Administering Workspace ONE in VMware Identity Manager Services with AirWatch

VMware AirWatch 9.1.1

vmware®

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

About Administering Workspace ONE in VMware Identity Manager with AirWatch

The Administering Workspace ONE in VMware Identity Manager with AirWatch guide provides information about configuring identity manager features for VMware Workspace™ ONE™.

You can set up and manage access policies, customize the branding for your catalog and user interface to the catalog, and set up auto discovery.

Intended Audience

This information is intended for VMware AirWatch® administrators that are deploying the Workspace ONE catalog, and supporting the use of unmanaged devices.

VMware Identity Manager Features in AirWatch 9.1

1

Upgrading your AirWatch environment to Workspace ONE with VMware Identity Manager enables the following features.

- A unified Workspace ONE application catalog that replaces the existing AirWatch catalog. This catalog includes a new interface, faster performance, and enhanced user management.
- Workspace ONE puts applications first. When users log in for the first time, they see all their applications. Some of the applications are available and others are locked. When users access a locked application, AirWatch enrollment kicks off. When the enrollment is complete, users land back at the application to begin using that resource.
- The option to bring your own device (BYOD) can be easier to implement with the enhanced container support for unmanaged devices. Access and single sign-on to approved Web and SDK-enabled first and third-party native applications is supported.

For information about how to configure these features for Workspace ONE, see the AirWatch Mobile Application Management guide.

Using the VMware Identity Manager Administration Console

After you install the VMware Identity Manager component with AirWatch and configure the Getting Started wizard to integrate the VMware Identity Manager service with AirWatch, the unified catalog is enabled. Users can sign in to their Workspace ONE application.

You can use the admin console to customize the branding for the Workspace ONE sign-in and user portal pages. You can also manage VMware Identity Manager configuration with AirWatch.

The tasks in the admin console are organized by tabs.

Tab	Description
Home	In the Home tab, you can see the users that are synced from AirWatch to the VMware Identity Manager service to access Workspace ONE. You can set up your SMTP settings for email notifications. The System Diagnostics page displays a detailed overview of the health of the VMware Identity Manager service in your environment. You can also see the certificates expiration date.
Auto Discovery	Register your email domain to use the auto-discovery service to make it easier for users to access their applications portal using Workspace ONE. End users can enter their email address instead of the organization's URL.
Custom Branding	In the Custom Branding > Login Branding page, you can customize the appearance of the Workspace ONE sign-in screen. You can also add you company logo and name to display in the catalog. In the User Portal Branding page, you can customize the end-user Web portal.
Identity & Access Management	The AirWatch Cloud Connector password adapter is set up during the initial configuration through the Getting Started wizard. In the Identity & Access Management tab, you can integrate third-party identity providers. The default user attributes used to sync users from Active Directory are listed. In the Authentication Method section, you can enable just-in-time sync from the AirWatch Cloud Connector.
Policies	The Policies tab lists the default access policy and any other Web application access policies you created.

Signing in to the Administration Console

After VMware Identity Manager is integrated with AirWatch, you sign in to the identity manager administration console as the local system administrator. The local administrator is created in the service when you installed the VMware Identity Manager service. Use the password you entered when you created the VMware admin user activation credentials during the AirWatch installation.

To access the administrator console, go to the VMware Identity Manager server hostname that was configured during the AirWatch installation. Example of the URL, `<myco.example.com>:6443`, where the host name is the external host name and port 6443 corresponds to the port entered during the install.

Select the System Domain and enter the administrator user name and password. The user name is **`admin`**.

Registering Email Domains for Auto Discovery

2

You can register your email domain in the auto discovery service in to make it easier for end users to access their apps portal through the Workspace ONE application. End users enter their email address instead of the organization's URL.

When the email domain of the organization is registered for auto discovery, end users enter only their email address in the sign-in page to access their apps portal. For example, they enter **`username@myco.com`**.

When auto discovery is not used, the first time that end users open the Workspace One application, they must provide the complete organization URL. For example, they enter **`myco.vmwareidentity.com`**.

This section includes the following topics:

Set up Auto Discovery in VMware Identity Manager

To register a domain, you enter your email domain and email address in the identity manager admin console Auto Discovery page.

An email message with an activation-token is sent to your email address on the domain. To activate the domain registration, you enter the token in the Auto Discovery page and verify that the domain you registered is your domain.

Note To set up auto discovery for VMware Identity Manager on-premises deployments, you must log in to the admin console as the local admin. You enter the AirWatch ID and password that you created in the AirWatch Web site, https://secure.air-watch.com/register.

Procedure

1 In the administration console, Identity & Access Management tab, click **Setup > Auto Discovery**.

2 (On-premises deployments only). Configure the AirWatch auto discovery URL.

Option	Description
Auto Discovery URL	Enter the URL as https://discovery.awmdm.com.
AirWatch ID	Enter the email address you registered with AirWatch to log in to their Web site.
Password	Enter the password associated with the AirWatch account.

3 In the **Email Domain** text box, enter your organizations email domain to register.

4 In the **Confirmation Email Address** text box, enter an email address on that email domain to receive the verification token.

5 Click **OK**.

The status of this email domain registration is marked Pending. You can have only one pending email domain at a time.

6 Navigate to the email and copy the activation token that is in the message.

7 Return to the **Identity & Access Management > Auto Discovery** page and paste the token in the Activation Token text box

8 Click **Verify** to register the domain.

The email domain is registered and is added to the list of registered email domains on the Auto Discovery page.

End users can now enter their email address in the Workspace ONE application to access their app portal.

What to do next

If you have more than one email domain, add another email domain to register.

Configure SMTP Settings

Configure SMTP server settings to receive an email notification that includes the auto discovery verification token.

Procedure

1 Log in to the administration console.

2 Select the **Home** tab and click **SMTP**.

3 Enter the SMTP server host name.

For example: `smtp.example.com`

4 Enter the SMTP server port number.

For example: `25`

5 (Optional) If the SMTP server requires authentication, enter the user name and password.

6 Click **Save**.

Custom Branding for VMware Identity Manager Services

3

You can customize the logos, fonts, and background that appear in the administration console, the user and administrator sign-in screens, the Web view of the Workspace ONE applications portal, and the Web view of the Workspace ONE application on mobile devices.

You can use the customization tool to match the look and feel of your company's colors, logos, and design.

This section includes the following topics:

Customize Branding in VMware Identity Manager Service

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

Procedure

1 In the administration console, select **Custom Branding**.

2 Select **Login Page Branding** and edit the following settings in the form as appropriate.

Form Field	Description
	Names and Logos
Company Name	Company Name applies to both desktops and mobile devices. You can add your company's name as the title that appears in the browser tab. Enter a new company name over the existing one to change the name.
Product Name	Product Name applies to both desktops and mobile devices. The product name displays after the company name in the browser tab.
Favicon	A favicon is an 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

Form Field	Description
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**.

Custom branding updates to the administration 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.

Update the appearance of the end-user Workspace ONE portal and mobile and tablet view. See Customize Branding for the User Portal

Customize Branding for the User Portal

You can add a logo, change the background colors, and add images to customize the Workspace ONE portal.

Procedure

1 In the administration console, select **Custom Branding**.

2 Select **User Portal Branding** and edit the settings in the form as appropriate.

Form Item	Description
Logo	Add a masthead logo to be the banner at the top of the admin console and Workspace ONE portal Web pages. The maximum size of the image is 220 x 40 px. The format can be JPEG, PNG or GIF.
	Portal

Form Item	Description
Masthead Background Color	Enter a six-digit hexadecimal color code over the existing one to change the background color of the masthead. The background color changes in the application portal preview screen when you type in a new color code.
Masthead Text Color	Enter a six-digit hexadecimal color code over the existing one to change the color of the text that displays in the masthead.
Background Color	The color that displays for the background of the Web portal screen. Enter a new six-digit hexadecimal color code over the existing one to change the background color. The background color changes in the application portal preview screen when you type in a new color code. Select **Background Highlight** to accent the background color. If Background Highlight is enabled, browsers that support multiple background images show the overlay in the launcher and catalog pages. Select **Background Pattern** to set the predesigned triangle pattern in the background color.
Icon Background Color	Enter a six-digit hexadecimal color code to change the background color box surrounding application icons.
Icon Transparency	To set a transparency color, move the slider on the transparency bar.
Name and Icon Color	You can select the text color for names listed under the icons on the app portal pages. Enter a hexadecimal color code over the existing one to change the font color.
Lettering effect	Select the type of lettering to use for the text on the Workspace ONE portal screens.
Image (Optional)	To add an image to the background on the app portal screen instead of a color, upload an image.

3 Click **Save**.

Custom branding updates are refreshed every 24 hours for the user portal. To push the changes sooner, as the administrator, open a new tab and enter this URL, substituting your domain name for myco.example.com. `https://<myco.example.com>/catalog-portal/services/api/branding?refreshCache=true`.

What to do next

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

Implementing Authentication with AirWatch Cloud Connector

4

AirWatch Cloud Connector is integrated with VMware Identity Manager for user password authentication in Workspace ONE.

To implement AirWatch Cloud Connector authentication, in the Built-in Identity Provider, the Password (Local Directory) authentication method is associated to the AirWatch Cloud Connector password authentication method.

You can enable just-in-time support in AirWatch to add new users to VMware Identity Manager when users sign in for the first time. When just-in-time support is enabled, users do not need to wait for the next scheduled sync from the AirWatch server to access Workspace ONE. Instead, new users log in to their Workspace ONE portal, either from an iOS or Android device or their desktop computer and enter their Active Directory user name and password. The VMware Identity Manager service authenticates the Active Directory credentials through the AirWatch Cloud Connector and adds the user profile to the directory.

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

Note User name and password authentication are integrated into the AirWatch Cloud Connector deployment. To authenticate users using other VMware Identity Manager-supported authentication methods, the VMware Identity Manager connector must be configured.

This section includes the following topics:

Viewing Password Authentication Methods for Built-In Identity Providers

The password (with AirWatch Connector) authentication method and the Password (Local Directory) authentication method where configured when you installed and configured the VMware Identity Manager service with AirWatch.

The local directory password authentication is used to authentication the VMware Identity Manager service administrator. The local directory password is associated with the system domain. When admins log in to the service, they select the system domain and enter the password that was configured during the AirWatch installation.

You can view the configuration from the Identity & Access Management > Authentication Methods page.

Managing Configuration of Password Authentication to AirWatch

You can review and manage the Password (AirWatch Connector) configuration that was set up when you installed Airwatch and added the VMware Identity Manager service.

The Password (AirWatch Connector) authentication method is managed from the Identity & Access Management > Authentication Methods page and is associated to the Built-in identity provider in the Identity Providers page.

Important When you upgrade the AirWatch Cloud Connector software, make sure that you update the VMware Identity Manager AirWatch configuration.

Procedure

1. To review and manage the configuration, In the administration console Identity & Access Management tab, select **Authentication Methods**.
2. In the **Password (AirWatch Connector)** Configure column, click the pencil icon.
3. Review the configuration.

Option	Description
Enable AirWatch Password Authentication	This check box enables AirWatch password authentication.
AirWatch Admin Console URL	Pre-populated with the AirWatch URL.
AirWatch API Key	Pre-populated with the AirWatch Admin API key.
Certificate Used for Authentication	Pre-populated with the AirWatch Cloud Connector certificate.
Password for Certificate	Pre-populated with the password for the AirWatch Cloud Connector certificate.
AirWatch Group ID	Pre-populated with the organization group ID.

Option	Description
Number of authentication attempts allowed	The maximum number of failed login attempts when using AirWatch password authentication. No more log ins are allowed after the failed login attempts reach this number. The VMware Identity Manager service tries to use the fallback authentication method if it is configured. The default is five attempts.
JIT Enabled	If JIT is not enabled, select this check box to enable just-in-time provisioning of users in the VMware Identity Manager service dynamically when they log in the first time.

4 Click **Save**.

Managing User Attributes Mapping

You can configure the user attribute mapping between the AirWatch directory and the VMware Identity Manager directory.

The User Attributes page in the VMware Identity Manager, Identity & Access Management tab lists the default directory attributes that are mapped to AirWatch Directory attributes. Attributes that are required are marked with an asterisk. Users missing a required attribute in their profile are not synced to the VMware Identity Manager service.

Table 4-1. Default AirWatch Directory Attributes Mapping

VMware Identity Manager User Attribute Name	Default Mapping to AirWatch User Attribute
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeID	employeeID
domain	Domain
disabled (external user disabled)	disabled
phone	telephoneNumber
lastName	lastname*
firstName	firstname*
email	Email*
userName	username*

Select Attributes to Sync with Directory

When you set up the VMware Identity Manager directory to sync with Active Directory, you specify the user attributes that sync to the directory. Before you set up the directory, you can specify on the User Attributes page which default attributes are required and add additional attributes that you want to map to Active Directory attributes.

When you configure the User Attributes page before the directory is created, you can change default attributes from required to not required, mark attributes as required, and add custom attributes.

After the directory is created, you can change a required attribute not to be required, and you can delete custom attributes. You cannot change an attribute to be a required attribute.

Procedure

1. In the administration console, Identity & Access Management tab, click **User Attributes**.
2. In the Default Attributes section, review the required attribute list and make appropriate changes to reflect which attributes should be required.
3. Click **Save**.

Managing Users

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

Select a user name to see detailed user information.

User Profile

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.

Configuring a Third-Party Identity Provider Instance to Authenticate Users

5

You can configure a third-party identity provider that is used to authenticate users in the VMware Identity Manager service.

Complete the following tasks before using adding the third-party identity provider instance.

- Verify that the third-party instances are SAML 2.0 compliant and that the service can reach the third-party instance.
- Obtain the appropriate third-party metadata information to add when you configure the identity provider in the administration console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

This section includes the following topics:

Download SAML Certificates to Configure with Relying Applications

You copy the SAML signing certificate and the SAML service provider metadata from the service and edit the SAML assertion in the third-party identity provider to map VMware Identity Manager users.

Procedure

1. In the administration console Identity & Access Management tab, select **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. On the Download SAML Certificate page, 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 VMware Identity Manager.

When you configure the third-party identity provider, edit the SAML assertion in the third-party identity provider to map VMware Identity Manager 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 VMware Identity Manager.
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	The NameID value in the SAML assertion is mapped to the username attribute in VMware Identity Manager.

What to do next

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

Add and Configure an Identity Provider Instance

By adding and configuring identity provider instances for your VMware Identity Manager deployment, you can provide high availability, support additional user authentication methods, and add flexibility in the way you manage the user authentication process based on user IP address ranges.

Prerequisites

- Configure the network ranges that you want to direct to this identity provider instance for authentication. See Add or Edit a Network Range.
- Access to the third-party metadata document. This can be either the URL to the metadata or the actual metadata.

Procedure

1 In the admin console Identity & Access Management tab select **Identity Providers**.

2 Click **Add Identity Provider**.

3 Edit the identity provider instance settings.

Form Item	Description
Identity Provider Name	Enter a name for this identity provider instance.
SAML Metadata	Add the third-party IdPs XML-based metadata document to establish trust with the identity provider. 1 Enter the SAML metadata URL or the xml content into the text box. 2 Click **Process IdP Metadata**. The NameID formats supported by the IdP are extracted from the metadata and added to the Name ID Format table. 3 In the Name ID value column, select the user attribute in the service to map to the ID formats displayed. You can add custom third-party name ID formats and map them to the user attribute values in the service. 4 (Optional) Select the NameIDPolicy response identifier string format.
Just-in-Time Provisioning	N/A

Form Item	Description
Users	Select the **Other Directory** which includes the users who can authenticate using this identity provider.
Network	The existing network ranges configured in the service are listed. Select the network ranges for the users based on their IP addresses, that you want to direct to this identity provider instance for authentication.
Authentication Methods	Add the authentication methods supported by the third-party identity provider. Select the SAML authentication context class that supports the authentication method.
Single Sign-Out Configuration	Enable single sign-out to log users out of their identity provider session when they sign out. If single sign-out is not enabled, when users sign out, their identity provider session is still active. (Optional) If the identity provider supports the SAML single logout profile, enable single sign-out and leave the **Redirect URL** text box blank. If the identity provider does not support the SAML single logout profile, enable single sign-out and enter the sign-out URL of the identity provider where users are redirected to when they sign out from VMware Identity Manager. If you configured the redirect URL and if you want users to return to the VMware Identity Manager sign-in page after being redirected to the identity provider sign-out URL, enter the parameter name used by the identity provider redirect URL.
SAML Signing Certificate	Click **Service Provider (SP) Metadata** to see URL to VMware Identity Manager SAML service provider metadata URL. Copy and save the URL. This URL is configured when you edit the SAML assertion in the third-party identity provider to map VMware Identity Manager users.
IdP Hostname	If the Hostname text box displays, enter the host name where the identity provider is redirected to for authentication. If you are using a non-standard port other than 443, you can set the host name as Hostname:Port. For example, myco.example.com:8443.

4 Click **Add**.

What to do next

- Edit the third-party identity provider's configuration to add the SAML Signing Certificate URL that you saved.

Managing Access Policies

6

To provide secure access to the users' apps portal and to launch Web and desktop applications, you configure access policies. Access policies include rules that specify criteria that must be met to sign in to their apps portal and to use their resources.

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

The VMware Identity Manager service includes a default policy that controls access to the service as a whole. This policy is set up to allow access to all network ranges, from all device types, for all users. The session timeout is eight hours and the authentication method is password authentication. You can edit the default policy.

Note The policies do not control the length of time that an application session lasts. They control the amount of time that users have to launch an application.

This section includes the following topics:

Configuring Access Policy Settings

A policy contains one or more access rules. Each rule consists of settings that you can configure to manage user access to their Workspace ONE portal as a whole or to specific Web and desktop applications.

A policy rule can be configured to take actions such as block, allow, or step-up authenticate users based on conditions such as network, device type, AirWatch device enrollment and compliant status, or application being accessed.

Network Range

For each rule, you determine the user base by specifying a network range. A network range consists of one or more IP ranges. You create network ranges from the Identity & Access Management tab, Setup > Network Ranges page before configuring access policy sets.

Each identity provider instance in your deployment links network ranges with authentication methods. When you configure a policy rule, ensure that the network range is covered by an existing identity provider instance.

You can configure specific network ranges to restrict from where users can log in and access their applications.

Device Type

Select the type of device that the rule manages. The client types are Web Browser, Workspace ONE App, iOS, Android, Windows 10, OS X, and All Device Types.

You can configure rules to designate which type of device can access content and all authentication requests coming from that type of device use the policy rule.

Authentication Methods

In the policy rule, you set the order that authentication methods are applied. The authentication methods are applied in the order they are listed. The first identity provider instance that meets the authentication method and network range configuration in the policy is selected. The user authentication request is forwarded to the identity provider instance for authentication. If authentication fails, the next authentication method in the list is selected.

Authentication Session Length

For each rule, you set the number of hours that this authentication is valid. The **re-authenticate after** value determines the maximum time users have since their last authentication event to access their portal or to start a specific application. For example, a value of 4 in a Web application rule gives users four hours to start the Web application unless they initiate another authentication event that extends the time.

Custom Access Denied Error Message

When users attempt to sign in and fail because of invalid credentials, misconfiguration or system error, an access denied message is displayed. The default message is `Access denied as no valid authentication methods were found.`

You can create a custom error message for each access policy rule that overrides the default message. The custom message can include text and a link for a call to action message. For example, in a policy rule for mobile devices that you want to manage, if a user tries to sign in from an unenrolled device, you can create the following custom error message. `Enroll your device to access corporate resources by clicking the link at the end of this message. If your device is already enrolled, contact support for help.`

Add or Edit a Network Range

Create network ranges to define the IP addresses from which users can log in. You add the network ranges you create to specific identity provider instances and to access policy rules.

One network range, called ALL RANGES, is created as the default. This network range includes every IP address available on the Internet, 0.0.0.0 to 255.255.255.255. If your deployment has a single identity provider instance, you can change the IP address range and add other ranges to exclude or include specific IP addresses to the default network range. You can create other network ranges with specific IP addresses that you can apply for a specific purpose.

Note The default network range, ALL RANGES, and its description, "a network for all ranges," are editable. You can edit the name and description, including changing the text to a different language, using the **Edit** feature on the Network Ranges page.

Prerequisites

- Define network ranges for your VMware Identity Manager deployment based on your network topology.

Procedure

1. In the administration console Policies tab, select **Network Ranges**.
2. Edit an existing network range or add a new network range.

Option	Description
Edit an existing range	Click the network range name to edit.
Add a range	Click **Add Network Range** to add a new range.

3. Edit the Add Network Range page.

Form Item	Description
Name	Enter a name for the network range.
Description	Enter a description for the network range.
IP Ranges	Edit or add IP ranges until all desired and no undesired IP addresses are included.

What to do next

- Associate each network range with an identity provider instance.
- Associate network ranges with an access policy rule as appropriate. See Chapter 6 Managing Access Policies.

Applying the Default Access Policy

The VMware Identity Manager service includes a default access policy that controls user access to their Workspace ONE portals and their Web applications. You can edit the policy to change the policy rules as necessary.

When you enable authentication methods other than password authentication, you must edit the default policy to add the enabled authentication method to the policy rules.

Each rule in the default access policy requires that a set of criteria be met to allow user access to the applications portal. You apply a network range, select which type of user can access content, and select the authentication methods to use. See Chapter 6 Managing Access Policies.

The number of attempts the service makes to log in a user using a given authentication method varies. The service only makes one attempt at authentication for Kerberos or certificate authentication. If the attempt is not successful in logging in a user, the next authentication method in the rule is attempted. The maximum number of failed login attempts for Active Directory password and RSA SecurID authentication is set to five by default. When a user has five failed login attempts, the service attempts to log in the user with the next authentication method on the list. When all authentication methods are exhausted, the service issues an error message.

Edit Default Access Policy

You can edit the default access policy to change the policy rules, and you can edit application-specific policies to add or remove applications and to change policy rules.

You can remove an application-specific access policy at anytime. The default access policy is permanent. You cannot remove the default policy.

Prerequisites

- Configure the appropriate network ranges for your deployment. See Add or Edit a Network Range.

Procedure

1. In the administration console Policies tab, select **Edit Default Policy**.
2. In the Policy Rules section, Authentication Method column, select the rule to edit.

   The Edit a Policy Rule page appears with the existing configuration displayed.
3. To configure the authentication order, in the **then the user must authenticate using the following method** drop-down menu, select the authentication method to apply first.
4. (Optional) To configure a fallback authentication method if the first authentication fails, select another enabled authentication method from the next drop-down menu.

   You can add multiple fallback authentication methods to a rule.
5. Click **Save** and click **Save** again on the Policy page.

The edited policy rule takes effect immediately.

What to do next

If the policy is an application-specific access policy, you can also apply the policy to applications from the Catalog page. See Add a Web or Desktop Application-Specific Policy

Add a Web or Desktop Application-Specific Policy

You can create application-specific policies to manage user access to specific Web and desktop applications.

Prerequisites

- Configure the appropriate network ranges for your deployment. See Add or Edit a Network Range.
- If you plan to edit the default policy (to control user access to the service as a whole), configure it before creating an application-specific policy.

Procedure

1. In the administration console Policies tab, click **Add Policy** to add a new policy.
2. Add a policy name and description in the respective text boxes.
3. In the **Applies To** section, click **Select** and in the page that appears, select the applications to associate with this policy.
4. In the Policy Rules section, click **+** to add a rule.

   The Add a Policy Rule page appears.

   a. Select the network range to apply to this rule.

   b. Select the type of device that can access the applications for this rule.

   c. Select the authentication methods to use in the order the authentication method should be applied.

   d. Specify the number of hours an application session can be open.

   e. Click **Save**.
5. Configure additional rules as appropriate.
6. Click **Save**.

Requiring Terms of Use to Access the Workspace ONE Catalog

7

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.

This section includes the following topics:

Set Up and Enable Terms of Use

In the Terms of Use page, 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 administration 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

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

Procedure

1 In the administration 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.