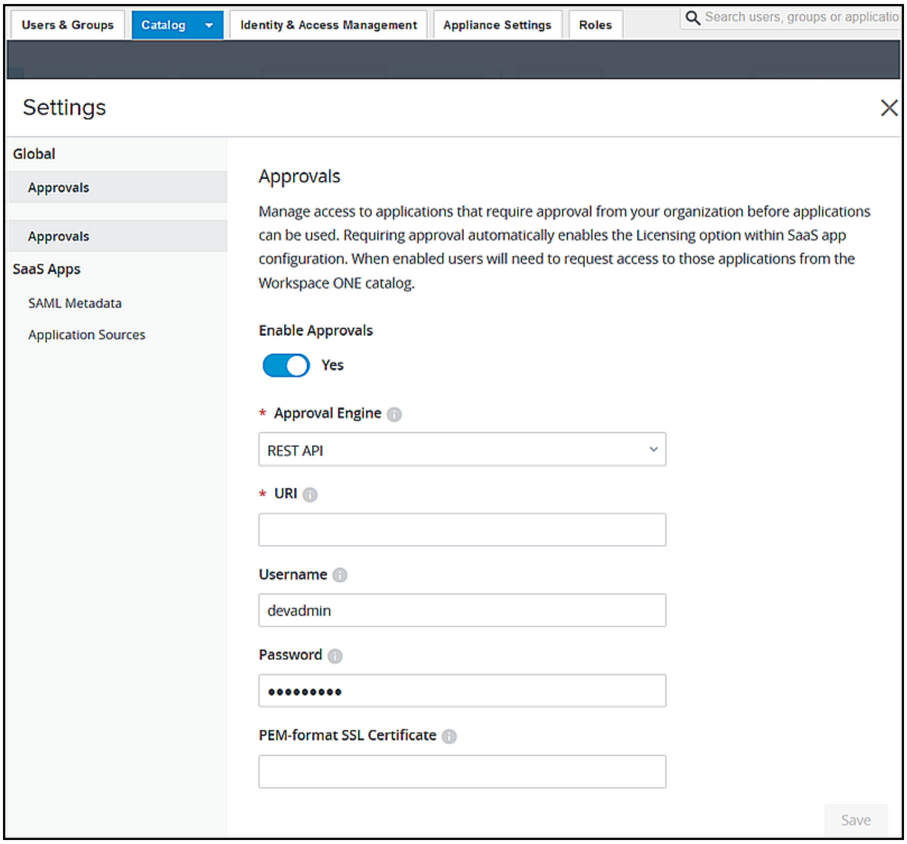
When you select the REST API approval engine, your application management system must be configured, and the URI available through the callout REST API that receives the requests from Workspace ONE Access.

Procedure

1. In the Workspace ONE Access console Catalog tab, select **Web App > Settings > Approvals**.
2. Check **Enable Approvals**.
3. In the Approval Engine drop-down menu, select **REST API**.
4. Configure the following text boxes.

Option	Description
URI	Enter the callback URI of the REST resource that listens for the callout request.
User Name	(Optional) If the REST API requires a user name and password to access, enter the name here. If no authentication is required, you can leave user name and password blank.

Option	Description
Password	(Optional) Enter the password of the user.
PEM-format SSL Certificate	(Optional) If your REST resource is running on a server that has a self-signed certificate or a certificate not trusted by a public certificate authority and is using HTTPS, add the SSL certificate in PEM format here.



Approvals

Manage access to applications that require approval from your organization before applications can be used. Requiring approval automatically enables the Licensing option within SaaS app configuration. When enabled users will need to request access to those applications from the Workspace ONE catalog.

Enable Approvals: Yes

* Approval Engine: REST API

* URI:

Username: devadmin

Password: •••••••••

PEM-format SSL Certificate:

What to do next

Go to the Catalog page and configure the Licensing feature for those apps that require approval before users can use the app.

Working with SAML Signing Certificates in Workspace ONE Access

When configuring SAML, the SAML signing certificate is used to establishes a trust relationship between the identity provider and the service provider to ensure that messages are coming from the expected identity and service providers. The SAML signing certificate is used to sign SAML requests, responses, and assertions from the service to relying applications such as WebEx or Google Apps.

The Workspace ONE Access service automatically creates a self-signed certificate for SAML signing to handle the signing and encryption keys. You do not need a certificate from a certificate authority.

However, if your organizations require signing certificates from a certificate authority, you can generate a certificate signing request (CSR) in the Workspace ONE Access console and send it to your certificate authority. When you receive the signed certificate, you upload the external signing certificate to the Workspace ONE Access service, replacing the self-signed certificate.

The SAML metadata and the SAML signing certificate display from the Catalog > Settings tab. Links for the SAML identity provider and service provider metadata files are also available from this page. The metadata includes configuration information and the certificates.

Download the SAML Signing Certificate from Workspace ONE Access to Configure with Relying Applications

You copy the SAML signing certificate and the SAML service provider metadata from the Workspace ONE Access console and edit the SAML assertion in the third-party identity provider to map Workspace ONE Access users.

Procedure

1 In the Workspace ONE Access console Catalog tab, select **Web Apps Settings > SAML Metadata**.

   a Copy the certificate information that is in the **Signing Certificate** section.

2 Make the SAML SP metadata available to the third-party identity provider instance.

   a In the **SAML Metadata**a section, click **Service Provider (SP) metadata**.

   b Copy and save the displayed information using the method that best suits your organization.

   Use this copied information later when you configure the third-party identity provider.

3 Determine the user mapping from the third-party identity provider instance to Workspace ONE Access.

   When you configure the third-party identity provider, edit the SAML assertion in the third-party identity provider to map Workspace ONE Access users.

NameID Format	User Mapping
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress	The NameID value in the SAML assertion is mapped to the email address attribute in Workspace ONE Access.
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	The NameID value in the SAML assertion is mapped to the username attribute in Workspace ONE Access.

What to do next

Apply the information you copied for this task to configure the third-party identity provider instance.

Generate and Use an External Signing Certificate for SAML Authentication in Workspace ONE Access

To use an external certificate for SAML signing, you must generate a Certificate Signing Request (CSR) from the Workspace ONE Access console. The CSR is sent to a certificate authority to generate the SAML signing certificate.

Note To use an external signing certificate in Workspace ONE Access, you must generate the CSR that you send to the certificate authority from the Workspace ONE Access console.

Generate the Certificate Signing Request

Procedure

1 In the Catalog tab, select **Web Apps Settings > SAML Metadata**.

2 Open the **Generate CSR** tab.

3 Enter the requested information.

Option	Description
Common Name	Enter the fully qualified domain name. For example, `www.example.com`
Organization	Enter the legally registered name of the organization. For example, `Mycompany, Inc.`
Department	Enter the department in your company that is added in the certificate. For example, `IT Services`.
City	Enter the city where your organization is legally located.
State/Province	Enter the state or region where your organization is located. Do not abbreviate.
Country	Enter a few letters of your country name to select the correct country from the list.
Key Generation Algorithm	Select the secure hash algorithm used to sign the CSR.
Key Size	Select the number of bits used in the key. RSA 2048 is recommended. RSA key size smaller than 2048 is considered insecure.

4 Click **Generate**.

Copy the CSR and give it to the certificate authority who will create the certificate.

Upload a Certificate Authority Signing Certificate

When you receive the certificate, upload the certificate to the Workspace ONE Access service. The CA replaces the self-signed certificate.

1 In the Catalog tab, select **Web Apps Settings > SAML Metadata**.

2 Open the **Generate CSR** tab.

3 Click **Upload Certificate** and navigate to the certificate.

4 Click **Open**.

The SAML signing certificate and the SAML metadata files in Workspace ONE Access console are updated with the new certificate.

5 Go to the Identity & Access Management tab, Connectors page and click **Restart** for each connector.

The metadata is updated in the connector.

Next, reconfigure all SAML service provider and identity provider configurations with the updated SAML metadata file. If this is not done, SAML transactions fail and single sign-on does not work. See Download the SAML Signing Certificate from Workspace ONE Access to Configure with Relying Applications.

Replace an Expired Self-Signed SAML Signing Certificate in Workspace ONE Access

When your self-signed SAML signing certificate expires, you must regenerate a new signing certificate in the Workspace ONE Access console and reconfigure all SAML service provider and identity provider configurations with the updated SAML metadata files.

When you are replacing the self-signed SAML signing certificate, users cannot access their apps until all SAML service provider and identity provider configurations are updated. We recommend that you schedule updating the expired certificate during a time that least impacts users access to their apps.

Prerequisites

Take a snapshot of your Workspace ONE Access virtual appliance, connectors, and database before you update the SAML metadata.

Procedure

1 In the Workspace ONE Access console Catalog tab, select **Web Apps > Settings > SAML Metadata**.

2 To confirm that the certificate has expired, open the Service Provider metadata file and the Identity Provider metadata file and verify that the **validUntil** date has expired.

3 To create a new self-signing certificate, in the **Signing Certificate** section on the SAML Metadata page, click **REGENERATE**.

   The self-signed certificate is regenerated and the Service Provider and Identity Provider metadata is updated. Open the files to view the updated **validUntil** date.

4 Go to the Identity & Access Management tab Connectors page and click **Refresh Metadata** for each connector to update the connectors with the regenerated metadata.

What to do next

Make the SAML metadata available to the third-party identity provider instances. In the SAML Metadata page, copy and save the service provider and identity provider metadata files. Reconfigure your SAML service provider and identity provider configuration with the updated SAML metadata files.

Note If you use an external signed CA certificate that expired, create a new Certificate Signing Request in Workspace ONE Access.

Configure Application Sources in Workspace ONE Access

You can add third-party identity providers as an application source in the Workspace ONE Hub catalog to simplify the deployment of large numbers of applications from the third-party identity provider to Workspace ONE.

Web applications that use the SAML 2.0 authentication profile can be added to the catalog. The application configuration is based on the settings configured in the application source. Only the application name and the target URL are required to be configured.

The configured settings and policies from the third-party application source can be applied to all applications managed by the application source.

See the *Setting Up Resources in VMware Workspace ONE Access* guide, Providing Access to Third-Party Managed Applications in Workspace ONE Access for more information.

Grouping Resource into Categories in Workspace ONE Access Catalog

You can organize resources into logical categories to make it easier for users to locate the resource they need in their user portal from a browser or in the VMware Workspace ONE® Intelligent Hub app on devices.

When you create categories consider the structure of your organization, the job function of the resources, and type of resource. For example, you might create a category called HR and another category called Benefits. Assign HR to all the HR resources in your catalog. Also assign Benefits to a specific HR benefit resource you prefer your users to use. You can also assign more than one category to a resource. For example, the resources in the preceding example can also be in a Sales category.

A predefined category called **Recommended** is available in the catalog. In the Intelligent Hub app and web portal, a Recommended section displays the preferred applications that you categorized as recommended. Users select the apps to use and can mark them as favorites. These apps display in the Favorites section on the Hub Catalog page.

Create a Categories in the Catalog Page on Workspace ONE Access

You can create a resource category without immediately applying it or you can create and apply a category to the resource at the same time.

Procedure

1 In the Workspace ONE Access console, click the **Catalog** tab.

2 Click **CATEGORIES** and enter the name.

3 Click **Add category...**.

A new category is created, but not applied to any resource.

4 Select the applications that you want to add to a category and then in **CATEGORIES**, select the check box to use.

The category is added to the application and is listed in the Categories column.

Apply a Category to Resources

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

Prerequisites

Create a category.

Procedure

1 In the Workspace ONE Access console, click the **Catalog** tab.

2 Select the check boxes of all the applications to which to apply the category.

3 Click **Categories** and select the name of the category to apply.

The category is applied to the selected applications.

Remove a Category from an Application

You can disassociate a category from an application.

Procedure

1 In the console, click the **Catalog** tab.

2 Select the check boxes of applications to remove a category.

3 Click **Categories**.

The categories that are applied to the applications are checked.

4 Deselect the category to be removed from the application and close the menu box.

The category is removed from the application's Categories list.

Delete a Category

You can permanently remove a category from the catalog.

Procedure

1 In the Workspace ONE Access console, click the **Catalog** tab.

2 Click **Categories**.

3 Hover over the category to be deleted. An x appears. Click the **x**.

4 Click **OK** to remove the category.

Results

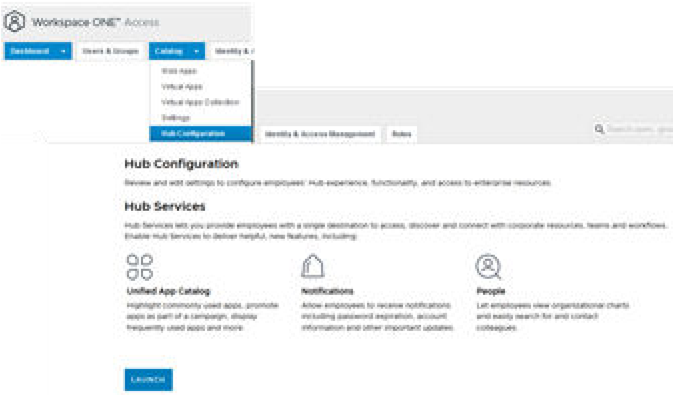
The category no longer appears in the Categories drop-down menu or as a label to any application to which you previously applied it.

Accessing Hub Services in Workspace ONE Access to Set Up Workspace ONE Intelligent Hub

8

You design and set up how employees use Workspace ONE Intelligent Hub to access, discover, and connect with a company's corporate resources, teams, and work flows from the Hub Services console. Users use the Workspace ONE® Intelligent Hub app or the Intelligent Hub portal in a web browser to access these resources.

You navigate to the Hub Services console from the Catalog > Hub Configuration tab in the Workspace ONE Access console.



Hub Configuration

Review and edit settings to configure employees' Hub experience, functionality, and access to enterprise resources.

Hub Services

Hub Services lets you provide employees with a single destination to access, discover and connect with corporate resources, teams and workflows. Enable Hub Services to deliver helpful, new features, including:

Unified App Catalog

Highlight commonly used apps, promote apps as part of a campaign, display frequently used apps and more.

Notifications

Allow employees to receive notifications including password expiration, account information and other important updates.

People

Let employees view organizational charts and easily search for and contact colleagues.

The table shows the features available for cloud and on-premise deployments.

Table 8-1. Hub Features for Workspace ONE Access Cloud and On-premise Deployments

Hub Feature	Availability for Cloud Deployments	Availability for On-premises Deployments
Hub Catalog	Yes	Yes
Notifications	Yes	Yes* *Workspace ONE mobile flow is not available for on premises deployments.
People Search	Yes	Yes
Employee Self-Service support	Yes	Yes
Hub Virtual Assistant	Yes	No
Custom Tab	Yes	Yes
Branding	Yes	Yes

Table 8-1. Hub Features for Workspace ONE Access Cloud and On-premise Deployments (continued)

Hub Feature	Availability for Cloud Deployments	Availability for On-premises Deployments
Templates	Yes	Yes
New Hire Onboarding	Yes	No

You can access Hub Services documentation from the VMware Workspace ONE Documentation page.

Hub Catalog

The Hub catalog is a component of Hub Service used in the Workspace ONE Access service to provide a single destination where users can access their web and virtual apps.

You can arrange the layout of the catalog page to make it easy for users to find apps in the Workspace ONE Intelligent Hub app and in the Hub portal. The App tab displays the New Apps, Recommended, and Categories sections. You can customize the App tab view to show sections such as Promotions and Favorites. You can enable the App Rating feature to let users rate an app with a thumb up or down click.

See Setting Up the Hub Catalog in Hub Services.

Notifications

The Notifications service in Hub Service is a cloud-hosted service designed to generate and serve real-time notifications to your employees. In Hub Services, you can create custom informational and actionable notifications to send to selected groups in your organization.

You can enable the functionality to send a weekly new app notification to all employees.

Users can receive and view notifications in the Workspace ONE Intelligent Hub apps and in the Hub web portal within the For You tab. They can take action or dismiss the notifications so that it moves to the History section.

Users do not need to be in the Workspace ONE Intelligent Hub app to receive notifications if push notifications are enabled.

To use the push notification feature in the Hub Services Notifications service with on premises Workspace ONE Intelligent Hub deployments, you register Workspace ONE Intelligent Hub to the cloud notifications service in the Hub Services console, Notifications tab..

Note Workspace ONE mobile flows is not available for integration into the on-premises version of Workspace ONE Access.

See Using Hub Notifications Service in Workspace ONE Hub Services.

People

The People service in Hub Services lets users search for their colleagues and view user details and organization charts directly from the People tab in the Workspace ONE Intelligent Hub app or Hub portal.

To use the People service in Workspace ONE Intelligent Hub, you enable the People Search feature in the Workspace ONE Access Catalog > Settings page. You then select the user profile attributes that you want to display in the People search results. The attributes are mapped to the corresponding Active Directory attributes. The Workspace ONE Access directory is updated with this information when the directory syncs to Active Directory.

To set up People in Workspace ONE Access, see Set Up People Search in Workspace ONE Access.

Employee Self-Service Support

In the Hub Services Employee Self-Service Support pages, you can customize the type of self-service support that is available in Workspace ONE Intelligent Hub app.

You can add helpful links to the self-service support tab to empower and educate users about how to perform basic device management tasks, investigate issues, and fix problems.

See Configuring Intelligent Hub Employee Self-Service in Hub Services.

Customize the Workspace ONE Intelligent Hub Display and Add a Custom Tab

You can customize the branding design to display your company's logo and company colors in the Workspace ONE Intelligent Hub app and Hub portal.

You can add a custom tab to the Workspace ONE Intelligent Hub app view on devices and web portal. The custom tab can be configured to send users to company resources you want to share with them.

See Customizing the Intelligent Hub Layout from Hub Services.

Note You customize the sign-in screen from the Workspace ONE Access console Branding pages. See Chapter 9 Customize Workspace ONE Access Branding .

Templates

You can create Hub templates with different sets of features and settings to provide a curated experience in Workspace ONE Intelligent Hub. With templates, you can control assignment of Hub Services capabilities to groups of users

Your initial configurations of the Hub Services settings for Workspace ONE Intelligent Hub are the global level settings. You configure global Hub Services settings to meet most of your users' needs. When users require Workspace ONE Intelligent Hub features that are different from the global configuration, you create templates. See Using Hub templates to Set Up Different Workspace ONE Intelligent Hub Experiences for Users.

Hub Virtual Assistant (Cloud Only)

The Hub Services Virtual Assistant, named Hub Assistant, is a digital chatbot you can deploy in your Cloud deployment to offer employee self-service tools. The Hub Assistant chatbot provides employees with an engaging, conversational experience to complete common workflows and to get answers to frequently asked company questions. When Hub Assistant is enabled in the Hub Services console, users can access the virtual assistant from the Intelligent Hub app and from a web browser.

Users can interact with Hub Assistant to open and track ServiceNow Help tickets and to get answers to their questions about benefits and company policies. You can use Hub Assistant as provided out of the box, or you can train Hub Assistant and build out your own internal workflows. See Setting Up Hub Virtual Assistant in Workspace ONE Hub Services.

This chapter includes the following topics:

Set Up People Search in Workspace ONE Access

To use the Hub Services People component in Workspace ONE Intelligent Hub, you enable the People Search feature in Workspace ONE Access. To set up the feature, you map the Active Directory attributes that are required to retrieve information about employees, including profile pictures and management hierarchy in the Workspace ONE Access console.

Prerequisites

- Active Directory must be integrated with Workspace ONE Access to use the People Search feature.
- A list of the Active Directory attributes that must sync to the directory to create the searchable user profiles and organizational hierarchy.

  The attributes that are required to be mapped are **title**, **managerDN**, and **distinguishedName**. The organizational hierarchy and direct reports information in the People Search results is based on the **managerDN** attribute. See the Directory Integration Workspace ONE Access guide on the Workspace ONE Access documentation page.

The attributes that can be mapped are listed in the People Search attributes table. To sync the user's image to the directory, the Active Directory attribute **thumbnailPhoto** must be pre-populated with the user's thumbnail photo. To make sure that the photo is viewed correctly in People Search results, make sure that the thumbnail photo image is square and that the minimum image size is 240 px x 240 px.

Attributes that can be configured for Workspace ONE People Search		
userName	lastName	firstName
email	address	alternatePhoneNumber
businessUnit	costCenter	country
locality	managerDN	mobile
phone	physicalDeliveryOfficeName	postalCode
region	telephoneNumber	title
userPrincipalName	distinguishedName	socialCast
slack	linkedInProfileUrl	imageURL
skypeForBusiness	msExchHideFromAddressLists	

When you do not want user names to appear in People Search, set attribute **`msExchHideFromAddressLists`** in your Active Directory and map that attribute to **`msExchHideFromAddressLists`** in the Workspace ONE Access directory.

- User accounts with the **`msExchHideFromAddressLists`** value set to TRUE do not appear in People Search.
- User accounts, with **`msExchHideFromAddressLists`** set to FALSE or if the attribute value is empty, appear in People Search.

Procedure

1 In the Workspace ONE Access console Catalog tab, select **Settings > People Search.**

2 Select **Enable People Search** and click **Next**.

3 In the page that displays, select the directory to configure for People Search.

4 Review the attribute list and select attributes to reflect which attributes to map to the Active Directory attributes and click **Next**.

To sync the photo profiles from the thumbnailPhoto attribute in the Active Directory, select the **imageURL** attribute.

5 Map the attribute names listed to the Active Directory attributes.

6 If the Workspace ONE Access service is not already configured to sync all users, specify the DN to sync all users. For example, enter **`CN=Users,DC=example,DC=com`**.

   To use the People service successfully, sync all users in your organization to the directory.

   The directory sync profile you configured is added to the Directory > Sync Settings > Users sync list.

7 Click **Save and Sync**.

   The Active Directory mapped attributes for People are synced to the directory.

What to do next

Go to the Hub Services console and enable the People service. See Enabling Access to Workspace ONE People Search in the Hub Service documentation guide.

Customize Workspace ONE Access Branding

9

You can change the appearance of the Workspace ONE Access address tab and the sign-on dialog box from the Identity & Access Management tab.

In addition, you can customize the following from the Workspace ONE Access console.

- Customize the appearance of the VMware Verify app pages.
- Customize the appearance of the Windows 10 desktops provisioned through the Windows 10 Provisioning Service by Workspace ONE UEM.

You can change the appearance of the Workspace ONE Intelligent Hub app view on devices and the Hub portal view in web browsers from the Hub services console. See Customize Branding for Workspace ONE Intelligent Hub.

This chapter includes the following topics:

Customize Branding in Workspace ONE Access Console

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

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Setup > Custom Branding**.

2 Edit the following settings in the form as appropriate.

Form Field	Description
	Names and Logos for Workspace ONE Access Console Address Bar
Company Name	You can add your company's name as the title that appears in the console browser tab. For example, VMware Enter a new company name over the existing one to change the name.
Product Name	The product name displays after the company name in the browser tab. For example, Workspace ONE
Favicon	A favicon is a web site icon associated with a URL that is displayed in the browser address bar. The maximum size of the favicon image is 16 x 16 px. The format can be JPEG, PNG, GIF, or ICO. Click **Upload** to upload a new image to replace the current favicon. You are prompted to confirm the change. The change occurs immediately.
	Sign-In Screen Pages
Logo	Click **Upload** to upload a new logo to replace the current logo on the sign-in screens. When you click **Confirm**, the change occurs immediately. The minimum image size recommended to upload is 350 x 100 px . If you upload images that are larger than 350 x 100 px, the image is scaled to fit 350 x 100-px size. The format can be JPEG, PNG, or GIF.
Background Color	The color that displays for the background of the sign-in screen. Enter the six-digit hexadecimal color code over the existing one to change the background color.
Box Background Color	The sign-in screen box color can be customized. Enter the six-digit hexadecimal color code over the existing code.
Login Button Background Color	The color of the login button can be customized. Enter the six-digit hexadecimal color code over the existing one.
Login Button Text Color	The color of the text that displays on the login button can be customized. Enter the six-digit hexadecimal color code over the existing one.

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

3 Click **Save**.

Results

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

What to do next

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

Customize Branding for VMware Verify Application

If you enabled VMware Verify for two-factor authentication in Workspace ONE Access, you can customize the sign-in page with your company logo.

Prerequisites

VMware Verify enabled as an authentication method in the Workspace ONE Access service.

Procedure

1 In the Workspace ONE Access console Catalogs tab, select **Settings > User Portal Branding**.

2 Edit the VMware Verify section.

Form Item	Description
Logo	Upload the company logo that displays on the approval request pages. The size of the image is 540 x 170 px., PNG format, and 128 KB or smaller.
Icon	Upload an icon that is displayed on the device when VMware Verify is launched. The size of the image is 81 x 81 px., PNG format, and 128 KB or smaller.

3 Click **Save**.

Branding Workspace ONE for Windows 10 Custom Out-of-Box in Workspace ONE Access (On -Premises only)

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

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

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

Procedure

1 In the Workspace ONE Access console Catalogs tab, select **Settings > User Portal Branding**.

2 In the **Desktop Out-of-Box-Experience** section, edit the settings to customize the Workspace ONE registration pages.

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

3 Click **Save**.

Working in the Workspace ONE Access Console Dashboard

10

Two dashboards are available in the Workspace ONE Access console. The User Engagement dashboard can be used to monitor users and resource usage. The System Diagnostics dashboard can be used to monitor the health of the Workspace ONE Access service. The User Engagement dashboard in the administration console can be used to monitor users and resource usage.

This chapter includes the following topics:

Monitor Users and Resource Usage from the Workspace ONE Access Dashboard

The User Engagement Dashboard in the Workspace ONE Access console displays information about users and resources. You can see who is signed in, which applications are being used, and how often the applications are being accessed. You can create reports to track users and group activities and resources usage.

The time that displays on the User Engagement Dashboard is based on the time zone set for the browser. The dashboard updates every one minute.

Procedure

- The header displays the number of unique users that logged in on that day and displays a timeline that shows the number of daily login events over a seven-day period. The Users Logged in Today number is surrounded by a circle that displays the percentage of users that is signed in. The Logins sliding graph displays login events during the week. Point to one of the points in the graph to see the number of logins on that day.
- The Users and Groups section shows the number of user accounts and groups set up in Workspace ONE Access. The most recent users that logged in are displayed first. You can click **See Full Reports** to create an Audit Events report that shows the users who logged in over a range of days.

- The App popularity section displays a bar graph grouped by app type of the number of times that apps were launched over a seven-day period. Point to a specific day to see a tool tip showing which type of apps were being used and how many were launched on that day. The list below the graph displays the number of times the specific apps were launched. Expand the arrow on the right to select to view this information over a day, a week, a month, or 12 weeks. You can click **See Full Reports** to create a Resource Usage report that shows app, resource type and number of users' activity over a range of time.
- The App adoption section displays a bar graph that shows the percentage of people who opened the apps they are entitled to. Point to the app to see the tool tip that shows the actual number of adoptions and entitlements.
- The Apps launched pie chart displays resources that have been launched as a percentage of the whole. Point to a specific section in the pie chart to see the actual number by type of resources. Expand the arrow on the right to select to view this information over a day, a week, a month or 12 weeks.
- The Clients section shows the number of desktops being used.

Monitoring Workspace ONE Access System Information and Health (On-Premises Only)

The Workspace ONE Access System Diagnostics Dashboard displays a detailed overview of the health of the Workspace ONE Access appliances in your environment and information about the services. You can see the overall health across the Workspace ONE Access database server, and the services available on each appliance.

From the System Diagnostics Dashboard, you can select the appliance that you want to monitor and see the status of the services on that appliance, including the version of Workspace ONE Access that is installed. If the database or an appliance is having problems, the header bar displays the appliance's status in red. To see the problems, select the appliance that is shown in red.

You can monitor and manage the configuration settings for each Workspace ONE Access appliance from the System Diagnostics Dashboard page. Click **VA Configuration** under the appliance name to be directed to the configuration pages to install certificates, manage appliance passwords, and download log files. You can also update the database, change the Workspace ONE Access FQDN, and configure an external syslog server.

Information for each service loads independently. The date and time that the data was last updated is shown for each service. You can refresh each section for updated information.

Service being Monitored	Description
Disk Space	Disk space utilization information is displayed by disk partition for /db, /var, /opt/vmware, and /horizon.
Port Connectivity	The port connectivity for each node in the cluster is displayed.

Service being Monitored	Description
User Password Expiration	The expiration dates for the Workspace ONE Access appliance root and remote login passwords are displayed. If a password expires, go to the Settings page and select **VA Configurations**. Open the **System Security** page to change the password.
Configurator - Application Deployment Status	The Web Server Status shows whether the Appliance Configurator page can be accessed. The appliance version shows the version of the Workspace ONE Access appliance that is installed.
Integrated Components	The Workspace ONE Access database connection, audit services, analytics connection information, Elasticsearch health, and Elasticsearch configuration details are displayed.
Certificates	The certificate issuer, subject, start date, and end date are displayed. To manage the certificate, go to the Appliance Settings page and select **VA Configurations**. Open the **Install SSL Certificate** page.
ACS Health - Application Deployment Status	
File Permissions Check	The permission level granted for the following files is displayed. ■ /etc/krb5.conf file owner ■ /etc/krb5.conf file group ■ /etc/krb5.conf file permissions ■ /usr/local/horizon/conf/idm-cacerts file owner ■ /usr/local/horizon/conf/idm-cacerts file group ■ /usr/local/horizon/conf/idm-cacerts file permissions
Application Manager - Application Deployment Status	The Workspace ONE Access Web Application connection status is displayed.
Workspace ONE UEM API Server Status	
Workspace ONE Access FQDN	

Monitoring Rate Limits and Concurrency Limits in Workspace ONE Access (Cloud Only)

Use the Limit Monitoring dashboard to view the rate and concurrency limits that the Workspace ONE Access cloud service imposes on login, launch, and WS-Fed API requests per tenant, and to monitor your usage of these APIs. You can see if the limits are being exceeded and, if so, how often and by how much. When limits are exceeded, users are unable to log in or launch applications during that minute and need to try again the next minute.

Limits improve service availability by helping to prevent your tenant from being overloaded by unforeseen spikes in usage, protect the cloud service from being overloaded by excessive requests to a single tenant, and protect the cloud service from malicious attacks.

About Rate and Concurrency Limits

The Workspace ONE Access Cloud service sets limits on your tenant on login, application launch, and WS-Fed Active Logon API requests. WS-Fed Active Logon requests are typically used to launch Office 365 applications from non-browser clients.

The following limits are set for each API:

- Rate limit: The maximum number of requests allowed per minute
- Concurrency limit: The maximum number of concurrent requests allowed

When the limit is reached, subsequent requests are denied during that minute. For example, if the rate limit for login requests is 750 per minute, the first 750 login requests in a minute are accepted but requests 751-*n* are denied. Similarly, if the concurrency limit for login requests is 500, 500 concurrent requests are accepted but additional requests are denied.

When users cannot log in or launch an application because of the rate limits, they see the following error:

```
Received too many requests. Please try after some time.
```

When users cannot log in or launch an application because of the concurrency limits, they see the following error:

```
Received too many concurrent requests. Please try after some time.
```

If they get an error, users should attempt to log in or launch the application again in the next minute.

Viewing Limits and Monitoring Your Usage

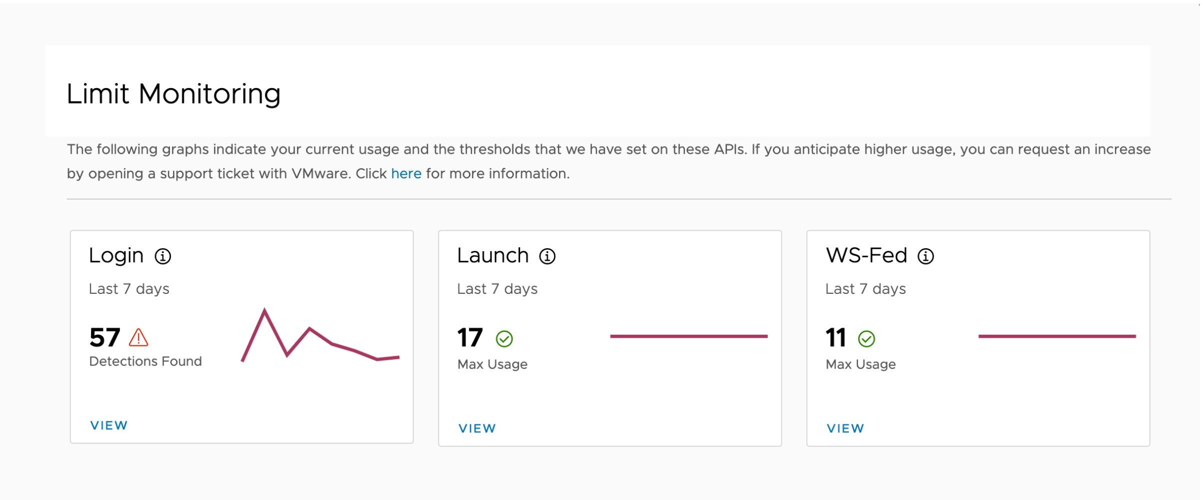
Use the Limit Monitoring dashboard to view the rate and concurrency limits and track your usage against them. You can monitor the usage for each type of request and see if the limit is being exceeded, how often, and by how much. By tracking the trends over time, you can manage your resources better and determine if you have a valid business need for a higher limit. Tracking the usage helps you deliver the best login and application launch experience to your users.

Note The Limit Monitoring dashboard reports the data in terms of API requests, not users. The number of API requests might not always be identical to the number of users.

1 In the Workspace ONE Access console, select **Dashboard > Limit Monitoring**.

   The graphs provide a high-level look at the login, launch, and WS-Fed request rates over the last 7 days and indicate if the rate limit was exceeded. If the rate limit was exceeded, the graph displays a warning and lists the number of times the limit was exceeded. If the rate limit was not exceeded, the graph displays the highest rate that was reached in the last 7 days.

   For example:



Limit Monitoring

The following graphs indicate your current usage and the thresholds that we have set on these APIs. If you anticipate higher usage, you can request an increase by opening a support ticket with VMware. Click here for more information.

Login ⓘ
Last 7 days
57 ⚠
Detections Found
VIEW

Launch ⓘ
Last 7 days
17 ✓
Max Usage
VIEW

WS-Fed ⓘ
Last 7 days
11 ✓
Max Usage
VIEW

In this example, login requests exceeded the rate limit 57 times over the last 7 days, while launch requests and WS-Fed requests were within the limits. The highest rate for launch requests was 17 requests per minute and the highest rate for WS-Fed requests was 11 requests per minute.

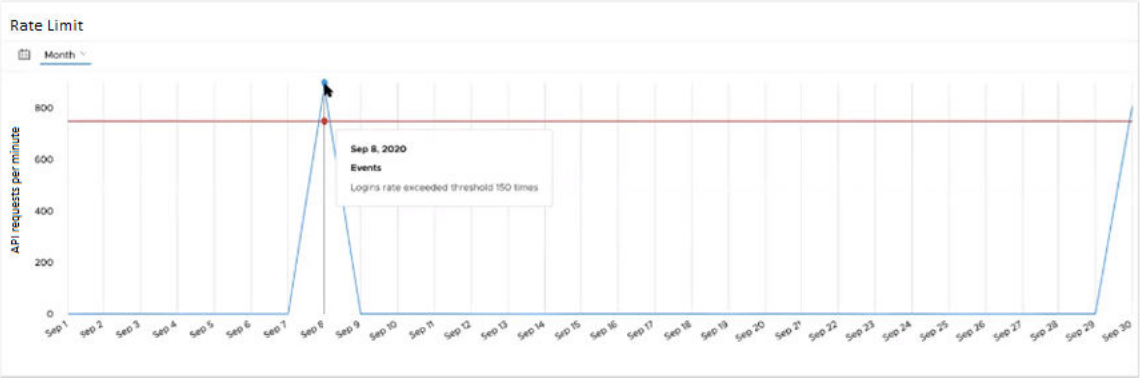
2 For detailed information, click the **VIEW** link for **Login**, **Launch**, or **WS-Fed**, depending on the type of data you want to see.

Rate limit and concurrency limit graphs are displayed.

Rate Limit Graph

The Rate Limit graph displays the rate limit that is currently set on your tenant and your usage during the specified time range.

For example:



Sep 8, 2020
Events
Logins rate exceeded threshold 150 times

The red line indicates the rate limit for your tenant, that is, the maximum number of requests allowed per minute, while the blue line indicates the number of requests made per minute. In this example, the login rate limit is 750 requests per minute and the login rate exceeded the limit 150 times, which indicates that approximately 150 login requests were blocked because the limit was reached.

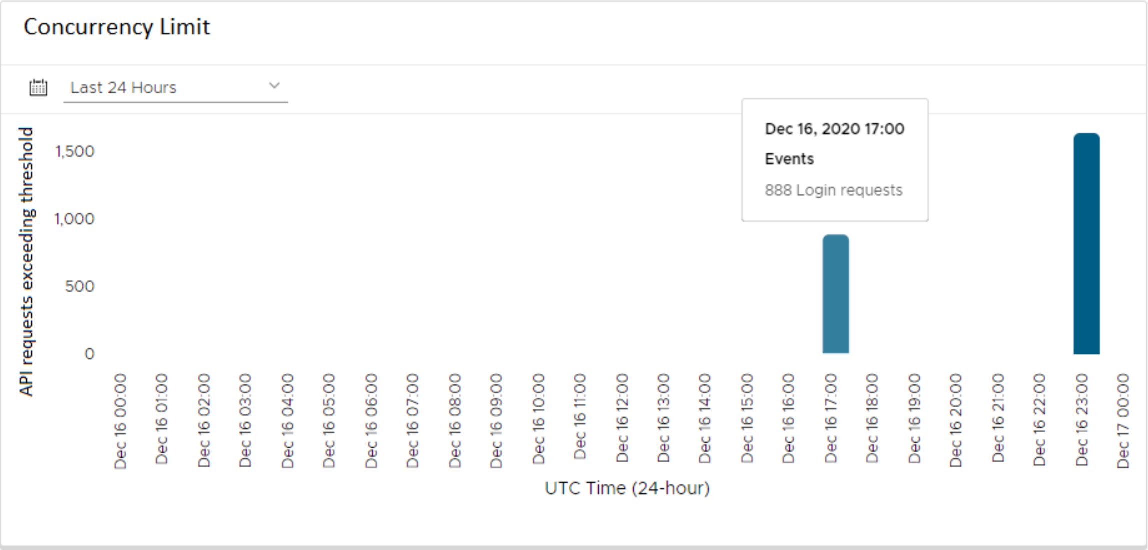
Place your cursor over any data point on the graph to see details. You can also click any data point to get a more granular view. Place your cursor over the red line to view details about the rate limit.

By default, the graph shows usage for the last 7 days but you can customize the time range and interval. Data for the last 90 days is available.

Concurrency Limit Graph

The Concurrency Limit graph displays all events where the concurrency limit was exceeded during the specified time range.

For example:



The bars indicate the number of requests that were blocked within the same minute because the concurrency limit was reached. In this example, the concurrency limit was exceeded twice on December 16. 888 login requests were blocked at 5:00 P.M. and 1641 login requests were blocked at 11:00 P.M.

By default, the graph shows events for the last 7 days but you can customize the time range and interval. Data for the last 90 days is available.

Viewing Additional Information in Audit Events Report

You can view detailed information in the Audit Events report about each login, launch, and WS-Fed request that was denied because rate or concurrency limits were exceeded.

1 In the Workspace ONE Access console, select **Dashboard > Reports** .

2 Select **Audit Events** in the reports drop-down list.

3 For **Type**, select **REQUEST LIMITED** to see all events that occurred because the rate limit was reached or **REQUEST THROTTLED** to see all events that occurred because the concurrency limit was reached

4 Specify the time range and click **SHOW**.

5 In the report, click **View Details** for information about a specific event.

Requesting a Rate Limit Increase

The preset rate limits on the login, launch, and WS-Fed APIs should be sufficient for most tenants under normal circumstances. However, if you consistently exceed the rate limit for a specific API, or if you anticipate an increase in usage for a special event, you can request that the limits be increased.

All requests are subject to an approval process.

To request a rate limit increase:

1. Open a support ticket at https://help.vmware.com.
2. In the ticket, provide answers to the following:
   - What are your usage trends, such as maximum usage per week?
   - Have you exceeded the rate limits in the past? If so, how often?
   - For which API do you want to raise the rate limit?
   - What do you want to raise the rate limit to? Specify your answer as requests per minute.
   - How did you determine the new number?
   - Are you requesting a temporary or permanent increase?
   - Provide a business justification for your request.
   - If you are requesting the increase for a specific event, provide the following information:
     - Projected login requests per minute
     - Projected application launch requests per minute
     - Projected Office 365 launches from non-browser clients per minute

Viewing Reports in Workspace ONE Access

You can create reports to track users and group activities and resource usage from the Workspace ONE Access console Dashboard > Reports page.

You can export reports in an comma-separated value (csv) file format.

Table 10-1. Report Types

Report	Description
Recent Activity	Recent activity is a report about the actions that users performed while using their Hub portal for the past day, past week, past month, or past 12 weeks. The activity can include user information such as how many unique user logins, how many general logins and resource information such as number of resources launched, resource entitlements added. You can click **Show Events** to see the date, time, and user details for the activity.
Resource Usage	Resource usage is a report of all resources in the Catalog with details for each resource about the number of users, launches, and licenses. You can select to view the activities for the past day, past week, past month, or past 12 weeks.
Resource Entitlements	Resource entitlements is a report by resource that shows the number of users entitled to the resource, number of launches, and number of licenses used.
Resource Activity	The resource activity report can be created for all users or a specific group of users. The resource activity information lists the user name, the resource entitled to the user and the date the resource was last accessed, and information about the type of device the user used to access the resource.
Group Membership	Group membership is a lists the members of a group you specify.
Role Membership	Role assignment lists the users that are either API-only administrators or administrators and their email addresses.
Users	Users report lists all the users and provides details about each user, such as the user's email address, role, and group affiliations.
Device Usage	The device usage report can show device usage for all users or a specific group of users. The device information is listed by individual user and includes the user's name, device name, operating system information, and date last used.
Audit events	The audit events report lists the events related to a user you specify, such as user logins for the past 30 days and login failures. You can also view the audit event details. This feature is useful for troubleshooting purposes. See Generate an Audit Event Report in Workspace ONE Access.

Generate an Audit Event Report in Workspace ONE Access

You can generate an audit events report in Workspace ONE Access that lists the events related to a user, including the type of action within a specific date. This feature is useful for troubleshooting purposes.

Procedure

1 In the Workspace ONE Access console, select **Reports > Audit events**

2 Select audit event criteria.

Audit Event Criteria	Description
User	Select this text box to narrow the search of audit events to those generated by a specific user.
Type	This drop-down menu lets you to narrow the search of audit events to a specific audit event type. The drop-down menu does not display all potential audit event types. The list only displays event types that have occurred in your deployment. Audit event types that are listed with all uppercase letters are access events, such as LOGIN and LAUNCH, which do not generate changes in the database. Other audit event types generate changes in the database.
Action	This drop-down menu lets you to narrow your search to specific actions. The list displays events that make specific changes to the database. If you select an access event in the Type drop-down menu, which signifies a non-action event, do not specify an action in the Action drop-down menu.
Object	This text box lets you to narrow the search to a specific object. Examples of objects are groups, users, and devices. Objects are identified by a name or an ID number.
Date range	These text boxes lets you to narrow your search to a date range in the format of "From ___ days ago to ___ days ago." The maximum date range is 30 days. For example, from 90 days ago to 60 days ago is a valid range while 90 days ago to 45 days ago is an invalid range because it exceeds the 30-day maximum. 10,000 records is the maximum number of records that can be exported in one audit report. Export a date range that produces less than 10,000 records and combine the results.

3 Click **Show**.

An audit event report appears according to the criteria you specified.

Note At times when the auditing subsystem is restarting, the Audit Events page might display an error message and not render the report. If you see such an error message about not rendering the report, wait a few minutes and then try again.

4 For more information about an audit event, click **View Details** for that audit event.

Using SSL Certificates in Workspace ONE Access Service (On-Premises Only)

11

When the Workspace ONE Access appliance is installed on premises, a default SSL server certificate is automatically generated. You can use this self-signed certificate for general testing of your implementation.

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate. Workspace ONE Access supports using PEM formatted certificates that include the private key.

You install a signed CA certificate for an appliance from the System Diagnostics page. Select the appliance and click **VA Configuration** to log in as admin to the appliance configuration pages. Select **Install SSL Certificates**.

If you deploy Workspace ONE Access with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client who accesses the Workspace ONE Access service. The clients can include end-user machines, load balancers, proxies, and so on. You can download the root CA from the **Install SSL Certificates > Server Certificates** page.

This chapter includes the following topics:

Installing an SSL Certificate for the Workspace ONE Access Service (On-Premises Only)

When the Workspace ONE Access service is installed, a default SSL server certificate is generated. You can use this self-signed certificate for testing purposes. However, best practice is to use SSL certificates signed by a public Certificate Authority (CA) for your production environment.

Note If a load balancer in front of Workspace ONE Access terminates SSL, the SSL certificate is applied to the load balancer.

Prerequisites

- Generate a Certificate Signing Request (CSR) and obtain a valid, signed SSL certificate from a CA. The certificate can be either a PEM or PFX file. PEM certificates ae encoded with the private key using the PKCS #1 standard.

  If a PEM file is imported, make sure that the file includes the entire certificate chain in the correct order. Make sure to include these tags -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- for each certificate. The order is the primary certificate first and then your intermediate certificate, then the ROOT certificate.
- For the Common Name part of the Subject DN, use the fully qualified domain name that users use to access the Workspace ONE Access service. If the Workspace ONE Access appliance is behind a load balancer, this name is the load balancer server name.
- If SSL is not terminated on the load balancer, the SSL certificate used by the service must include Subject Alternative Names (SANs) for each of the fully qualified domain names in the Workspace ONE Access cluster. Including the SAN enables the nodes within the cluster to make requests to each other. Also include a SAN for the FQDN host name that users use to access the Workspace ONE Access service, in addition to using it for the Common Name, because some browsers require it.
- If your deployment includes a secondary data center, ensure that the Workspace ONE Access certificate includes the FQDN of the load balancer from the primary data center as well as the FQDN of the load balancer from the secondary data center. Otherwise, the certificate must be a wildcard certificate.

Procedure

1. Log in to the Workspace ONE Access console.
2. Select **Dashboard > System Diagnostics Dashboard**.
3. Click **VA Configuration** of the service node you want to configure and log in with the admin user password.
4. Select **Install SSL Certificates > Server Certificate**.
5. In the SSL Certificate tab, select **Custom Certificate**.
6. To import the certificate file, click **Choose File** and navigate to the certificate file to import.

   If a PEM file is imported, make sure that the file includes the entire certificate chain in the correct order. Make sure to include these tags -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- for each certificate. The order is the primary certificate first and then your intermediate certificate.
7. If a PEM file is imported, import the private key. Click **Choose File** and navigate to the Private Key file . Everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY must be included.

   If a PFX file is imported, enter the PFX password.

8 Click **Save.**

Example: PEM Certificate Example

Certificate Chain Example
-----BEGIN CERTIFICATE-----
(Your Primary SSL certificate:your domain_name.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Your Intermediate certificate: <CA>.crt)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Your Root certificate: TrustedRoot.crt)
-----END CERTIFICATE-----

Private Key Example
-----BEGIN RSA PRIVATE KEY-----
(Your PrivateKey: your_domain_name.key)
-----END RSA PRIVATE KEY-----

Installing Trusted Root Certificates for Workspace ONE Access (On-Premises Only)

Install the root or intermediate certificates that should be trusted by the Workspace ONE Access server. The Workspace ONE Access server will be able to establish secure connections to servers whose certificate chain includes any of these certificates.

If the Workspace ONE Access server is configured behind a load balancer and SSL is terminated on the load balancer, install the load balancer's root certificate.

Procedure

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**.

3 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

4 Click **Install SSL Certificates**, then select the **Trusted CAs** tab.

5 Paste the root or intermediate certificate into the text box.

Include everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----.

6 Click **Add.**

Installing a Passthrough Certificate on Workspace ONE Access

To enable sign in using the certificate authentication method, you configure SSL passthrough on the load balancer for the port defined on the **Install SSL Certificate** > **Passthrough Certificate** tab in the Workspace ONE Access console.

Enabling certificate authentication for a Workspace ONE Access on-premises deployment requires setting SSL pass-through at the load balancer. Upload a root certificate and intermediate certificates and private key to Passthrough Certificate tab.

You can also upload a certificate to be used for Android SSO device authentication. See the Android Mobile Single Sign-on to VMware Workspace ONE publication.

Procedure

1 Log in to the Workspace ONE Access console and select **Dashboard > System Diagnostics Dashboard**.

2 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

3 Click **Install Certificates**, then select the **Passthrough Certificate** tab.

4 Enter the passthrough certificate port number to use.

5 Paste the entire certificate in to the **SSL Certificate Chain** text box.

   The certificate must be in an OpenSSL PEM format with the primary certificate first, the intermediate certificates in the middle, and then the root CA certificate.

   The entire certificate is everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----.

6 Paste the certificate private key into the **Private Key** text box.

7 Click **Add**.

Manually Modify Runtime Configuration File for Each Node in Cluster

You must manually update the `runtime-config.properties` file to apply the passthrough certificate port number to use.

1 Using an SSH client, log in to the Workspace ONE Access appliance as the root user.

2 Open the `/usr/local/horizon/conf/runtime-config.properties` file. Enter **`vi /usr/local/horizon/conf/runtime-config.properties`**.

3 Change the `components.certauth.port` gateway port value to the passthrough certificate port number you configured earlier.

4 Save the `runtime-config.properties` file.

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

Repeat this for all appliances in your environment.

Replace SSL Certificate in Workspace ONE Access Service (On-Premises Only)

When the certificate on the service expires, you update the certificate from the Workspace ONE Access console.

Prerequisites

Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.

Procedure

1 Log in to the Workspace ONE Access console.

2 Select **Dashboard > System Diagnostics Dashboard**.

3 Click **VA Configuration** of the service node you want to configure and log in with the admin user password.

4 Select **Install SSL Certificates > Server Certificate**.

5 In the SSL Certificate text box, select **Custom Certificate**.

6 To import the file, click **Choose File** and navigate to the certificate file to import.

   For PEM files, make sure that the file includes the entire certificate chain in the correct order, primary certificate first, then your intermediate certificate, and then the ROOT certificate. The entire certificate is everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- must be included.

7 If a PEM file is imported, import the private key, **Private Key**. Everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY must be included.

   If a PFX file is imported, enter the pfx password.

8 Click **Save.**

   The service is restarted and the certificate is updated.

Workspace ONE Access Security Settings Guidelines (On Premises only)

12

VMware recognizes that security is critical for the consumption of Workspace ONE services within a customer organization. This section provides context to all current security settings available for Workspace ONE Access.

Workspace ONE Access security settings restrict capabilities that might be vulnerable to misconfiguration in Workspace ONE Access. Security settings can be different for different versions of Workspace ONE Access. Make sure to check the version compatibility for each security feature.

Break-Glass URL Endpoint /SAAS/Login/0 Security Setting (Workspace ONE Access 21.08 and later)

URL endpoint `/SAAS/Login/0` is considered a break-glass URL endpoint because this URL endpoint login bypasses all access policies and attempts to authenticate system domain admins using Password (Local Directory) as the authentication method.

Beginning with Workspace ONE Access version 21.08, access through this URL endpoint is deactivated by default as this access might not meet security compliance for customer environments. To enable this break-glass URL endpoint, see Enabling Break-Glass URL Endpoint /SAAS/Login/0 in Workspace ONE Access (On Premises only).

This chapter includes the following topics:

Enabling Break-Glass URL Endpoint /SAAS/Login/0 in Workspace ONE Access (On Premises only)

When Workspace ONE Access system domain admin users cannot log in to the console from the Workspace ONE Access login page, use the break-glass URL endpoint `/SAAS/login/0` hosted by the Workspace ONE Access appliance to log in and resolve the issue.

When the default access policy configuration locks out administrators, system domain admin users can use the break-glass URL endpoint, `/SAAS/login/0`, to access the Workspace ONE Access console. The `/SAAS/login/0` URL authenticates system directory admins with a user name and password.

This login URL is deactivated in Workspace ONE Access service by default. You see an error message instead of the login page when you try to use `https://{yourFQDN}/SAAS/login/0`. All attempts to reach `/SAAS/login/0` are logged to `/opt/vmware/horizon/workspace/logs` with the following message.

```
com.vmware.horizon.service.controller.auth.LoginController - "Break-glass" login end-point
called, access is disabled.
```

Enable /SAAS/login/0

Enable `/SAAS/login/0` so that system domain admin users can log in to the Workspace ONE Access console.

Procedure

1. SSH into the Workspace ONE Access appliance as the root user.
2. Enter **`hznAdminTool configureBreakGlassLogin -enable -loginZero`**.
3. Restart the service on the appliance. Enter **`service horizon-workspace restart`**.

   Repeat this process for all appliances in your environment.

Now Workspace ONE Access system domain admin users can log in using the following login URL.

`https://{yourFQDN}/SAAS/login/0`

Deactivate /SAAS/login/0

After you resolve the default access policy configuration issues, deactivate `/SAAS/login/0` as a login option.

Procedure

1. SSH into the Workspace ONE Access appliance as the root user.
2. Enter **`hznAdminTool configureBreakGlassLogin -disable -loginZero`**.
3. Restart the service on the appliance. Enter **`service horizon-workspace restart`**.

   Repeat this process for all appliances in your environment.