Managing User Authentication Methods in VMware Workspace ONE Access

JAN 2020

VMware Workspace ONE Access 20.01

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

Configuring Authentication in VMware Workspace ONE Access

1

In the VMware Workspace ONE Access™ service, formerly known as VMware Identity Manager, you can manage the following types of authentication services.

- Beginning with the VMware Workspace ONE Access connector version 21.01, the connector provides the following types of authentication services.
  - User Auth service. User Auth service provides Password (cloud deployment), RSA SecurID (cloud deployment), and RADIUS (cloud deployment) authentication methods associated to the Workspace ONE Access service from a built-in identity provider.
  - Kerberos Auth service. Kerberos Auth service provides the connector-based Kerberos authentication for internal users managed from the Workspace ONE Access identity provider.
- Cloud-based authentication methods managed from the Workspace ONE Access service and associated to a built-in identity provider.
- Authentication managed by third-party identity providers.

To install the User Auth and Kerberos Auth authentication services, see the Installing Workspace ONE Access Connector guide. The connector is an on-premises component of the Workspace ONE Access service that integrates with your on-premises infrastructure to provide user authentication..

You can install both authentication services on one connector or the authentication services can be installed on separate connectors. To determine if more than one connector is required, review the sizing requirements in the Workspace ONE Access Connector Installation guide.

The following are the connector-based authentication methods that are enabled and configured from the Enterprise Authentication Methods page in the Workspace ONE Access console.

Authentication Methods	Description
Password (cloud deployment)	For password (cloud) authentication, users are synced from your enterprise directory and are authenticated directly against your enterprise directory. You can select the option to set up password authentication when you configure the directory. You can also set up password authentication later from the Enterprise Authentication Methods page in the Workspace ONE Access console.
RSA SecurID (cloud deployment)	To use the RSA SecurID (cloud deployment) authentication method with Workspace ONE Access, the Workspace ONE Access server is configured as the authentication agent in the RSA SecurID server. RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is an authentication method for users accessing Workspace ONE Access from outside the enterprise network.
RADIUS (cloud deployment)	RADIUS (cloud deployment) authentication provides two-factor authentication options. You set up a RADIUS server that is accessible to the User Auth service on the connector. When users sign in with their user name and passcode, an access request is submitted to the RADIUS server for authentication.
Kerberos Auth	Kerberos authentication provides users who are successfully signed in to their Active Directory domain, access to their apps portal without additional prompts for their credentials. Kerberos authentication uses Integrated Windows Authentication (IWA).

The following are the authentication methods associated to the Workspace ONE Access service. These authentication methods and do not require a Workspace ONE Access connector.

Authentication Method	Description
Certificate (cloud deployment)	Certificate-based authentication can be configured to allow clients to authenticate with certificates on their desktop and mobile devices or to use a smart card adapter for authentication. Certificate-based authentication is based on what the user has and what the person knows. An X.509 certificate uses the public key infrastructure standard to verify that a public key contained within the certificate belongs to the user.
Mobile SSO (for Android)	Mobile SSO for Android is a certificate proxy authentication used for single sign-in authentication for Workspace ONE UEM-managed Android devices. A proxy service is set up between the Workspace ONE Access service and Workspace ONE UEM to retrieve the certificate from Workspace ONE UEM for authentication.
Mobile SSO (for iOS)	Mobile SSO for iOS authentication is used for single sign-in authentication on Workspace ONE UEM-managed iOS devices. Mobile SSO for iOS authentication uses a Key Distribution Center (KDC) that is part of the Workspace ONE Access service.
Password (AirWatch Connector)	The AirWatch Cloud Connector can be integrated with the Workspace ONE Access service for user password authentication. You configure the Workspace ONE Access service to sync users from the Workspace ONE UEM directory.
VMware Verify	VMware Verify can be used as the second authentication method when two-factor authentication is required. The first authentication method is user name and password, and the second authentication method is a VMware Verify requested approval or code.

After the authentication methods are configured, you create access policy rules that specify the authentication methods to be used by device type. Users are authenticated based on the authentication methods, the default access policy rules, network ranges, and the identity provider instance you configure. See Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users .

User Auth Service Authentication Methods in Workspace ONE Access

2

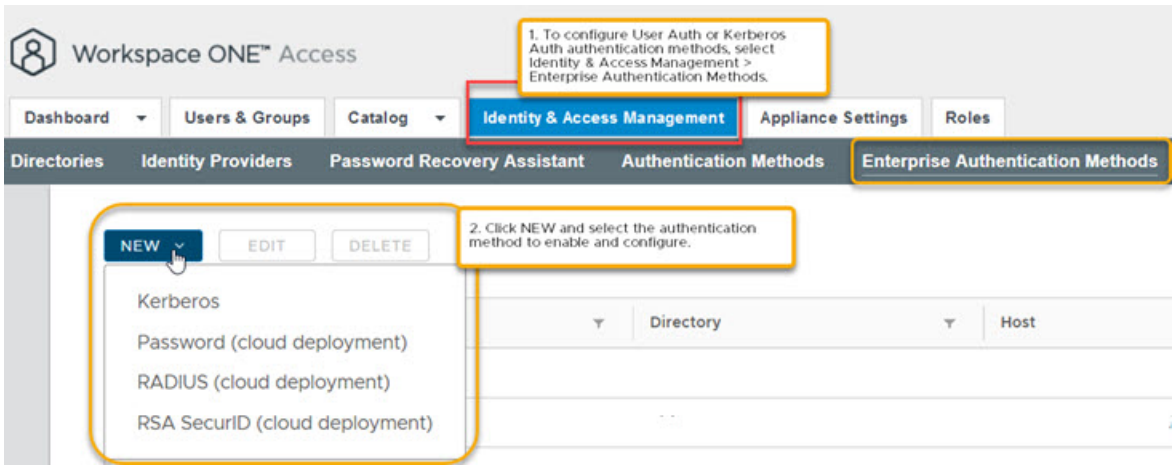
The User Auth service is a component of the Workspace ONE Access connector that includes Password (cloud deployment), RSA SecurID (cloud deployment), and RADIUS (cloud deployment) authentication methods. You enable and configure these authentication methods from the Workspace ONE Access console.

To set up User Auth service authentication methods, you install a Workspace ONE Access connector on a Windows server and select to install the User Auth service. The Workspace ONE Access connector is configured in outbound-only connection mode in the enterprise network. Inbound connectivity is not required. See the Installing VMware Workspace ONE Access Connector guide for system requirements and installation procedures.

A wizard walks you through the steps to select the directory and host to be used and the configuration steps required for each authentication method. After the authentication method is added, you associate the method to a built-in identity provider.

The Workspace ONE Access service manages the user authentication methods.

Figure 2-1. Accessing the Authentication Method Page in the Console



This chapter includes the following topics:

- Configuring Password (Cloud) Authentication in Workspace ONE Access
- Configuring RSA SecurID (Cloud) For Workspace ONE Access
- Configuring RADIUS for Workspace ONE Access

- Enable User Auth Service Debug Logs In Workspace ONE Access Connector

Configuring Password (Cloud) Authentication in Workspace ONE Access

Password (cloud deployment) authentication validates the user name and password against your enterprise directory.

You can set up password authentication when you create a directory in the Workspace ONE Access service, or you can set it up later from the Enterprise Authentication Methods section in the Workspace ONE Access console.

When you configure Password authentication, you select the directory types that correspond to the Directory Sync services directory types you configured for the directory.

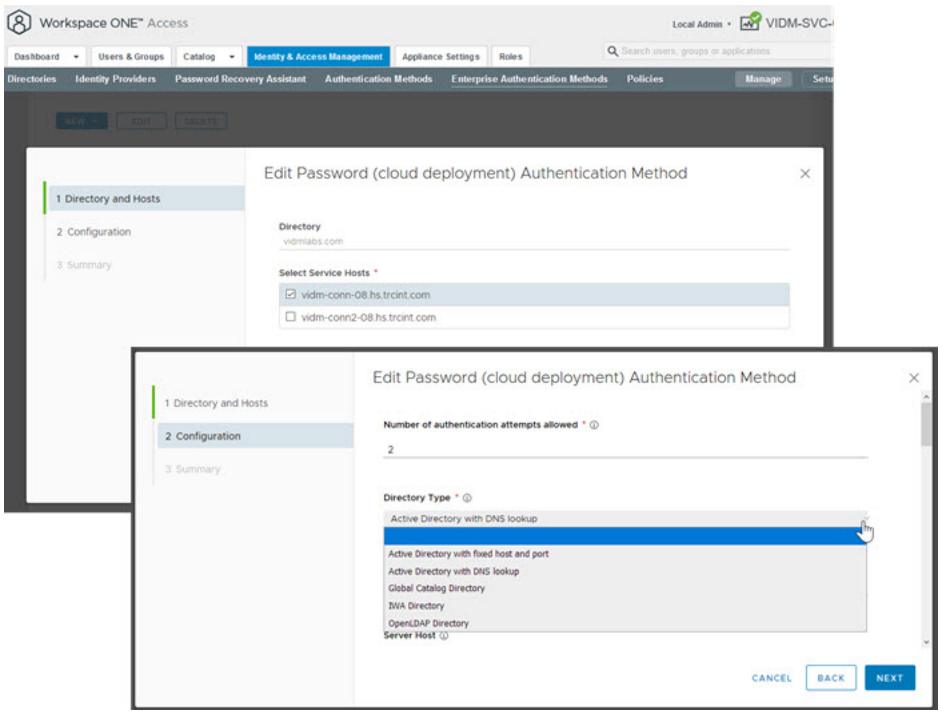


Table 2-1. Directory Types

Directory Sync Type	Select One of These Password Directory Types
Active Directory over LDAP/IWA	■ **Active Directory with fixed host and port**. You created a directory that uses a fixed host and port. ■ **Active Directory with DNS lookup**. You created a directory that uses DNS Service Location lookup. ■ **Global Catalog Directory**. You created a directory that uses the Global Catalog. ■ **IWA Directory**. You created a directory to use Integrated Windows Authentication.
LDAP Directory	**LDAP Directory**. A directory that was created to integrate with your enterprise LDAP directory.

Configure Password (Cloud) Authentication with Your Enterprise Directory

You can configure and edit password (cloud) authentication in the Workspace ONE Access console, Enterprise Authentication page after the Directory Sync service is configured with your Active Directory.

Which text boxes you configure for password (cloud) authentication are based on the directory type you select. The following is a list of the type of directories for password authentication.

- Active Directory with fixed host and port
- Active Directory with DNS lookup
- Global Catalog Directory
- IWA Directory
- LDAP Directory

See the Directory Integrations with Workspace ONE Access guide to learn how directory sync service integrates with your Active Directory.

Prerequisites

- The User Auth service installed as a component of the Workspace ONE Access connector version 20.01. See Installing VMware Workspace ONE Access Connector 20.01.
- The Directory Sync service installed as a component of the Workspace ONE Access connector version 20.01. See Directory Integration with VMware Workspace ONE Access.
- Directories configured in the Workspace ONE Access console Identity & Access Management section.
- User attributes correctly mapped to Active Directory.

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Enterprise Authentication Methods**.

2 Click **NEW** and select **Password (cloud deployment)**.

3 In the Directory and Hosts screen, select the **directory** and the **service host** to configure with password authentication.

4 In the Configuration page, configure the Password (cloud) authentication method.

Directory Type	Option	Action
All types	Number of authentication attempts allowed.	Enter the maximum number of failed login attempts when using password authentication against a directory. The default is 2 attempts.
All types	Directory Type	Select the type of directory that you set up when you installed the Directory Sync service in the connector server.
Active Directory with fixed host and port	Server Port	Select the port used for Active Directory, either 389 or 636 for standard LDAP queries. For global catalog queries, enter either ports 3268 or 3269 .
Active Directory with fixed host and port	Server Host	Select one or more Directory Sync Service instances to use.
All Types	Communication Mode	Basic mode is selected by default. You can change the communication mode. ■ Select SSL, if SSL/TLS is used for communication with the directory. ■ Select STARTTLS, if the DNS service location and SSL are used for communication with the directory. Add the certificates.
All types	Directory Certificate	If the enterprise directory requires access over SSL, copy and paste the enterprise directory server's root CA SSL certificate into the text box. Ensure that the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE lines.
Active Directory with DNS lookup	Use DNS Service Location	Select this box to use the DNS service location records to locate the Active Directory domains. If you do not use DNS service location lookup, deselect the check box and enter the Active Directory server host name and port.
■ Active Directory with fixed host and port ■ Active Directory with DNS lookup ■ IWA Directory ■ LDAP Directory	Base DN	Enter the DN from which to start searches in the directory. For example, cn=users,dc=example,dc=com.

Directory Type	Option	Action
All Types	Bind DN / User Name (IWA)	Enter the user name to use to search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Note** Using a Bind DN user account with a non-expiring password is recommended.
All Types	Bind Password	Enter the Bind DN user password.
■ Active Directory with fixed host and port ■ Active Directory with DNS lookup ■ IWA Directory	Search Attribute	Enter the account attribute that contains the user name. This can be either sAMAcountName, UPN, or Custom.
■ LDAP Directory	Custom Directory Search Attribute for Users	When you enter Custom in the Search Attribute text box, enter the custom search attribute to use to query your LDAP directory to obtain user and group names. For example, **UID**.
■ Active Directory with fixed host and port ■ Active Directory with DNS lookup ■ IWA Directory	Filter query to get AD users	Enter the search filters used to query your enterprise directory. ■ Groups search filter to obtain groups. For example, (objectClass=groupOfNames). ■ Users search filter to obtain users to sync. For example, (&(objectClass=user)(objectCategory=person))
■ Active Directory with fixed host and port ■ Active Directory with DNS lookup ■ IWA Directory ■ Global Catalog Directory	SAML Name-Id Format	Enter the nameIdFormat value that is used to identify the user after authentication. By default, the value is the Directory search UID attribute.
All Types	Change password feature enabled	Enable this feature to allow users to reset their Active Directory passwords from the Workspace ONE Access login page.
All Types	Display domain in login page	Enable this to show the System Domain as an option when users are signing on. If this is disabled and only one domain is available, the domain selection page is not displayed.

5 Click **NEXT** to review the configuration and then click **SAVE**.

Results

What to do next

Add Password (cloud deployment) as an authentication method to the built-in identity provider.

Add the authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the password authentication method to the rule. See Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users .

Configuring RSA SecurID (Cloud) For Workspace ONE Access

When the RSA SecurID authentication method is used, Workspace ONE Access is configured as the authentication agent in the RSA SecurID security console. RSA SecurID authentication requires users to use a token-based authentication system. RSA SecurID is a recommended authentication method for users accessing Workspace ONE Access from outside the enterprise network.

When you configure SecurID to provide additional security, you must ensure that your network is properly configured for your Workspace ONE Access deployment. For SecurID specifically, you must ensure that the appropriate port is open to enable SecurID to authenticate users outside your network.

After you install the Directory Sync service and configured your Active Directory connection, you have the information necessary to prepare the RSA SecurID server. After the SecurID server is prepared, you set up the SecurID authentication method in the Workspace ONE Access console Enterprise Authentication Methods page.

- Prepare the RSA SecurID Server

  To make Workspace ONE Access the authentication agent, the RSA SecurID security console must be configured with the host name and IP address of the Workspace ONE Access connector.

- Configure RSA SecurID Authentication in Workspace ONE Access

  After the Workspace ONE Access connector is configured as the authentication agent in the RSA SecurID server, you set up RSA SecurID in the Workspace ONE Access console.

Prepare the RSA SecurID Server

To make Workspace ONE Access the authentication agent, the RSA SecurID security console must be configured with the host name and IP address of the Workspace ONE Access connector.

Prerequisites

- Verify that one of the following RSA Authentication Manager versions is installed and functioning on the enterprise network: RSA AM 6.1.2, 7.1 SP2 and later, and 8.0 and later. The Workspace ONE Access connector server uses AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), which only supports the preceding versions of RSA Authentication Manager (the RSA SecurID server). For information about installing and configuring RSA Authentication Manager (RSA SecurID server), see RSA documentation.

Procedure

1 On a supported version of the RSA SecurID security console, add the Workspace ONE Access connector host name and IP address as an authentication agent. Enter the following information.

Option	Description
Hostname	The host name of Workspace ONE Access connector.
IP address	The IP address of Workspace ONE Access connector.
Alternate IP address	If traffic from the connector passes through a network address translation (NAT) device to reach the RSA SecurID server, enter the private IP address of the appliance.

2 Download the compressed configuration ZIP file and extract the `sdconf.rec` file.

This file is uploaded when you configure RSA SecurID in the Workspace ONE Access console.

What to do next

Go to the Workspace ONE Access console Identity & Access Management > Setup > Enterprise Authentication Methods page to configure RSA SecurID (cloud deployment).

Configure RSA SecurID Authentication in Workspace ONE Access

After the Workspace ONE Access connector is configured as the authentication agent in the RSA SecurID server, you set up RSA SecurID in the Workspace ONE Access console.

Prerequisites

- Verify that RSA Authentication Manager (the RSA SecurID server) is installed and properly configured.
- Download the ZIP file from the RSA SecurID server and extract the sdconf.rec file.
- The User Auth service installed as a component of the Workspace ONE Access connector version 20.01. See Installing VMware Workspace ONE Access Connector 20.01.

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Enterprise Authentication Methods**.

2 Click **NEW** and select RSA SecurID (cloud deployment).

3 In the Directory and Hosts screen, select the **directory** and the **service host** to configure with this authentication method.

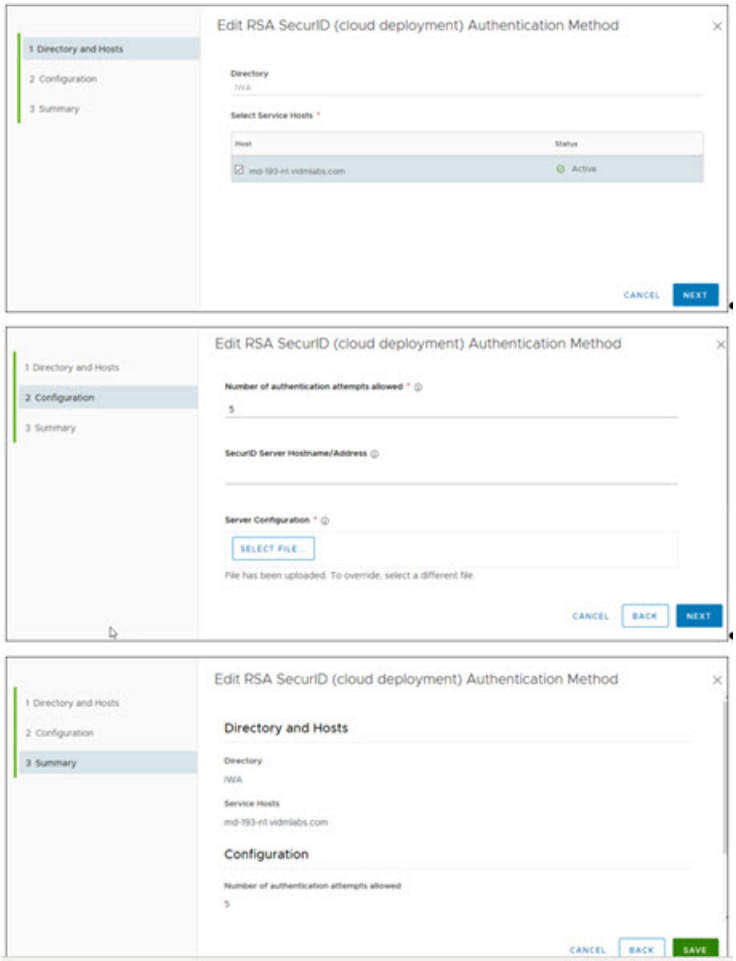
4 In the Configuration page, configure the RSA SecurID authentication method.

Information used and files generated on the RSA SecurID server are required when you configure the SecurID page.

Option	Action
Number of authentication attempts allowed	Enter the maximum number of failed login attempts when using the RSA SecurID token. The default is five attempts. **Note** When more than one directory is configured and you implement RSA SecurID authentication with additional directories, configure **Number of authentication attempts allowed** with the same value for each RSA SecurID configuration. If the value is not the same, SecurID authentication fails.
SecurID Server Hostname/ Address	Enter the hostname or IP address of the SecurID server instance used as the authentication agent to the RSA SecurID server. If your RSA SecurID server has a value assigned to the Alternate IP address prompt, enter that value as the connector IP address. If no alternate IP address is assigned, enter the value assigned to the IP address prompt.
Server Configuration	Upload the RSA SecurID server configuration file named `sdconf.rec`.

5 Click **NEXT** to review the configuration and then click **SAVE**.

Figure 2-2. Configure RSA SecurID Authentication



What to do next

Add the RSA SecurID as an authentication method to the built-in identity provider.

Add the authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the SecurID authentication method to the rule. See Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users .

Configuring RADIUS for Workspace ONE Access

You can configure Workspace ONE Access so that users are required to use RADIUS (Remote Authentication Dial-In User Service) authentication when they log in to Workspace ONE.

Because RADIUS two-factor authentication solutions work with authentication managers installed on separate servers, the RADIUS server must be configured and accessible to the Workspace ONE Access service.

When users sign in to their Workspace ONE portal and RADIUS authentication is enabled, the login dialog box requests that users enter their RADIUS authentication user name and passcode. If the RADIUS server issues an access challenge, the Workspace ONE Access service displays a dialog box prompting for a second passcode.

After a user enters credentials in the dialog box, the RADIUS server can send an SMS message or email, or text using some other out-of-band mechanism to the user's cell phone. The user enters the one-time passcode into the login dialog box to complete the authentication. Currently support for RADIUS challenges is limited to prompting for text input.

If the RADIUS server provides the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.

Prepare the RADIUS Server

Set up the RADIUS server and then configure the RADIUS server to accept RADIUS requests from the Workspace ONE Access service.

Refer to your RADIUS vendor's setup guides for information about setting up the RADIUS server. Note your RADIUS configuration information as you use this information when you configure RADIUS in the service. To see the type of RADIUS information required to configure Workspace ONE Access go to Configure RADIUS Authentication in Workspace ONE Access.

You can set up a secondary RADIUS authentication server to be used for high availability. If the primary RADIUS server does not respond within the server timeout configured for RADIUS authentication, the request is routed to the secondary server.

Configure RADIUS Authentication in Workspace ONE Access

You enable the RADIUS authentication method and configure the RADIUS settings in the Workspace ONE Access console.

Prerequisites

Install and configure the RADIUS software on an authentication manager server. For RADIUS authentication, follow the vendor's configuration documentation.

The following RADIUS server information is required to configure RADIUS on the Workspace ONE Access service.

- IP address or DNS name of the RADIUS server.
- Authentication port numbers. Authentication port is usually 1812.
- Authentication type. The authentication types include PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 and 2).
- RADIUS shared secret that is used for encryption and decryption in RADIUS protocol messages.
- Specific timeout and retry values needed for RADIUS authentication

The User Auth service installed as a component of the Workspace ONE Access connector version 20.01. See Installing VMware Workspace ONE Access Connector 20.01.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Enterprise Authentication Methods**.
2. Click **NEW** and select RADUS (cloud deployment).
3. Select the directory and the service host to configure with this authentication method.
4. Configure the RADIUS authentication method.

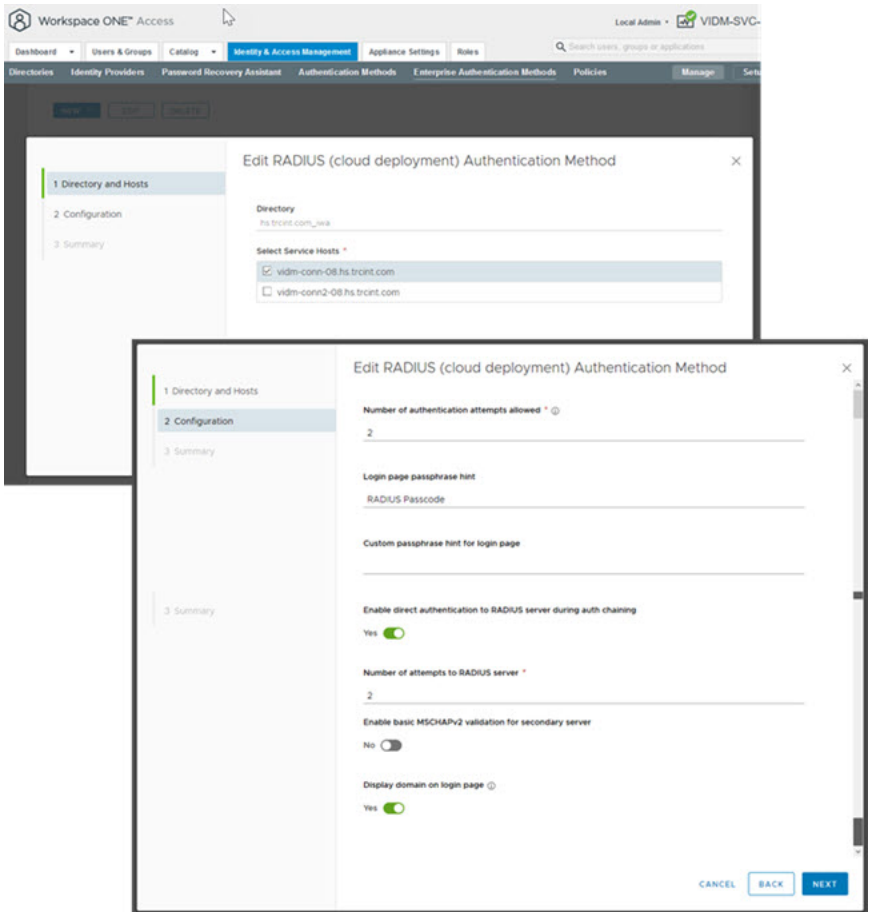
Option	Action
Number of authentication attempts allowed	Enter the maximum number of failed login attempts when using RADIUS to log in. The default is five attempts.
Login page passphrase hint	Enter the text string to display as the message on the user login page to direct users to enter the correct RADIUS passcode. For example, if this text box is configured with **AD password first and then SMS passcode**, the login page message reads **Enter your AD password first and then SMS passcode.**. The default text string is **RADIUS Passcode**.
Enable direct authentication to Radius server	Select this box to enable direct user authentication. When this is enabled, users are not required to reenter their credentials. To use direct authentication to the RADIUS server, the user name must be configured the same way on both the RADIUS server and in Active Directory. Note that a user name **JSmith** in Active Directory does not match **jsmith** in the RADIUS server.
Number of attempts to RADIUS server	Enter the total number of retry attempts. If the primary server does not respond, the service waits for the configured time before retrying again.

Option	Action
Server timeout in seconds	Enter the RADIUS server timeout in seconds, after which a retry is sent if the RADIUS server does not respond.
RADIUS Server Hostname/ Address	(Optional) Enter the host name or the IP address of the RADIUS server.
Authentication port	Enter the RADIUS authentication port number. The port is usually 1812.
Accounting port	Enter 0 for the port number. The accounting port is not used currently.
Authentication type	Enter the authentication protocol that is supported by the RADIUS server. Either PAP, CHAP, MSCHAP1, OR MSCHAP2.
Shared secret	Enter the shared secret that is used between the RADIUS server and the Workspace ONE Access service.
Realm prefix	(Optional) The user account location is called the realm. Enter the realm prefix to use. If you enter a realm prefix string, the string is placed at the beginning of the user name when the name is sent to the RADIUS server. For example, if the user name is entered as jdoe and the realm prefix DOMAIN-A\ is specified, the user name DOMAIN-A\jdoe is sent to the RADIUS server. If you do not configure the Realm text boxes, only the user name that is entered is sent.
Realm suffix	(Optional) If you specify a realm suffix, the string is placed at the end of the user name. For example, if the suffix is @myco.com, the user name jdoe@myco.com is sent to the RADIUS server.

5 You can enable a secondary RADIUS server for high availability.

Configure the secondary server as described in step 4.

6 Click **NEXT** to review the configuration and then click **SAVE**.



What to do next

Add RADIUS as an authentication method to the built-in identity provider configuration page.

Add the RADIUS authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the RADIUS authentication method to the rule. See Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users .

For high availability, associate this RADIUS authentication method to other registered Workspace ONE Access connectors where the enterprise service User Auth is installed.

Enable User Auth Service Debug Logs In Workspace ONE Access Connector

You can set the log level to DEBUG for the User Auth service on the Workspace ONE Access connector to help you debug problems.

Do not make entries under the <Loggers> tag. This tag contains <Root> and <AppenderRef> tags such as `<Root level="INFO">` and `<AppenderRef ref="syslog"/>`.

Procedure

1 On the windows server on which Workspace ONE Access connector is installed, go to the \VMware\Workspace ONE Access\User Auth Service\conf directory.

2 To update the log level in the log4j2-override.xml file in the installation directory, select the module to be debugged and modify the request as `<Logger name="com.vmware.vidm.eas.adapters.[modulename]" level="DEBUG"/>`.

SI Number	Module to be Debugged	Logger Modification
1	Adapters Common	`<Logger name="com.vmware.vidm.eas.adapters.common" level="DEBUG"/>`
2	Auth-Adapter: Password	`<Logger name="com.vmware.vidm.eas.adapters" level="DEBUG"/>`
3	Auth-Adapter: Radius	`<Logger name="com.vmware.vidm.eas.adapters.radius" level="DEBUG"/>`
4	Auth-Adapter: Secur-id	`<Logger name="com.vmware.vidm.eas.adapters.securid" level="DEBUG"/>`
5	Comm-Channel-Client (MessgeProcessorV2)	`<Logger name="com.vmware.vidm.enterprise.sockjs.v2.client" level="DEBUG"/>`
6	Comm-Channel-Client (setup) Note this requires a restart.	`<Logger name="com.vmware.vidm.enterprise.comm.channel.SockJS Service" level="DEBUG"/>`

Comm-Channel Client (MessageProcessorV2) handles all the request received by the User Auth Service Use the logger if debugging a particular request is required.

Comm-Channel-Client (setup) is used when the User Auth service starts up. Use this logger if Comm-Channel is not starting up or unexpected behavior is noticed. For example, if the Message Size capacity is expected to be something else.

Configuring Kerberos Authentication In Workspace ONE Access 3

Kerberos authentication provides users who are successfully signed in to their Active Directory domain access to their apps portal without additional credential prompts. You enable the Kerberos authentication method for secure interactions between users' browsers and the Workspace ONE Access service.

Kerberos authentication can be configured for Active Directory over LDAP or Active Directory (Integrated Windows Authentication).

The Kerberos auth service installed on the connector requires Workspace ONE Access inbound connectivity. See Prerequisites for Installing the Workspace ONE Access Connector.

- Configure and Enable Kerberos Authentication in Workspace ONE Access

  When the Kerberos Auth service is installed on a Workspace ONE Access connector, you enable and configure the Kerberos authentication method from the Workspace ONE Access console. You then add the Workspace ONE Access identity provider and associate the Kerberos authentication method in the identity provider.

- Configuring your Browser for Kerberos

  When Kerberos is enabled, you need to configure the Web browsers to send your Kerberos credentials to the service when users sign in.

- Kerberos Initialization Error in Workspace ONE Access

  After the Kerberos Auth service is installed on the Workspace ONE Access connector, you get an error that states that Kerberos initialization failed.

Configure and Enable Kerberos Authentication in Workspace ONE Access

When the Kerberos Auth service is installed on a Workspace ONE Access connector, you enable and configure the Kerberos authentication method from the Workspace ONE Access console. You then add the Workspace ONE Access identity provider and associate the Kerberos authentication method in the identity provider.

Prerequisites

The Kerberos Auth services must be correctly configured in the Workspace ONE Access connector. A correct configuration includes the following.

- The Windows machine on which the Kerberos Auth service is installed must be joined to the domain.
- During the installation of the Kerberos Auth service, you specified the domain user account to use to run the service. This domain user is part of the administrator group on the Windows machine on which the service is installed.
- A trusted SSL certificate signed by a public or internal CA was uploaded. If you deployed multiple instances of the Kerberos Auth service for high availability, a trusted SSL certificate signed by a public or internal CA was uploaded to each connector.
- To set up high availability for Kerberos authentication, a load balance is required. The load balance must have a trusted SSL certificate signed by a public or internal CA. See the Installing the Workspace ONE Access Connector guide for configuration information.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Enterprise Authentication Methods**.
2. Click **NEW** and select Kerberos.
3. Select the directory and the service host to configure with this authentication method.
4. Configure the Kerberos authentication method.

Option	Description
Directory UID Attribute	Enter the account attribute that contains the user name.
Enable Redirect	**Enable Redirect** displays if redirect is enabled because you are deploying multiple connectors configured with the Kerberos Auth service for high availability with a load balancer.

5. Click **NEXT** to review the configuration and then click **SAVE**.

What to do next

In the Identity Provider page, add the Workspace ONE Access identity provider and associated the Kerberos Authentication method to the identity provider. See Configure Workspace ONE Access Identity Provider Instance with Kerberos Authentication.

Add the authentication method to the default access policy. Go to the Identity & Access Management > Manage > Policies page and edit the default policy rules to add the Kerberos authentication method to the rule in the correct authentication order, with Password authentication (cloud) configured as the fallback authentication method. See Managing Access Policies.

If high availability is configured, on each connector, configure the Kerberos authentication method for the Kerberos Authentication service.

Configuring your Browser for Kerberos

When Kerberos is enabled, you need to configure the Web browsers to send your Kerberos credentials to the service when users sign in.

The following Web browsers can be configured to send your Kerberos credentials to the Workspace ONE Access service on computers running Windows: Firefox, Internet Explorer, and Chrome. All the browsers require additional configuration.

Configure Internet Explorer to Access the Web Interface

You must configure the Internet Explorer browser if Kerberos is configured for your deployment and if you want to grant users access to the Web interface using Internet Explorer.

Kerberos authentication works in conjunction with Workspace ONE Access on Windows operating systems.

Note Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

Configure the Internet Explorer browser for each user or provide users with the instructions after you configure Kerberos.

Procedure

1. Verify that you are logged into Windows as a user in the domain.
2. In Internet Explorer, enable automatic log in.
   a. Select **Tools > Internet Options > Security**.
   b. Click **Custom level**.
   c. Select **Automatic login only in Intranet zone**.
   d. Click **OK.**
3. Verify that this instance of the connector virtual appliance is part of the local intranet zone.
   a. Use Internet Explorer to access the Workspace ONE Access sign in URL at *https://myconnectorhost.domain/authenticate/*.
   b. Locate the zone in the bottom right corner on the status bar of the browser window.

      If the zone is Local intranet, Internet Explorer configuration is complete.

4 If the zone is not Local intranet, add the Workspace ONE Access connector sign in URL to the intranet zone.

   a Select **Tools > Internet Options > Security > Local intranet > Sites.**

   b Select **Automatically detect intranet network**.

   If this option was not selected, selecting it might be sufficient for adding the connector to the intranet zone.

   c (Optional) If you selected **Automatically detect intranet network**, click **OK** until all dialog boxes are closed.

   d In the Local Intranet dialog box, click **Advanced.**

   A second dialog box named Local intranet appears.

   e Enter the Workspace ONE Access connector URL in the **Add this Web site to the zone** text box.

   https://myconnectorhost.domain/authenticate/

   f Click **Add > Close > OK**.

5 Verify that Internet Explorer is allowed to pass the Windows authentication to the trusted site.

   a In the Internet Options dialog box, click the **Advanced** tab.

   b Select **Enable Integrated Windows Authentication**.

   This option takes effect only after you restart Internet Explorer.

   c Click **OK**.

6 Log in to the Web interface to check access.

   If Kerberos authentication is successful, the test URL goes to the Web interface.

Results

The Kerberos protocol secures all interactions between this Internet Explorer browser instance and Workspace ONE Access. Now, users can use single sign-on to access their Workspace ONE portal.

Configure Firefox to Access the Web Interface

You must configure the Firefox browser if Kerberos is configured for your Workspace ONE Access deployment and you want to grant users access to the web interface using Firefox.

Kerberos authentication works in conjunction with Workspace ONE Access on Windows operating systems.

Prerequisites

Configure the Firefox browser, for each user, or provide users with the instructions, after you configure Kerberos.

Procedure

1. In the URL text box of the Firefox browser, enter `about:config` to access the advanced settings.
2. Click **Accept the Risk and Continue**.
3. Double-click **network.negotiate-auth.trusted-uris** in the Preference Name column.
4. Enter your Workspace ONE Access connector URL in the text box.

   https://myconnectorhost.domain.com

   If you are using multiple connectors for Kerberos authentication, add a comma separated list of connectors.
5. Click **OK.**
6. Test Kerberos functionality by using the Firefox browser to log in to connector login URL. For example, https://myconnectorhost.domain.com.

   If the Kerberos authentication is successful, the test URL goes to the Web interface.

Results

The Kerberos protocol secures all interactions between this Firefox browser instance and Workspace ONE Access. Now, users can use single sign-on access their Workspace ONE portal.

Configure the Chrome Browser to Access the Web Interface

You must configure the Chrome browser if Kerberos is configured for your deployment and if you want to grant users access to the Web interface using the Chrome browser.

Kerberos authentication works in conjunction with Workspace ONE Access on Windows operating systems.

Note Do not implement these Kerberos-related steps on other operating systems.

Prerequisites

- Configure Kerberos.
- Since Chrome uses the Internet Explorer configuration to enable Kerberos authentication, you must configure Internet Explorer to allow Chrome to use the Internet Explorer configuration. See Google documentation for information about how to configure Chrome for Kerberos authentication.

Procedure

1. Test Kerberos functionality by using the Chrome browser.
2. Log in to Workspace ONE Access connector at *https://myconnectorhost.domain.com/authenticate/*.

   If Kerberos authentication is successful, the test URL connects with the Web interface.

Results

If all related Kerberos configurations are correct, the relative protocol (Kerberos) secures all interactions between this Chrome browser instance and Workspace ONE Access. Users can use single sign-on access their Workspace ONE portal.

Kerberos Initialization Error in Workspace ONE Access

After the Kerberos Auth service is installed on the Workspace ONE Access connector, you get an error that states that Kerberos initialization failed.

Problem

During the installation of the Kerberos Auth service in the Workspace ONE Access connector, if you did not select the **Would you like to run the Workspace ONE Access Services as a domain user account?** option or if you selected the option but specified a domain account that does not have the right to "Create, delete, and manage user accounts" in Active Directory, Kerberos cannot be initialized after installation. When you try to configure the Kerberos authentication adapter, you get an error message that states that Kerberos initialization failed.

Solution

Run the `setupkerberos.bat` script with a user account that has higher privileges. Use an account that:

- Is a domain user
- Has the right to "Create, delete, and manage user accounts" in Active Directory (members of Admin Users and Account Operators groups have those rights)
- Is part of the administrator group on the Windows server on which the Workspace ONE Access connector is installed

This user account with higher privileges is only required temporarily to run the script and is not stored or used again for connector services. After you run the script, you can continue configuring the Kerberos authentication method with the original user account that you were using.

To run the script:

1 Log in to the connector Windows machine and navigate to the `InstallDir\Workspace_ONE_Access\Support\scripts` directory.

2 Right click `setupkerberos.bat` and select **Run as administrator**.

3 Enter the user account with higher privileges described above.

A confirmation message appears after the script has run successfully.

4 Log in to the Workspace ONE Access console with the original user account that you were using and configure the Kerberos authentication method.

About the setupkerberos.bat Script

When Kerberos auth is installed on the Workspace ONE Access connector, 20.01 or later, the `setupkerberos.bat` script performs the following tasks:

1 Creates a service account with the same name as the machine account (without the `$`)

2 Sets a random password for the account

3 Generates a keytab file for the account, by default stored in `InstallDir\Workspace ONE Access\Kerberos Auth Service\conf`.

For Workspace ONE Access connector 19.03, the keytab file for the account is stored in `/usr/horizon/conf`.

4 Maps the given principal of the machine as an SPN inside the account

Associate Workspace ONE Access Authentication Methods In Built-In Identity Providers

4

The Workspace ONE Access service provides cloud-based authentication methods that you enable and configure from the console. After an authentication method is configured, you associate it to a built-in identity provider.

These cloud-based authentication methods do not require a connector.

- Workspace ONE UEM External Access Token
- Device Compliance with Workspace ONE UEM
- Certificate Cloud Deployment
- Password with Workspace ONE UEM
- VMware Verify for two-factor authentication
- Mobile SSO for iOS
- Mobile SSO for Android
- Password Local Directory

After you enable the authentication methods, you create access policies to apply to these authentication methods.

This chapter includes the following topics:

Managing Configuration of Password Authentication with Workspace ONE UEM

Password Authentication with Workspace ONE UEM authenticates using AirWatch Cloud Connector through the Workspace ONE UEM service. You enable this User Password Authentication through Workspace ONE UEM in the Identity & Access Management > Workspace ONE UEM page in the Workspace ONE Access console.

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

The Password (with Workspace ONE UEM) authentication method can be viewed and managed from the Identity & Access Management > Authentication Methods page and is associated to the built-in identity provider in the Identity Providers page.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Authentication Methods**.
2. In the **Password (with Workspace ONE UEM)** Configure column, click the pencil icon.
3. Review the configuration.

Option	Description
Enable Workspace ONE UEM Password Authentication	This check box enables Workspace ONE UEM password authentication.
Workspace ONE UEM Admin Console URL	Pre-populated with the Workspace ONE UEM URL.
Workspace ONE UEM API Key	Pre-populated with the Workspace ONE UEM Admin API key.
Certificate Used for Authentication	Pre-populated with the AirWatch Cloud Connector certificate.
Password for Certificate	Pre-populated with the password for the AirWatch Cloud Connector certificate.
Workspace ONE UEM Group ID	Pre-populated with the organization group ID.
Number of authentication attempts allowed	The maximum number of failed login attempts when using the Workspace ONE UEM password for authentication. No more login attempts are allowed after the failed log ins reach this number. The Workspace ONE Access 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 Workspace ONE Access service dynamically when they log in the first time.

4 Click **Save**.

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

Enabling Compliance Checking for Workspace ONE UEM Managed Devices

When users enroll their devices, samples containing data used to evaluate compliance are sent on a scheduled basis. The evaluation of this sample data ensures that the device meets the compliance rules set by the administrator in the Workspace ONE UEM console. If the device goes out of compliance, corresponding actions configured in the UEM console are taken.

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

The Workspace ONE Intelligent Hub app automatically signs out and blocks access to the applications if the device is compromised. If the device was enrolled through adaptive management, an enterprise wipe command issued through the UEM console unenrolls the device and removes the managed applications from the device. Unmanaged applications are not removed.

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

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

Enable Compliance Checking

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

When Device Compliance is configured, the access policy rules can be configured to check the Workspace ONE UEM server for device compliance status when users sign in from their devices. See Enabling Compliance Checking for Workspace ONE UEM Managed Devices.

Procedure

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

2 In the Device Compliance Check section, select **Enable** and click **Save**.

3 In the Identity & Access Management tab, go to **Manage > Authentication Methods**.

4 In the **Device Compliance (with Workspace ONE UEM)** Configure column, click the pencil icon.

5 Enable Device Compliance authentication and set the maximum number of failed login attempts. The other text boxes are pre-populated with the configured Workspace ONE UEM values.

Option	Description
Enable Device Compliance Adapter	Select this check box to enable Workspace ON UEM password authentication.
Workspace ONE UEM Admin Console URL	Pre-populated with the Workspace ONE UEM URL that you set up on the AirWatch configuration page.
Workspace ONE UEM API Key	Pre-populated with the Workspace ONE UEM Admin API key.
Certificate Used for Authentication	Pre-populated with the AirWatch Cloud Connector certificate
Password for Certificate	Pre-populated with the password for the AirWatch Cloud Connector certificate.

6 Click **Save**.

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

What to do next

Associate the Device Compliance authentication method in the built-in identity provider. See Chapter 5 Managing Authentication Methods in the Workspace ONE Access Identity Providers .

Configure the default access policy to create rules to use device compliance with Workspace ONE UEM. See Configure Compliance Checking Rules.

Configure Compliance Checking Rules

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

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

Prerequisites

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

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

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.

2 Click **Edit Default Policy**.

3 Click **Next**.

4 Click **Add Policy Rule** to add a rule, or select a rule to edit.

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

5 Click **Save**.

Configuring VMware Verify for Two-Factor Authentication

In the Workspace ONE Access console, you can enable the VMware Verify service as the second authentication method when two-factor authentication is required.

For Workspace ONE Access tenant deployments, you enable VMware Verify in the Built-in identity provider in the Workspace ONE Access console.

For Workspace ONE Access on-premises deployments, you enable VMware Verify in the Built-in identity provider in the Workspace ONE Access console and add the VMware Verify security token you receive from VMware support.

You configure two-factor authentication in the access policy rules to require users to authenticate using two authentication methods.

Users install the VMware Verify application on their devices and provide a phone number to register their device with the VMware Verify service. The device and phone number are also registered in the User & Groups user profile in the Workspace ONE Access console.

Users enroll their account once when they sign in using password authentication first and then enter the VMware Verify passcode that displays on their device. After the initial authentication, users can authenticate through one of these three methods.

- Push approval with OneTouch notification. Users approve or deny access from Workspace ONE Access with one click. Users click either Approve or Deny on the message that is sent.
- Time-based One Time Password (TOTP) passcode. A one-time passcode is generated every 20 seconds. Users enter this passcode on the sign-in screen.
- Text message. Phone SMS is used to send a one-time verification code in a text message to the registered phone number. Users enter this verification code on the sign-in screen.

VMware Verify uses a third-party cloud service to deliver this feature to user devices. To do so, user information such as name, email, and phone number are stored in the service but not used for any purpose other than to deliver the feature.

Enable VMware Verify

For two-factor authentication with the VMware Verify service, enable VMware Verify and then add it as an authentication method in a built-in identity provider.

Prerequisites

For on-premises deployments, to enable two-factor authentication with the VMware Verify service, you must add a security token to the VMware Verify page and then enable VMware Verify in the Built-in Identity provider. Create a support ticket with the VMware support group to receive the security token that enables VMware Verify. The Support team staff processes your request and updates the support ticket with instructions and a security token.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, go to **Manage > Auth Methods**.
2. In the **VMware Verify** Configure column, click the icon.
3. (On premises deployments) Paste the security token you received into the Security Token text box.
4. Select the check box **Enable VMware Verify**.
5. Click **Save**.

What to do next

Enable VMware Verify as an authentication method in a built-in identity provider. See Configure a Built-in Identity Provider in Workspace ONE Access.

Create an access policy rule in the default access polity to add the VMware Verify authentication method as the second authentication method in the rule.

(Optional) Customize the logo and icon that displays in the VMware Verify application on the devices. Apply custom branding to the VMware Verify sign-in page. See the Workspace ONE Access Administration guide.

Registering End Users with VMware Verify

When VMware Verify authentication is required for two-factor authentication, users install and use the VMware Verify app to register their device.

Note The VMware Verify application can be downloaded from the app stores.

When VMware Verify two-factor authentication is enabled, the first time users sign in to the Workspace ONE app, users are asked to enter their user name and password. When the user name and password are verified, users are prompted to enter their device phone number to enroll in VMware Verify.

When they click Enroll, the device phone number is registered with VMware Verify, and if they have not downloaded the application, they are asked to download the VMware Verify application.

When the application is installed, users are asked to enter the same phone number that was entered before and to select a notification method to receive a one-time registration code. The registration code is entered on the registration pin page.

After the device phone number is registered, users can use a time-based one-time passcode displayed in the VMware Verify application to sign in to Workspace ONE. The passcode is a unique number that is generated on the device and is constantly changing.

Users can register more than one device. The VMware Verify passcode is automatically synchronized to each of the registered devices.

Remove VMware Verify Registered Phone Number from User Profile

To troubleshoot problems with signing in to Workspace ONE, you can remove the user phone number in the user profile in the Workspace ONE Access console.

Procedure

1. In the Workspace ONE Access console, click **Users & Groups**.
2. On the User page, select the user name to reset.
3. In the VMware Verify tab, click **Reset VMware Verify**.

Results

The phone number is removed from the user profile and the User list shows N/A in the VMware Verify Phone number column. The phone number is unregistered from the VMware Verify service. When the user signs in to their Workspace ONE app, they are asked to enter the phone number to enroll in the VMware Verify service again.

VMware Verify Firewall IP Address List

For VMware Verify authentication, add the IP addresses to the access control allow list on your firewall. VMware Verify must be able to reach all the IP addresses over port 443.

The IP addresses to the allow list can be looked up on `vmware.authy.com` and `api.authy.com`.

Use the **nslookup** command or another command-line tool to obtain the IP addresses to add to your external firewall allow list.

Configuring a Certificate for Use with Workspace ONE Access

You can configure x509 certificate authentication to allow clients to authenticate with certificates on their desktop and mobile devices or to use a smart card adapter for authentication. Certificate-based authentication is based on what the user has (the private key or smart card), and what the person knows (the password to the private key or the smart-card PIN.) An X.509 certificate uses the public key infrastructure (PKI) standard to verify that a public key contained within the certificate belongs to the user. With smart card authentication, users connect the smart card with the computer and enter a PIN.

The smart card certificates are copied to the local certificate store on the user's computer. The certificates in the local certificate store are available to all the browsers running on this user's computer, with some exceptions, and therefore, are available to a Workspace ONE Access instance in the browser.

Note When Certificate Authentication is configured and the service appliance is set up behind a load balancer, make sure that the connector Windows server is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the server and the client to pass the certificate to the connector. You can configure additional connectors behind another load balancer configured with SSL pass-through and enable and configure certificate-based authentication on those connectors.

Using User Principal Name for Certificate Authentication

You can use certificate mapping in Active Directory. Certificate and smart card log ins uses the user principal name (UPN) from Active Directory to validate user accounts. The Active Directory accounts of users attempting to authenticate in the Workspace ONE Access service must have a valid UPN that corresponds to the UPN in the certificate.

You can configure the Workspace ONE Access service to use an email address to validate the user account if the UPN does not exist in the certificate.

You can also enable an alternate UPN type to be used.

Certificate Authority Required for Authentication

To enable logging in using certificate authentication, root certificates and intermediate certificates must be uploaded to the Workspace ONE Access connector.

The certificates are copied to the local certificate store on the user's computer. The certificates in the local certificate store are available to all the browsers running on this user's computer, with some exceptions, and therefore, are available to a Workspace ONE Access instance in the browser.

For smart-card authentication, when a user initiates a connection to the Workspace ONE Access instance, the Workspace ONE Access service sends a list of trusted certificate authorities (CA) to the browser. The browser checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user to enter a smart card PIN. If multiple valid user certificates are available, the browser prompts the user to select a certificate.

If a user cannot authenticate, the root CA and intermediate CA might not be set up correctly, or the service has not been restarted after the root and intermediate CAs were uploaded to the server. In these cases, the browser cannot show the installed certificates, the user cannot select the correct certificate, and certificate authentication fails.

Using Certificate Revocation Checking

You can configure certificate revocation checking to prevent users who have their user certificates revoked from authenticating. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

Certificate revocation checking with certificate revocation lists (CRLs) and with the Online Certificate Status Protocol (OCSP) is supported. A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of a certificate.

You can configure both CRL and OCSP in the same certificate authentication adapter configuration. When you configure both types of certificate revocation checking and the Use CRL in case of OCSP failure check box is enabled, OCSP is checked first and if OCSP fails, revocation checking falls back to CRL. Revocation checking does not fall back to OCSP if CRL fails.

Logging in with CRL Checking

When you enable certificate revocation, the Workspace ONE Access server reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked, authentication through the certificate fails.

Logging in with OCSP Certificate Checking

The Online Certificate Status Protocol (OCSP) is an alternative to certificate revocation lists (CRL) that is used to perform a certificate revocation check.

When you configure certificate-based authentication, when Enable Cert Revocation and Enable OCSP Revocation are both enabled, Workspace ONE Access validates the entire certificate chain, including the primary, intermediate and root certificates. The revocation check fails if the check of any certificate in the chain fails or the call to the OCSP URL fails.

The OCSP URL can either be configured manually in the text box or extracted from the Authority Information Access (AIA) extension of the certificate that is being validated.

The OCSP option that you select when you configure certificate authentication determines how Workspace ONE Access uses the OCSP URL.

- **Configuration Only**. Perform certificate revocation check using the OCSP URL provided in the text box to validate the entire certificate chain. Ignore the information in the certificate's AIA extension. The OCSP URL text box must also be configured with the OCSP server address for revocation checking.
- **Certificate Only (required)**. Perform certificate revocation check using the OCSP URL that exists in the AIA extension of each certificate in the chain. The setting in the OCSP URL text box is ignored. Every certificate in the chain must have an OCSP URL defined, otherwise the certificate revocation check fails.
- **Certificate Only (Optional)**. Only perform certificate revocation check using the OCSP URL that exists in the AIA extension of the certificate. Do not check revocation if the OCSP URL does not exist in the certificate AIA extension. The setting in the OCSP URL text box is ignored. This configuration is useful when revocation check is desired, but some intermediate or root certificates do not contain the OCSP URL in the AIA extension.
- **Certificate with fallback to configuration**. Perform certificate revocation check using the OCSP URL extracted from the AIA extension of each certificate in the chain, when the OCSP URL is available. If the OCSP URL is not in the AIA extension, check revocation using the OCSP URL configured in the OCSP URL text box. The OCSP URL text box must be configured with the OCSP server address.

Configure Certificate-Based Authentication

You configure the Certificate (Cloud Deployment) authentication method from the Authentication Methods page in the Workspace ONE Access console, and then you select the authentication method to use in the built-in identity provider.

Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- (Optional) List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.

- Consent form content, if a consent form displays before authentication.

Procedure

1. In the Identity & Access Management tab, go to **Manage > Authentication Methods**.
2. In the **Certificate (Cloud deployment)** Configure column, click the pencil icon.
3. Enable Device Compliance authentication and set the maximum number of failed login attempts. The other text boxes are pre-populated with the configured Workspace ONE UEM values.
4. Configure the Certificate Service Auth Adapter page.

Option	Description
Enable Certificate Adapter	Select the check box to enable certificate authentication.
***Root and intermediate CA certificates**	Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded as DER or PEM.
Uploaded CA Certificates	The uploaded certificate files are listed in the Uploaded CA Certificates section of the form.
User Identifier Search Order	Select the search order to locate the user identifier within the certificate. ■ **upn**. The UserPrincipalName value of the Subject Alternative Name ■ **email**. The email address from the Subject Alternative Name. ■ **subject**. The UID value from the Subject. If the UID is not found in the subject DN, the UID value in the CN text box is used, if the CN text box is configured.
Validate UPN Format	Enable this check box to validate the format of the UserPrincipalName text box.
Request Timeout	Enter the time in seconds to wait for a response. A value of zero (0) means that the wait for the response is indefinite.
Certificate Policies Accepted	Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID numbers (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs.
Enable Cert Revocation	Select the check box to enable certificate revocation checking. Revocation checking prevents users who have revoked user certificates from authenticating.
Use CRL from Certificates	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate the status of a certificate, revoked or not revoked.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL.
Enable OCSP Revocation	Select the check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP failure	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.

Option	Description
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.
OCSP URL Source	Select the source to use for revocation checking. ■ **Configuration Only**. Perform certificate revocation check using the OCSP URL provided in the text box to validate the entire certificate chain. ■ **Certificate Only (required)**. Perform certificate revocation check using the OCSP URL that exists in the AIA extension of each certificate in the chain. Every certificate in the chain must have an OCSP URL defined, other wise the certificate revocation check fails. ■ **Certificate Only (Optional)**. Only perform certificate revocation check using the OCSP URL that exists in the AIA extension of the certificate. Do not check revocation if the OCSP URL does not exist in the certificate AIA extension. ■ **Certificate with fallback to configuration**. Perform certificate revocation check using the OCSP URL extracted from the AIA extension of each certificate in the chain, when the OCSP URL is available. If the OCSP URL is not in the AIA extension, check revocation using the OCSP URL configured in the OCSP URL text box. The OCSP URL text box must be configured with the OCSP server address.
OCSP Responder's Signing Certificate	Enter the path to the OCSP certificate for the responder, */path/to/file.cer*.
Upload OCSP Signing Certificates	The uploaded certificate files are listed in this section.
Enable Consent Form before Authentication	Select this check box to include a consent form page to appear before users log in to their Workspace ONE portal using certificate authentication.
Consent Form Content	Type the text that displays in the consent form in this text box.

5 Click **Save**.

What to do next

- Associate the Certificate (Cloud Deployment) authentication method in the built-in identity provider. See Configure a Built-in Identity Provider in Workspace ONE Access.
- Add the certificate authentication method to the default access policy. See Managing Access Policies.
- (On Premises deployments) When Certificate Authentication is configured, and the service appliance is set up behind a load balancer, make sure that the Workspace ONE Access connector is configured with SSL pass-through at the load balancer and not configured to terminate SSL at the load balancer. This configuration ensures that the SSL handshake is between the connector and the client to pass the certificate to the connector.

Configuring Mobile SSO for iOS Authentication in Workspace ONE Access

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

Using the Cloud-Hosted KDC Service

To support using Kerberos authentication for Mobile SSO for iOS, Workspace ONE Access provides a cloud hosted KDC service.

The KDC service hosted in the cloud must be used when the Workspace ONE Access service deployed with Workspace ONE UEM in a Windows environment. The KDC service hosted in the cloud can also be used in a Workspace ONE Access cloud-hosted deployment.

When you configure Mobile SSO for iOS authentication, you configure the realm name for the cloud hosted KDC service. The realm is the name of the administrative entity that maintains authentication data. When you click **Save**, the Workspace ONE Access service is registered with the cloud hosted KDC service. The data that is stored in the KDC service is based on your configuration of the Mobile SSO for iOS authentication method. The data includes the CA certificate, the OCSP signing certificate, and the OCSP request configuration details.

The logging records are stored in the cloud service. The Personally Identifiable Information (PII) in the logging records includes the following.

- The Kerberos principal name from the user's profile
- The subject DN, UPN, and email SAN values
- The device ID from the user's certificate
- The FQDN of the IDM service that the user is accessing

To use the cloud hosted KDC service, Workspace ONE Access must be configured as follows.

- The FQDN of the Workspace ONE Access service must be reachable from the Internet. The SSL/TLS certificate used by Workspace ONE Access must be publicly signed.

  If you configure Workspace ONE Access with an external firewall, allow list the appropriate IP addresses or URLs .

- An outbound request/response port 88 (UDP) and port 443 (HTTPS/TCP) must be accessible from the service.
- If you enable OCSP, the OCSP responder must be reachable from the Internet.

Configure Mobile SSO for iOS Authentication in Workspace ONE Access

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

Prerequisites

- Certificate authority PEM or DER file used to issue certificates to users in the Workspace ONE UEM tenant.
- For revocation checking, the OCSP responder's signing certificate.
- For the KDC service, select the realm name of the KDC service. If using the built-in KDC service, the KDC must be initialized. See the Installing and Configuring Workspace ONE Access for the built-in KDC details.

Procedure

1. In the Identity & Access Management tab, go to **Manage > Authentication Methods**.
2. In the **Mobile SSO (for iOS)** Configure column, click the pencil icon.
3. Configure the Mobile SSO for iOS page.

Option	Description
Enable KDC Authentication	To enable users to sign in using iOS devices that support Kerberos authentication, select this check box.
Realm	For tenant deployments in the cloud , the realm value is read-only. The realm name displayed is the identity manager realm name for your tenant. For on-premises deployments, if you are using the cloud hosted KDC, enter the pre-defined supported realm name that is supplied to you. The text in this parameter must be entered in all caps. For example, OP.VMWAREIDENTITY.COM. If you are using the built-in KDC, the realm name that you configured when you initialized the KDC displays.
Root and Intermediate CA Certificate	Upload the certificate authority issuer certificate file. The file format can be either PEM or DER.
Uploaded CA Certificate Subject DNs	The content of the uploaded certificate file is displayed here. More than one file can be uploaded and whatever certificates that are included are added to the list.
Enable OCSP	To use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate, select the check box
Send OCSP Nonce	If you want the unique identifier of the OCSP request to be sent in the response, select this check box.
OCSP Responder's Signing Certificate	Upload the OCSP certificate for the responder. When you are using the Workspace ONE UEM Certificate Authority, the issuer certificate is used as the OCSP certificate. Upload the Workspace ONE UEM certificate here as well.

Option	Description
OCSP Responder's Signing Certificate Subject DN	The uploaded OCSP certificate file is listed here.
Cancel Message	Create a custom sign-in message that displays when authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials.`
Enable Cancel Link	When authentication is taking too long, give users the ability to click Cancel to stop the authentication attempt and cancel the sign-in. When the Cancel link is enabled, the word Cancel appears at the end of the authentication error message that displays.
Enterprise Device Management Server URL	Enter the Mobile Device Management (MDM) server URL to redirect users when access is denied because the device is not enrolled into Workspace ONE UEM for MDM management. This URL displays in the authentication failure error message. If you do not enter a URL here, the generic Access Denied message displays.

4 Click **Save**.

What to do next

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

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

Configure Mobile SSO for Android Authentication in the Built-In Identity Provider

To provide single sign-on from Workspace ONE UEM-managed Android devices, you configure Mobile SSO for Android authentication in the Workspace ONE Access built-in identity provider.

Mobile single sign-on (SSO) for Android is an implementation of the certificate authentication method for VMware Workspace ONE® UEM-managed Android devices. With mobile single sign-on, users can sign in to their device and securely access their VMware Workspace® ONE® apps without reentering a password. See the Android Mobile Single Sign-on to VMware Workspace ONE guide for detailed configuration information.

Prerequisites

- Obtain the root certificate and intermediate certificates from the CA that signed the certificates presented by your users.
- List of Object Identifier (OID) of valid certificate policies for certificate authentication.
- For revocation checking, the file location of the CRL and the URL of the OCSP server.
- (Optional) OCSP Response Signing certificate file location.

Procedure

1 In the Identity & Access Management tab, go to **Manage > Authentication Methods**.

2 In the **Mobile SSO (for Android** Configure column, click the pencil icon.

3 Configure the Mobile SSO for Android page.

Option	Description
Enable Certificate Adapter	Select this check box to enable Mobile SSO for Android.
Root and Intermediate CA Certificate	Select the certificate files to upload. You can select multiple root CA and intermediate CA certificates that are encoded. The file format can be either PEM or DER.
Uploaded CA Certificates	The contents of the uploaded certificate file is displayed here.
User Identifier Search Order	Select the search order to locate the user identifier within the certificate. ■ **upn**. The UserPrincipalName value of the Subject Alternative Name ■ **email**. The email address from the Subject Alternative Name. ■ **subject**. The UID value from the Subject. **Note** ■ If a AirWatch CA is used for the tunnel client certificate generation, the User Identifier Search Order must be **UPN | Subject**. ■ If a third-party enterprise CA is used, the User Identifier Search Order must be **UPN | Email | Subject** and the certificate template must contain the subject name **CN={DeviceUid}:{EnrollmentUser}**. Make sure to include the colon (:).
Validate UPN Format	Enable this check box to validate the format of the UserPrincipalName field.
Certificate Policies Accepted	Create a list of object identifiers that are accepted in the certificate policies extensions. Enter the object ID number (OID) for the Certificate Issuing Policy. Click **Add another value** to add additional OIDs.
Enable Cert Revocation	Select the check box to enable certificate revocation checking. Certificate revocation prevents users who have revoked user certificates from authenticating.
Use CRL from Certificates	Select the check box to use the certificate revocation list (CRL) published by the CA that issued the certificates to validate a certificate's status of revoked or not revoked.
CRL Location	Enter the server file path or the local file path from which to retrieve the CRL.
Enable OCSP Revocation	Select this check box to use the Online Certificate Status Protocol (OCSP) certificate validation protocol to get the revocation status of a certificate.
Use CRL in case of OCSP failure	If you configure both CRL and OCSP, you can select this box to fall back to using CRL if OCSP checking is not available.
Send OCSP Nonce	Select this check box if you want the unique identifier of the OCSP request to be sent in the response.
OCSP URL	If you enabled OCSP revocation, enter the OCSP server address for revocation checking.

Option	Description
OSCP URL Source	Select the source to use for revocation checking. ■ **Configuration Only**. Perform certificate revocation check using the OCSP URL provided in the text box to validate the entire certificate chain. ■ **Certificate Only (required)**. Perform certificate revocation check using the OCSP URL that exists in the AIA extension of each certificate in the chain. Every certificate in the chain must have an OCSP URL defined, other wise the certificate revocation check fails. ■ **Certificate Only (Optional)**. Only perform certificate revocation check using the OCSP URL that exists in the AIA extension of the certificate. Do not check revocation if the OCSP URL does not exist in the certificate AIA extension. ■ **Certificate with fallback to configuration**. Perform certificate revocation check using the OCSP URL extracted from the AIA extension of each certificate in the chain, when the OCSP URL is available. If the OCSP URL is not in the AIA extension, check revocation using the OCSP URL configured in the OCSP URL text box. The OCSP URL text box must be configured with the OCSP server address.
OCSP Responder's Signing Certificate	Enter the path to the OCSP certificate for the responder. Enter as `/path/to/file.cer`
Uploaded OCSP Signing Certificates	The uploaded certificate files are listed in this section.
Enable Cancel Link	When authentication is taking too long, if this link is enabled, users can click Cancel to stop the authentication attempt and cancel the sign-in.
Cancel Message	Create a custom message that displays when the authentication is taking too long. If you do not create a custom message, the default message is `Attempting to authenticate your credentials.`

4 Click **Save**.

What to do next

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

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

Configuring Risk Score Based Authentication in Workspace ONE Access (Cloud only)

You can configure the Risk Score authentication method in Workspace ONE Access to allow or deny authentication based on the user's risk score. Every user is assigned a risk score of either high, medium, or low. When users attempt to log in, the risk score associated with the user determines what action is taken next.

Note Risk Score based authentication is available only for cloud deployments.

Your Workspace ONE tenant must be registered with VMware Workspace ONE® Intelligence™ to enable and use the Risk Score authentication method.

The Workspace ONE Intelligence service is the source that calculates the user's risk score based on risk factors. See the VMware Workspace ONE Intelligence guide on the Workspace ONE documentation page. guide for more information about use risk scoring.

Workspace ONE Access receives a risk level calculation from the Workspace ONE Intelligence service for every user. The risk score is recalculated every 24 hours.

When you enable Risk Score authentication in the Workspace ONE Access console, you select the type of action that is applied for each score level. The three actions that can be triggered are to allow access, require step-up authentication, or to deny access. For example, you can configure that when the risk score is High, users are denied access; Medium, users must enter a second form of authentication to log in, and Low, users can log in as normal.

You must configure an Access Policy to use Risk Score authentication. When a rule requires Risk Score authentication, when users attempt to log in, the risk score authentication action that you configured is applied. Risk score authentication can be configured for mobile single sign-on to iOS and Android devices.

When a user is denied access because of their risk score, the options to login are limited.

- Risk scores are updated every 24 hours. The user can wait until the Workspace ONE Intelligence service marks the user to a lower risk score.
- If risk score authentication was applied to a particular device type in the access policy, such as iOS or Android, the user can log in from a web browser.

Enable Risk Score Authentication and Select the Required Action Workspace ONE Access (Cloud only)

Enable the Risk Score authentication method in the Workspace ONE Access console. You then set the high, medium, and low authentication action that is applied when users attempt to log in.

Note Risk Score based authentication is available for cloud deployments only.

When you enable Risk Score authentication, you must select the type of action to apply to the score. You can allow access, require step-up authentication, or deny access. The action associated to the risk score determines the user experience.

- Allow Access. The user can log in and access policy rules are followed.
- Step-Up Authentication. The user cannot log in with only the credential that was entered. The next authentication method configured in the access policy is presented to the user.
- Deny Access. User cannot log in and no other login option is presented to the user.

Prerequisites

Your Workspace ONE Access tenant must be registered with Workspace ONE Intelligence.

Procedure

1. In the Workspace ONE Access console Identity & Access Management > Authentication Methods tab, select **Risk Score**.
2. Enable Risk Score and configure the authentication action required for low, medium, and high risk scores.

   The actions available to select are **Allow Access**, **Step-Up Authentication**, **Deny Access**.
3. Click **Save**.

What to do next

Go the Policies tab and edit the default access policy to add the Risk Score authentication method to the policy rules and create the policy rule for the step-up authentication flow if applied to a score. See Add a Web or Desktop Application-Specific Policy. To see an example policy rule configuration with Risk Score, see Example Access Policy Using Risk Score Authentication in Workspace ONE Access (Cloud only).

Example Access Policy Using Risk Score Authentication in Workspace ONE Access (Cloud only)

After you enable Risk Score authentication in Workspace ONE Access, you must set up the access policy rules to use this authentication method.

This example shows an access policy that is configured with the following access flow.

- Users with a low risk score and a compliant iOS device can access the apps without entering additional credentials.
- Users with a medium risk score and a compliant iOS device must use VMware Verify as a second authentication method before accessing the app.
- Users with high risk-scores and a compliant iOS device are denied access to the apps.

Risk Score authentication can be applied to any policy rule, but Risk Score cannot be the first authentication method listed in the policy rule.

Prerequisites

For this example, the following authentication methods are enabled.

- Mobile SSO (for iOS)
- Device Compliance
- Risk Score with the action type set up as follows.
  - Low set to Allow Access
  - Medium set to Step-up Authentication
  - High set to Deny Access

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.

2 Create a new policy named **`Restricted Resources`**.

3 In the **Applies To** section, the secure apps to associate with this policy are added. For example, Company Restricted App 1, Company Restricted App 2, Company Restricted App 3.

4 Policy rule is configured as follows.

Option	Description
If a user's network range is	ALL RANGES
and user accessing content from	**iOS**
and user belongs to groups	No group is selected. The access policy rule applies to all users.
Then perform this action	**Authenticate using....**
then the user may authenticate using	**Mobile SSO (for iOS)**. **Device Compliance (with AirWatch)** **Risk Score**
If the preceding methods fails or is not applicable, then	Configured multi-factor authentication. **Mobile SSO (for iOS)** **Device Compliance (with AirWatch)** **VMware Verify**
Re-authenticate after	8 hours

Results

For more information about creating access policy rules, see Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users .

User Options When Access is Denied

When a user is denied access because of their risk score, the options to login are limited.

- Risk scores are updated every 24 hours. The user can wait until the Workspace ONE Intelligence service marks the user to a lower risk score.
- If risk score authentication was applied to a particular device type in the access policy, such as iOS or Android, the user can log in from a web browser.

Enabling the Out of Box Experience for Workspace ONE on Dell Windows 10 Devices in Workspace ONE Access

When users receive a new Dell® Windows 10 device with out-of-box (OOBE) provisioning enabled in the Workspace ONE UEM Windows 10 Provisioning Service, you can configure an authentication method in Workspace ONE Access to manage Workspace ONE app log ins.

To deliver this OOBE with the Workspace ONE application, you must enable the External Access Token authentication method as part of the Workspace ONE UEM integration. Then the authentication method is enabled in the built-in provider. You then create an access policy rule to use the External Access Token authentication method.

The Workspace ONE OOBE runs the Workspace ONE application without requiring users to enter their sign-in credentials a second time. If this authentication method is not enabled, users must sign in to Workspace ONE in addition to signing in to the device during the Windows registration process.

Activate External Access Token as an Authentication Method

In Workspace ONE Access, the External Access Token authentication method is unique to the Workspace ONE UEM integration and is required for both single sign-on (SSO) and triggering the out-of-box experience (OOBE) in Workspace ONE on Windows 10 devices.

Prerequisites

When using External Access Token authentication, the AirWatch Cloud Connector component must be deployed and configured.

- External Access Token Authentication enabled on the AirWatch page in the Identity & Access Management tab.
- AirWatch Provisioning Service for Windows 10 devices configured.

The configuration of External Access Token is read-only and is based off the Workspace ONE UEM (AirWatch) configuration in Workspace ONE Access. The exception is the token lifetime field.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Authentication Methods**.
2. In the **AirWatch External Access Token Configure** column, click the pencil icon.
3. Review the configuration.

Option	Description
Enable AirWatch External Access Token	This check box is enabled on the AirWatch page.
AirWatch Admin Console URL	Pre-populated with the AirWatch URL.
AirWatch API Key	Pre-populated with the AirWatch Admin API key.

Option	Description
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 External Access Token Lifetime in Seconds	The access token is used to validate the authentication with Workspace ONE Access. Access tokens have a limited lifetime. The time configured is the maximum time that the access token is valid. The token life is editable and defaulted to 600 seconds, which is 10 minutes. If the access token expires, users are prompted to authenticate again in the Workspace ONE application.

4 Click **Save**.

What to do next

Associate the AirWatch External Access Token authentication method in the built-in identity provider. See Configure a Built-in Identity Provider in Workspace ONE Access

After the AirWatch External Access Token is associated to the built-in identity provider, create an access policy rule to use this auth method. See Create Access Policy for Workspace ONE Out-of-Box Experience Process.

Configure the Local Directory Password Authentication Method

Configure password authentication for local directories in the Workspace ONE Access console, Identity & Access Management > Auth Methods page.

After the authentication method is configured, you associate the Password (Local Directory) authentication method in the built-in identity provider associated to the local directory.

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, go to **Manage > Auth Methods**.

2 In the **Password (Local Directory)** Configure column, click the icon.

3 Select the check box **Enable Local Directory Password Authentication**.

4 In the **Number of password tries** text box enter the maximum number of failed login attempts. No more logins are allowed after the failed login attempts reach this number. The default is five attempts.

5 Click **Save**.

What to do next

- Associate the Password (Local Directory) authentication method in the built-in identity provider.

Managing Authentication Methods in the Workspace ONE Access Identity Providers

5

The Workspace ONE Access identity providers are configured to manage who can authenticate and what authentication methods are used to provide single sign-on to access Workspace ONE resources.

In the Workspace ONE Access service, the identity provider offers user authentication as a service. The identity provider authenticates the user and provides an authentication token to the service provider.

The following is managed in identity provider configurations.

- Directory to use for users. One directory can be selected for each identity provider.
- Networks that the identity provider can be accessed from.
- Authentication methods associated with the identity provider. This can include authentication methods in the User Auth service, Kerberos Auth service, and authentication methods configured in the Workspace ONE Access console Identity & Access Management Manager > Authentication Methods page.

This chapter includes the following topics:

Configure a Built-in Identity Provider in Workspace ONE Access

In the built-in identity provider, configure the users, network ranges, and authentication methods that users use for single sign-on to their apps portal.

A built-in identity provider is automatically created when you set up a directory in the Directory Sync service and selected to set up the password authentication method for the directory. If you did not select to set up password authentication, you can create the built-in identity provider.

Prerequisites

To configure the built-in identity provider, make sure that the following are set up.

- Users and groups located in an enterprise directory synced to the Workspace ONE Access directory.
- Network ranges created in the Policies > Network Ranges page.
- The authentication methods to be used in the built-in identity provider configured.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, go to **Manage > Identity Providers**.
2. Select the identity provider labeled **Built-in** and configure the identity provider details.

Option	Description
Identity Provider Name	Enter the name for this built-in identity provider instance.
Users	Select the directory of the users to authentication from the list of configured directories. Only one directory can be selected.
Connector Authentication Methods	After you select a directory, the User Auth service authentication methods that are associated with that directory display. Select the methods to associate to this identity provider.
Authentication Methods	The authentication methods that are configured in the Identity & Access Management Manage > Authentication Methods page are displayed. Select the check box for the authentication methods to associate to the identity provider. For Device Compliance (with Workspace ONE UEM) and Password (AirWatch Connector), make sure that the option is enabled in the Workspace ONE UEM configuration page.
Network	The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication.
KDC Certificate Export	When the Mobile SSO (iOS) authentication method associated with the built-in identity provider, you download the KDC certificate.

3. Click **Add**.

What to do next

Make sure that all authentication methods are associated with an access policy rule.

Configure Workspace ONE Access Identity Provider Instance with Kerberos Authentication

Configure the Workspace ONE Access identity provider with the users, network ranges, authentication methods, and redirect host name for Kerberos authentication.

Prerequisites

To configure the Workspace ONE Access identity provider, make sure that the following are set up.

- Users and groups located in an enterprise directory synced to Workspace ONE Access Directory.
- Network ranges created in the Policies > Network Ranges page.
- The Kerberos authentication configured.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, go to **Manage > Identity Providers**.
2. Select the identity provider labeled **Workspace ONE Access IDP** and configure the identity provider details.

Option	Description
Identity Provider Name	Enter the name for this built-in identity provider instance.
Users	Select the directories of users to authentication. The configured directories are listed.
Authentication Methods	After you select a directory, the User Auth service authentication methods that are associated with that directory display. Select the methods to associate to this identity provider.
Network	The existing network ranges configured in the service are listed. Select the network ranges for the users based on the IP addresses that you want to direct to this identity provider instance for authentication.
IdP Hostname	Enter the hostname where the Workspace ONE Access identity provider redirects to for authentication. If you are using a load balancer for Kerberos authentication, the host name is the load balancer host name. For example, if the load balancer hostname is mylb, enter as **`mylb.company.com:port`**. If you are using a port other than 443, you can set this as Hostname:port.

3. Click **Add**.

What to do next

Configuring SAML as a Third-Party Identity Provider Instance to Authenticate Users

You can configure a third-party identity provider that is used to authenticate users in the Workspace ONE Access 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 Workspace ONE Access service can reach the third-party instance.
- Obtain the appropriate third-party metadata information to add when you configure the identity provider in the Workspace ONE Access console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

Add and Configure a SAML Third-Party Identity Provider Instance in Workspace ONE Access

When you add and configure new SAML identity provider instances for your Workspace ONE Access 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

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

- Verify that the third-party instances are SAML 2.0 compliant and that the Workspace ONE Access service can reach the third-party instance.
- Coordinate the integration with the third-party identity provider. Depending on the identity provider, you might need to configure both settings in unison.
- Obtain the appropriate third-party metadata information to add when you configure the identity provider in the Workspace ONE Access console. The metadata information you obtain from the third-party instance is either the URL to the metadata or the actual metadata.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Identity Providers**.
2. Click **Add Identity Provider** and select **Create SAML IDP**.

3 Configure the SAML identity provider settings.

Form Item	Description
Identity Provider Name	Enter a name for this identity provider instance.
SAML Metadata	Add the third-party identity provider 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. Click **Process IdP Metadata**. 2 Select how the user is identified. The identifier sent in an inbound SAML Assertion can be either sent in the Subject or in the Attribute element. ■ **NameID Element**. User identifier is retrieved from the NameID element of the Subject element. ■ **SAML Attribute**. User identifier is retrieved from a specific Attribute or AttributeStatement element. 3 If you select **NameID Element**, the NameID formats supported by the identity provider are extracted from the metadata and added to the Name ID Format table that is displayed. ■ In the **Name ID value** column, select the user attributes that are configured in the Workspace ONE Access service to map to the NameID formats that are displayed. You can add custom third-party name ID formats and map them to the user attribute values in the Workspace ONE Access service. ■ Select the **Name ID Policy in SAML Request** response identifier string format to use. This format must match the specific Name ID Policy format configuration of the third-party IDP used to establish trust with the Workspace ONE Access service. ■ Select the option to send Subject information in SAML Request when the information is available. 4 If you select **SAML Attribute**, include the Attribute Format and Attribute Name. Select the user attribute in the Workspace ONE Access service to map to the SAML Attribute.
Just-in-Time Provisioning	Just-in-Time provisioning users are created and updated dynamically when they log in, based on SAML assertions sent by the identity provider. See About Just-in-Time User Provisioning. If you enable JIT, enter the directory and domain name for the JIT directory.
Users	Select the directories that include 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.

Form Item	Description
Single Sign-Out Configuration	When users sign in to Workspace ONE from a third-party identity provider (IDP), two sessions are opened, one on the third-party identity provider, and the second on the identity manager service provider for Workspace ONE. The lifetime of those sessions is managed independently. When users sign out of Workspace ONE, the Workspace ONE session is closed, but the third-party IDP session might still be open. Based on your security requirements, you can enable single sign-out and configure single sign-out to sign out of both sessions, or you might keep the third-party IDP session intact. Configuration Option 1 ■ You can enable single sign-out when you configure the third-party identity provider. If the third-party identity provider supports SAML-based single logout protocol (SLO), users are logged out of both sessions when they sign out of the Workspace ONE portal. The Redirect URL text box is not configured. ■ If the third-party IDP does not support SAML-based single logout, you enable single sign-out, and in the Redirect URL text box designate an IDP single logout endpoint URL. You can also add a redirect parameter to append to the URL that sends users to a specific endpoint. Users are redirected to this URL when they sign out of the Workspace ONE portal and are signed out from the IDP as well. Configuration Option 2 ■ Another single sign-out option is to log users out of their Workspace ONE portal and redirect them to a customized endpoint URL. You enable single sign-out, designate the URL in the Redirect URL text box, and the redirect parameter of the customized endpoint. When users sign out of the Workspace ONE portal, they are directed to this page, which can display a customized message. The third-party IDP session might still be open. The URL is entered as **`https://<vidm-access-url>/SAAS/auth/federation/slo`**. If Enable Single Sign-out is not enabled, the default configuration in the Workspace ONE Access service is to directed users back to the Workspace ONE portal sign-in page when they sign out. The third-party IDP session might still be open.
SAML Signing Certificate	Click **Service Provider (SP) Metadata** to see URL to Workspace ONE Access 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 Workspace ONE Access 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

- Add the third-party identity provider authentication method to the Workspace ONE default access policy. See Chapter 6 Managing Access Policies in Workspace ONE Access That Apply to Users
- Edit the third-party identity provider's configuration to add the SAML Signing Certificate URL that you saved.

Disabling Authentication Methods Associated with Built-In Identity Provider

You can disable authentication methods from the Authentication Methods page. When you disable an authentication method, if the authentication method is associated with any identity provider, the authentication method is disabled in that identity provider.

The authentication method is also removed as an option in all the access policy rules.

Important If the authentication method you disabled is configured in an access policy rule, the access policy rule must be updated to select another authentication method. If the access policy rule is not updated, users might not be able to sign in to their apps portal or access their resources.

To disable an authentication for specific built-in identity providers, in the built-in identity provider configuration page, deselect the box for the associated authentication method.

Managing Access Policies in Workspace ONE Access That Apply to Users

6

The Workspace ONE Access service attempts to authenticate users based on the authentication methods, the default access policy, network ranges, and the identity provider instances you configure.

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

For example, you can configure a rule that requires users who sign in using iOS devices from a specific network to authenticate using RSA SecurID. Then configure another rule that requires users who sign in using any type of device from the internal network IP address to authenticate using their password.

A policy rule can also be configured to deny access to users by network range and device type.

This chapter includes the following topics:

Managing Access Policies

Access policies can be used to establish trust between users, devices, and apps in the Workspace ONE environment. You can configure access policies to manage how users access their catalog of resources and how users access specific resources.

Access policies consist of rules that specify criteria that users must meet to sign in to their apps portal and use their resources. Administrators configure features such as mobile single sign-on, conditional access to applications based on enrollment, compliance status, multi-factor authentication, and step-up authentication.

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 an access rule or you can apply the rule to everyone.

The Workspace ONE Access service includes a default access policy set that contains basic access policy rules that control access as a whole. The basic access policy rules are initially set up to allow all user access from all network ranges through a web browser or the Workspace ONE application. You can edit the default policy set to create more rules for specific types of devices and to use various types of authentication.

You can also create application-specific access policy rules to manage access to specific web and desktop applications. Application-specific access policy rules can be used to create step-up authentication that requires stronger authentication to more sensitive resources.

Access Policy Settings

Create access policy rules that specify the criteria that must be met to access the Workspace ONE portal and the entitled applications as a whole. You can also create application-specific access policies with rules to manage user access to specific web and desktop applications.

Network Range

Network addresses are assigned to the access policy rule to manage user access based on which IP address is used to sign in and access apps. When the Workspace ONE Access service is configured on premises, you can configure network IP address ranges for internal network access and external network access. You can then create different rules based on the network range configured in the rule.

Note When configuring network addresses for the Workspace ONE Access Cloud service, specify the Workspace ONE Access tenant public address used to access the internal network.

Network ranges are configured from the Identity & Access Management tab, Manage > Policies > Network Ranges page before configuring access policy rules.

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

Device Type

Access policy rules are configured to manage the type of device used to access the portal and resources. Devices that you can specify include iOS and Android mobile devices, computers that run either Windows 10 or macOS operating systems, Web Browser, Workspace ONE & Intelligent Hub App, and All Device Types.

The policy rule with device type Workspace ONE & Intelligent Hub App defines the access policy for launching applications from the Workspace ONE or Intelligent Hub app after signing in from a device. When this rule is the first rule in the policy list, after users are authenticated, they can stay signed in to the app and access their resources for up to 90 days according to the default setting.

The policy rule with device type Web Browser defines an access policy using any kinds of web browser, regardless of device hardware types and operations systems.

The policy rule with device type All Device Types matches all cases of access.

When the Workspace ONE or Intelligent Hub app is used to access apps, the device types are organized in the policy set with Workspace ONE App device type the first rule, followed by mobile, Windows, and macOS, Web Browser device types. All Device Types is listed last. The order the rules are listed indicates the order that the rules are applied. When a device type matches the authentication method, subsequent rules are ignored. If the device type Workspace ONE App rule is not the first rule in the policy list, users are not signed in to the Workspace ONE app for the extended time. See Applying Workspace ONE App Rules to Access Policies.

Add Groups

You can apply different authentication rules based on user's group membership. Groups can be groups that are synced from your enterprise directory and local groups that you created in the Workspace ONE Access console.

When groups are assigned to an access policy rule, users are asked to enter their unique identifier, and then are asked to enter the authentication based on the access policy rule. See Login Experience Using Unique Identifier in the Workspace ONE Access Administration guide. By default, the unique identifier is **userName**. Go to the Identity & Access Management > Setup > Preferences page to see the configured unique identifier value or to change the identifier.

Note When a group is not identified in a rule, the rule applies to all users. When you configure an access policy that includes a rule with a group and a rule with no group, rules configured with a group must be listed before rules that are not configured with groups.

Actions Managed by Rules

An access policy rule can be configured to allow or deny access to the workspace and resources. When a policy is configured to provide access to specific applications, you also can specify the action to allow access to the app with no further authentication required. For this action to apply, the user is already authenticated by the default access policy.

You can selectively apply conditions in the rule that apply to the action, such as which networks, device types, and groups to include, and the device enrollment and compliance status. When the action is to deny access, users cannot sign in or launch apps from the device type and network range configured in the rule.

Authentication Methods

The authentication methods that are configured in the Workspace ONE Access service are applied to access policy rules. For each rule, you select the type of authentication methods to use to verify the identity of users who sign in to Workspace ONE or access an app. You can select more than one authentication method in a rule.

The authentication methods are applied in the order they are listed in the rule. The first identity provider instance that meets the authentication method and network range configuration in the rule 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.

You can configure authentication chaining in an access policy rules to require users to pass credentials through more than one authentication methods before they can sign in. Two authentication conditions in one rule are configured and the user must correctly respond to both authentication requests. For example, if you set the authenticate using setting to Password and VMware Verify, users must enter both their password and the VMware Verify passcode before they are authenticated.

Fallback authentication can be set up to give users who fail to pass the previous authentication request another chance to sign in. If an authentication method fails to authenticate the user and fallback methods are also configured, users are prompted to enter their credentials for the additional authentication methods that are configured. The following two scenarios describe how this fallback can work.

- In the first scenario, the access policy rule is configured to require users to authenticate with their password and VMware Verify passcode. Fallback authentication is set up to require the password and the RADIUS credential for authentication. A user enters the password correctly, but fails to enter the correct VMware Verify passcode. Because the user entered the correct password, the fallback authentication request is only for the RADIUS credential. The user does not need to reenter the password.
- In the second scenario, the access policy rule is configured to require users to authenticate with their password and VMware Verify passcode. Fallback authentication is set up to require RSA SecurID and RADIUS for authentication. A user enters the password correctly but fails to enter the correct VMware Verify passcode. The fallback authentication request is for both the RSA SecurID credential and the RADIUS credential for authentication.

To configure an access policy rule that requires authentication and device compliance verification for Workspace ONE UEM-managed devices, Device Compliance with AirWatch must be enabled in the built-in identity provider page. See Enabling Compliance Checking for Workspace ONE UEM Managed Devices. The built-in identity provider authentication methods that can chain with Device Compliance with AirWatch are Mobile SSO (for iOS), Mobile SSO (for Android), or Certificate (Cloud Deployment).

When VMware Verify is used for two-factor authentication, VMware Verify is the second authentication method in the authentication chain. VMware Verify must be enabled in the Built-in identity provider page. See Configuring VMware Verify for Two-Factor Authentication.

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 open a specific application. For example, a value of 8 in a web application rule means once authenticated, users do not need to reauthenticate again for 8 hours.

The policy rule setting **Re-authentication after** does not control the application sessions. The setting controls the time after which users have to be reauthenticated.

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 that overrides the default message for each access policy rule. The custom message can include text and a link for a call to an action message. For example, in a policy rule to restrict access to devices that are enrolled, 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.`

Applying Workspace ONE App Rules to Access Policies

When the Workspace ONE app is installed on devices, users can access their entitled apps using the single sign-on functionality through Workspace ONE Access.

The Workspace ONE app is an OAuth client that uses the GreenBox-TemplatedId OAuth template to manage access to the app. This template is registered in the Catalog > Settings > Remote Access page in the Workspace ONE Access console.

When users successfully sign in to the Workspace ONE App the first time, an OAuth access token is applied to the app. This access token is configured with a time to live (TTL). The TTL value is the maximum time that users can access Workspace ONE without signing in again.

A refresh token is configured so that when the access token expires, Workspace ONE requests a new access token. This way users can stay signed in to the Workspace ONE app for an extended period without having to sign in again.

The Workspace ONE access token time to live settings is configured as follows.

- Access token time to live is 3 hours.
- Refresh token time to live is 90 days.
- Idle token time to live is 10 days.

If the user uses the Workspace ONE app every day, the user does not need to sign in again for 90 days, based on the refresh token TTL value. However, if the user is idle and does not use the Workspace ONE app for 10 days, the user must sign in to Workspace ONE again.

To sign in to Workspace ONE and have the access token applied to the app, the Device Type **Workspace ONE App** should be the first rule in the default access policy to enforce the OAuth TTL. After users are authenticated, the access token manages how long the session is valid, based on refresh token and idle token values.

You can configure the session reauthentication value in the access policy rule to be the same as the refresh token time to live value, 90 days, or 2160 hours. If you make the session reauthentication value less than the refresh token time to live, users are prompted to sign in to Workspace ONE when the session reauthentication threshold is met.

If the Workspace ONE App is not the first rule, an OAuth access token is not applied to the Workspace ONE app and single sign-on to other resources is not available. Users are required to sign to the apps in their portal in every time they access Workspace ONE from their device.

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.

Note Internet Protocol version 6 (ipV6) addresses are not supported.

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.

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 Workspace ONE Access deployment based on your network topology. The network ranges can be set based on internal and external access.
- For Workspace ONE Access Cloud services, verify the tenant public address used for the internal network range. For the cloud services, the internal network identifier is not 10.x.x.x.
- When Horizon is enabled in the service, you specify the Horizon URL on a per Network Range basis. To add a network range when the Horizon module is enabled, take note of the Horizon Client access URL and port number for the network range. See the Setting Up Resources in VMware Workspace ONE Access guide, Providing Access to View Desktop Pools and Application section.

Procedure

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

Add Deny Access Rule to Access Policy

A deny access rule can be created to deny access to an application by network range and by device type.

Procedure

1 In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.

2 Click **Add Policy**.

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

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

5 Click **Next**.

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

Option	Description
If a user's network range is	Select the network range.
and user accessing content from	Select the device type that this rule manages.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy rule applies to all users.
Then perform this action	Select **Deny access**.

7 Click **Save**.

Enabling Persistent Cookie on Mobile Devices

Enable Persistent Cookie for User Sessions to provide single sign-in between the system browser and native apps and single sign-in between native apps when apps use Safari View Controller on iOS devices and Chrome Custom Tabs on Android devices.

The persistent cookie stores users' sign-in session details so that users do not need to reenter their user credentials when they access their managed resources through Workspace ONE Access. The cookie timeout can be configured in the access policy rules you set up for iOS and Android devices.

Note Cookies are vulnerable and susceptible in common browser cookie-theft and cross site script attacks.

Enable Persistent Cookie

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.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Setup > Preferences**.
2. Check **Enable Persistent Cookie**.
3. Click **Save**.

What to do next

To set the persistent cookie session timeout, edit the reauthentication value in the access policy rules for the iOS and Android devices types.

Managing the Default Access Policy

The Workspace ONE Access service includes a default access policy set that controls user access to their Workspace ONE portals and their Web applications.

The default access policy is configured to allow access to all network ranges from all device types. The session timeout is eight hours. You can edit the policy set to change the policy rules as necessary.

When you enable authentication methods other than password authentication in the Workspace ONE Access service, you must edit the default policy to add these authentication methods to the policy rules.

Access rules can be created in the default access policy to manage mobile single sign-on from iOS, Android, macOS, and Windows 10 devices.

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

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 sign-in attempts for Active Directory password and for RSA SecurID authentication is five by default. When a user has five failed login attempts, the service attempts to sign in the user with the next authentication method on the list. When all authentication methods are exhausted, the service issues an error message.

Edit the Default Access Policy

You must edit the policy rules to select the authentication methods you configured in Workspace ONE Access and set the order in which the authentication methods are used for authentication.

Prerequisites

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

The Password (Local Directory) authentication method is applied to the System Directory. The default access policy includes a policy rule configured with Password (Local Directory) as a fallback method so that admins can log into the Workspace ONE Access console.

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

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.
2. Click **Edit Default Policy**.
3. You can change the policy name to be more specific. For example, Company Basic Access Policy.

   The policy applies to all apps that are in the catalog, unless the app is assigned to a web-specific access policy.
4. Click **Next** to open the Configuration page.
5. Select the rule name to edit, or to add a policy rule, click **Add Policy Rule**.

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

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

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

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

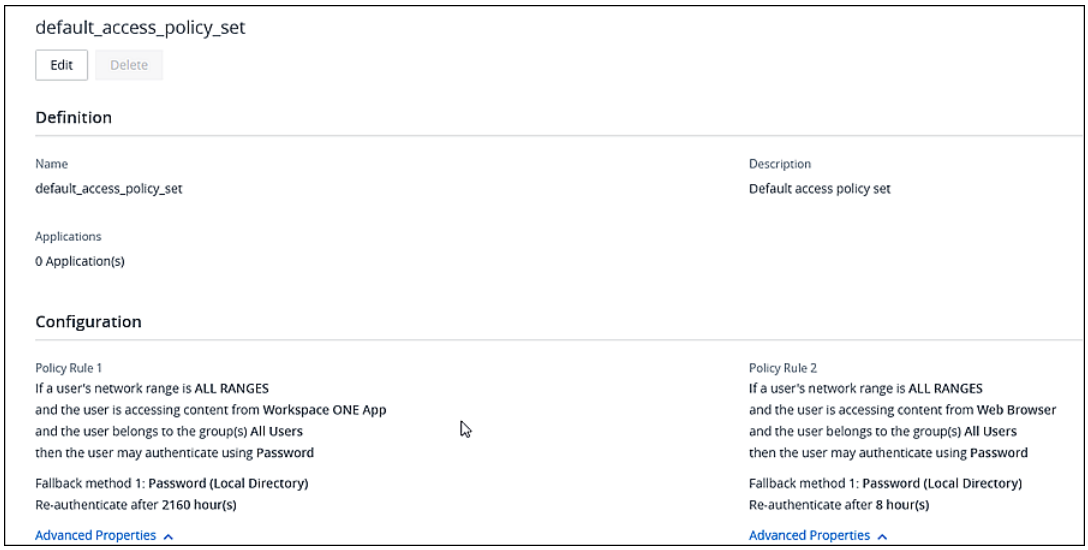
What to do next

Create additional rules, if necessary.

After all the rules are created, order the rules in the list as to how they are applied. If the Workspace ONE app is used to access Workspace ONE and other resources, make sure that the Workspace ONE app is the first rule in the list.

The edited policy rules take effect immediately.

Figure 6-1. Default Access Policy Configuration



Example of a Default Access Policy for Single Sign-On to the Workspace ONE App

To achieve the single sign-on experience when users access resources from the Workspace ONE app, the default access policy is configured with rules for each type of device that is used in your environment, Android, iOS, MacOS, or Windows 10..

In this example of a default access policy configuration, the default access policy is created with rules to cover users who sign in from all network ranges. For managed access, Device Compliance for AirWatch is configured for the devices and the Workspace ONE app rules. The following rules are created.

- A rule for each type of mobile device that can be used to access the Intelligent Hub App.
- A rule for user access from the Workspace ONE App device type for the Intelligent Hub app. All authentication methods for all devices that are supported are configured in this rule. The Device Compliance authentication method is applied to support access from managed devices.
- A rule for user access from the Web Browser device type to access Workspace ONE from any web browser.
- A rule for users on unmanaged devices to access resources.

When users use one of the devices to sign in to the Workspace ONE app, they are authenticated according to the authentication method configured for the device type. After the user is successfully authenticated, when they launch other resources from the Intelligent Hub app screen, that authentication method is recognized and the user is not prompted to authenticate again.

If the authentication method used to authenticate to Workspace ONE is not recognized, when a user launches resources from the Intelligent Hub app, the user is prompted to authenticate according to the Workspace ONE App rule.

Example of Access Policy Rule Conditions to Use for Workspace ONE

For the best user experience, list the device type Workspace ONE App as the first rule in the default access policy. When the rule is first, users are signed in to the app and can launch resources without reauthenticating until the session expires.

1. Create rules for each device that can be used to access Workspace ONE. This example is for the rule for allow access from the device type iOS.

- Network range is **ALL RANGES**.
- Users can access the content from **iOS**.
- No groups are added to the policy rule. **All Users** are supported.
- Configure all authentication methods that are supported.
  - Authenticate using **Mobile SSO (for iOS)** and **Device Compliance (with AirWatch)**.
  - Fallback method 1: **Password (cloud deployment)**.
- Session reauthentication after **8 hours**.

2. Create the rule for the device type Workspace ONE App. Each authentication method configured for the devices in step 1 must be included in this rule.

- Network range is **ALL RANGES**.
- Users can access the content from **Workspace ONE App**.
- No groups are added to the policy rule. **All Users** are supported.
- Configure all authentication methods that are supported.
  - Authenticate using **Mobile SSO (for iOS)** and **Device Compliance (with AirWatch)**.
  - Fallback method 1: **Mobile SSO (for Android)** and **Device Compliance (with AirWatch)**.
  - Fallback method 2: **Password (cloud deployment)**.
- Session reauthentication after **2160 hours**.

2160 hours is equal to 90 days, which are the Workspace ONE App OAuth token refresh token time to live.

3. Create the rule for the device type Web Browser to access the Workspace ONE portal from any web browser. This example includes as a fallback the authentication method Password (Local Directory). To authentication system administrators who sign in, at least one rule must be configured to authentication using Password (Local Directory). The session times out after 24 hours.

- Network range is **ALL RANGES**.
- Users can access the content from **Web Browser**.
- No groups are added to the policy rule. **All Users** are supported.
- Configure all authentication methods that are supported.
  - Authenticate using **Password (cloud deployment)**.
  - Fallback method 2: **Password**.
  - Fallback method 3: **Password (Local Directory)**.
- Session reauthentication after **8 hours**.

4. Create the rule for all device types to access unmanaged resources.

- Network range is **ALL RANGES**.
- Users can access the content from **All Devices**.
- No groups are added to the policy rule. **All Users** are supported.
- Configure all authentication methods that are supported.
  - Authenticate using **Password (cloud deployment)**.
- Session reauthentication after **8 hours**.

When you create rules for all devices, Workspace ONE App and Web Browser, you default policy set looks like the following screenshot.

Figure 6-2. Default Policy Set with Workspace ONE App Listed First

Flow with this default access policy configured.

1 UserA signs in to the Intelligent Hub app from their iOS device and is asked to authenticate with Mobile SSO (for iOS). The third rule is Mobile SSO (for iOS) and the authentication is successful.

2 UserA launches a resource listed in the Workspace ONE app and because the Workspace ONE App rule includes the authentication method Mobile SSO (for iOS) as a fallback authentication method, the resource is launched without requesting authentication again. The user can launch resources without signing in to Workspace ONE again for 2160 hours.

Also see Configure Access Policy Rule for Compliance Checking.

Configure Device Enrollment Policy Rules for Workspace ONE UEM Enrollments in Workspace ONE Access (Cloud Only)

You can configure an access policy rule in the Workspace ONE Access default access policy to authenticate users for device enrollment into Workspace ONE UEM.

When the device enrollment rule is applied, users who sign into the Workspace ONE Intelligent Hub app on a device that is not enrolled are authenticated according to the Device Enrollment rule. After they are authenticated, the Intelligent Hub app facilitates the enrollment with Workspace ONE UEM. After a device is enrolled, users are prompted to sign in to the Intelligent Hub using the authentication method configured in the default access policy for mobile single sign-on to an iOS or Android device.

You can configure an access policy rule in the Workspace ONE Access default access policy to authenticate users for device enrollment or registration through the Workspace ONE Intelligent Hub app into Workspace ONE UEM. This policy only applies to a user enrolling or registering with the Workspace ONE Intelligent Hub app. This policy does not apply to staging workflows nor Web or Apple DEP enrollments.

Prerequisites

- Workspace ONE Access must be enabled as the authentication source in Workspace ONE UEM.

  Note To see which service is the source for authentication in the Intelligent Hub app, in the UEM console go to the Devices > Device Settings > Devices & Users > General > Enrollment > Authentication tab.

- Authentication methods that are used for device enrollment authentication configured in Workspace ONE Access.
- Workspace ONE Intelligent Hub app installed on iOS or Android device.

Procedure

1. In the Workspace ONE Access console, navigate to **Manage > Policies** and click **EDIT DEFAULT POLICY**.
2. On the Definition page, verify the default policy name and click **Next**.
3. On the Configuration page, click **+ ADD POLICY RULE**.

Option	Description
If a user's network range is	Select the network range.
and user accessing content from	Select **Device Enrollment** as the device type.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy rule applies to all users.
Then perform this action	Select **Authenticate using....**
then the user may authenticate using	Select the authentication method that the enrollment policy requires. To set up multi-factor authentication, click **+** and select the MFA method to use.
If the preceding method fails or is not applicable, then	You can configure fallback authentication.
Reauthenticate after	Select the length of the session, after which users must authenticate again.

4. Click **Save**.
5. Click **ADD POLICY RULE** to add rules for mobile single sign-on for iOS and Android devices.
6. On the **Configuration** page, order the rules to make sure that the Device Enrollment rule is listed above the iOS and Android mobile SSO rules.

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

When WS-Fed Web Application (Office 365) clients (VMware Boxer, iOS, and Android native email clients) uses the legacy authentication flow user name and password authentication, you configure client access policies in the Office 365 application from the Catalog page. See the VMware Identity Manager Integration with Office 365 guide.

Note Access policies are not created for applications that are managed by an Application Source nor for weblinks.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.
2. Click **Add Policy**.
3. Add a policy name and description in the respective text boxes.
4. In the **Applies To** section, type the application in the Search text box, and select the applications to associate with this policy.
5. Click **Next**.
6. Click **Add Policy Rule** to add a rule.

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

7 Configure additional rules, if necessary.

8 Click **Save**.

Applying Web and Desktop Application-Specific Policies

You can create custom access policies for individual web and desktop applications that are in the catalog. These access policies can restrict access based on location, device type, authentication method, and session length. To limit access, you can associate a specific group to an application rule.

The following are examples of web-application-specific policies that you can create to control access to specified Web applications.

Example 1 Basic Web-Application-Specific Policy Assigned to a Group

In this example, a new application-specific access policy is created and applied to web applications that the Sales Team group can access. Two rules are applied. The first rule is specific to users in the Sales Team group who access the app from the internal network.

The rule to access from the internal network is configured as follows.

- Network range is **INTERNAL NETWORK**.
- Users can access the content from the **Web Browser**.
- Users belong to the group **Sales Team**.
- First authentication method is **Kerberos**.
- Fallback is **Password**.
- Session reauthentication after **8 hours**.

To access the sales team applications from the internal network, a member of the Sales Team group, launches an app from a web browser and is asked to enter a name and Kerberos password. If Kerberos authentication fails, the user is asked to enter the Active Directory password. The session is available for eight hours. After eight hours, the user is prompted to sign in again.

The second rule is applied if users in the Sales Team group access the app from an eternal site through a web browser.

The rule to access from an external site is configured as follows.

- Network range is **ALL RANGES**.
- Users can access the content from the **Web Browser**.
- Users belong to the group **Sales Team**.
- Authentication methods implemented include the ability to sign in with mobile devices and from a computer.
  - Authenticate using **Mobile SSO (for iOS)**.
  - Fallback to **Mobile SSO (for Android)**.

    - Fallback to **RSA SecurID.**
- Session reauthentication after **4 hours**.

To access these applications from outside the enterprise network, depending on the type of device, the user is required to sign in with the mobile device passcode or with the RSA SecurID passcode. The session starts and is available for four hours. After four hours, the user is prompted to sign in again.

Example 2 Strict Web-Application-Specific Policy Assigned to a Group

In this example, an application-specific access policy is created and applied to an extra sensitive web application. Members of the sales team group can access this application from any type of device but only for 1 hour before authentication is required again.

- Network range is **ALL RANGES**.
- Users can access the content from **All Device Types**.
- Users belong to the group **Sales Team**.
- Authentication method is **RSA SecurID**.
- Session reauthentication after **1 hour**.

The Sales Team user signs in and is authenticated based on the default access policy rules and can access the apps portal and resources. The user clicks the app that is managed by the strict access policy rule as specified in Example 2. The user is redirected to the RSA SecurID authentication sign-in screen.

After the user successfully signs in, the service launches the app and saves the authentication event. The user can continue to launch the app without signing in for up to one hour. After the hour, the user is prompted to reauthenticate through RSA SecurID.

Configure Custom Access Denied Error Message

For each policy rule, you can create a custom access denied error message that displays when users attempt to sign in and fail because their credentials are invalid.

The custom message can include a message and a link to another URL to help users resolve their issues. You can use up to 4000 characters, which are about 650 words.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.
2. Select the access policy to edit.
3. Click **Edit** and then **Next**.
4. Select the rule to edit.
5. Click **Advanced Properties** and in the **Custom Error Message** text box, type the error message.

6 To add a link to a URL, in the **Custom Error Link text** text box enter the message to display as the link that sends users to another screen when authentication fails.

   The link is displayed at the end of the custom message. If you do not add a message in the Link text box but add a URL, the link that displays is

   ```
   Continue.
   ```

7 In the **Custom Error Link URL** text box, enter the URL.

8 Click **Save** and then click **Next** and click **Save** again.

What to do next

Create custom error messages for other policy rules.

Create a Policy Rule to Prevent Enrollment Using the Workspace ONE App

The Workspace ONE App is a legacy application and is no longer updated. The Workspace ONE Intelligent Hub app is the app that users now use to enroll their devices into Workspace ONE UEM and to access their company resources.

Admins can block new enrollments from the Workspace ONE app without blocking enrollment through the Workspace ONE Intelligent Hub app. You create an access policy rule for device enrollment through the Workspace ONE Intelligent Hub app and make it the first rule on the default access policy list.

See Configure Device Enrollment Policy Rules for Workspace ONE UEM Enrollments in Workspace ONE Access (Cloud Only).

The legacy Workspace ONE app does not support the Device Enrollment access policy rule. When new users attempt to use the Workspace ONE app to enroll their iOS or Android device, they are denied access and cannot be authenticated. They must use the Workspace ONE Intelligent Hub app to enroll their devices before they can access their resources.

You can configure a custom denial message that displays when they are not authenticated to tell users that they must install the Workspace ONE Intelligent Hub app before they can enroll their device.

The Workspace ONE Intelligent Hub app allows users to authenticate initially using a password and successfully sends the enrollment flag to Workspace ONE UEM. The Mobile SSO policy rule handles subsequent access authentications since the device now has the certificate from the initial enrollment.

Prerequisites

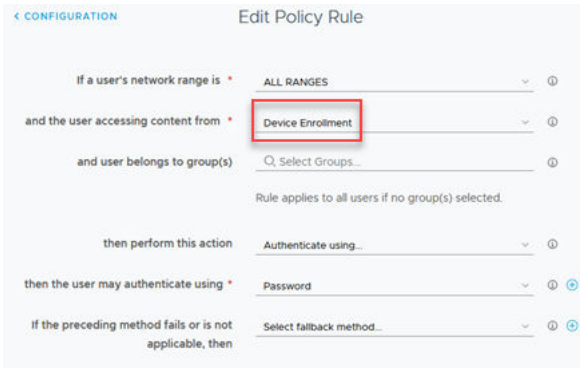
- Workspace ONE Access enabled as the authentication source in Workspace ONE UEM.
- Hub Services configured with the unified Hub catalog.

- Rules for mobile single sign-on for iOS and Android devices are configured in the default access policy.
- Communicate to your users about the end of life for the Workspace ONE app and ask them to install the Intelligent Hub app.

Note Existing users can still log in using the Workspace ONE app.

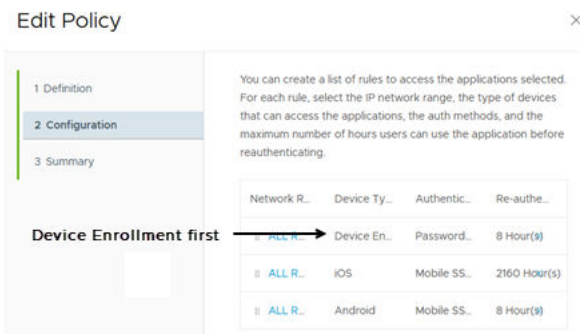
Procedure

1 In the Workspace ONE Access console, navigate to **Manage > Policies** and create the device enrollment rule.



2 Click **Advanced Properties** and in the **Custom Error Message** text box, type an error message that tells users to download the Workspace ONE Intelligent Hub app and try again.

3 On the **Configuration** page, order the rules to make sure that the Device Enrollment rule is listed above the iOS and Android mobile SSO rules.



Results

After the access policy is set up, the new user experience is as follows.

1 Users who try to enroll with the Workspace ONE app are not authenticated because the first rule in the access policy is requesting enrollment with the Intelligent Hub app.

2 User must install the Intelligent Hub app on their device.

3 The first time users use the Intelligent Hub app to sign on, they are authenticated based on the device enrollment policy rule and are asked to enroll their device.

4 The next time they use the Intelligent Hub app to access Workspace ONE, they are authenticated according to the mobile SSO rules.

Create Access Policy for Workspace ONE Out-of-Box Experience Process

To establish the Workspace ONE out-of-box experience (OOBE) after the External Access Token is enabled and added to the built-in identity provider, you must add the External Access Token authentication method to the default access policy set.

Prerequisites

External Access token Authentication enabled as an authentication method for Built-in Identity Providers in the Identity & Access Management > Authentication Methods page.

Procedure

1 In the Workspace ONE Access console, Identity & Access Management tab, select **Manage > Policies**.

2 Click **Edit Default Policy** and then click **Next**.

3 Select the row that lists the **Workspace ONE App** in the Device Type column.

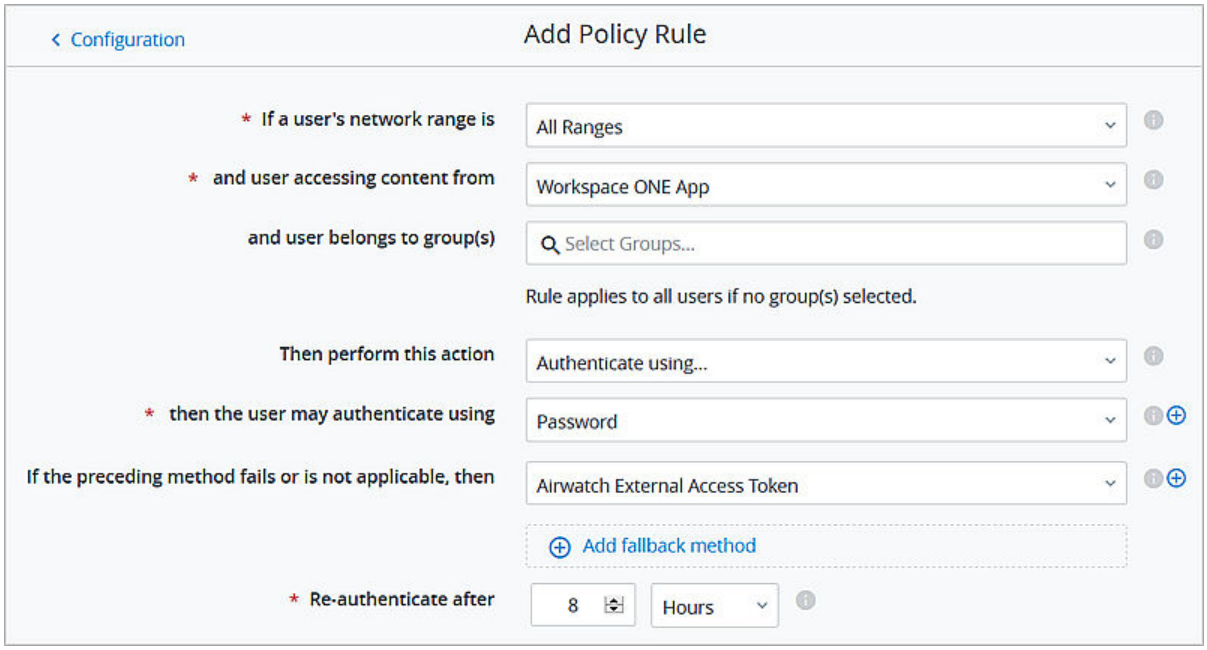
If the Workspace ONE App rule is not listed, click **Add Policy Rule** and create a rule with Workspace ONE App as the device type.

4 Select the authentication methods to use to access the content from the Workspace ONE application.

List the External Access Token authentication method as the last fallback method in the rule. When the External Access Token is detected in the authentication request, the authentication method is honored. Any other authentication methods listed after the External Access Token are not detected.

5 Click **Next** to review the configuration.

6 Click **Save**.



7 On the Configuration page, review the order of the rules in the rules list. If the Workspace ONE app rule is not the first rule in the default access policy list, drag the rule to be the first row in the list.

Workspace ONE App must be the first rule in the default access policy rules list.

8 Click **Next**.

9 Review the Summary page and click **Save**.

Create an Access Policy in Workspace ONE Access for Windows 10 Device Enrollment

When you create an application-specific access policy for Office 365 in the Workspace ONE Access console, to restrict access to Office 365 from only managed Windows 10 devices create a rule using the **Windows 10 Enrollment** as a device type.

You create or update a second access policy rule that uses **Windows 10** as a device type. The rule is configured to authenticates using the Certificate (Cloud Deployment) method with no fallback configured. When users try to access Office 365, if the device is unmanaged, the Office 365 app launch fails, and the Windows 10 Enrollment rule is applied to enroll and manage the device. Uses trying to access Office 365 with a managed device are authenticated based on the second access policy rule.

Prerequisites

- Office 365 configured with the primary identity provider. The primary identity provider can be Workspace ONE Access, Okta, or ADFS. Workspace ONE Access must be configured as the secondary identity provider when Okta or ADFS is the primary identity provider.

- Device enrollment is managed through the Windows 10 Out-of-Box experience (OOBE) or when joining the Azure Active Directory domain.
- Authentication methods configured and enabled for the identity provider.
- Office 365 app added to the Hub catalog.

Procedure

1. In the Workspace ONE Access console Identity & Access Management tab, select **Manage > Policies**.
2. Click **Add Policy**.
3. Add a policy name and description in the respective text boxes.
4. In the **Applies To** section, select the applications that require restricted access.
5. Click **Next**.
6. Click **Add Policy Rule** to add a rule.

Option	Description
If a user's network range is	Select a network range.
and user accessing content from	Select **Windows 10 Enrollment** as the device type.
and user belongs to groups	If this access rule is going to apply to specific groups, search for the groups in the search box. If no group is selected, the access policy rule applies to all users.
Then perform this action	Select **Authenticate using....**
then the user may authenticate using	Select the authentication method to use. **Important** Do not use Certificate (Cloud Deployment). Devices do not have the proper certificate before the device is enrolled. To require users to authenticate through two authentication methods, click + and in the drop-down menu select a second authentication method.
If the preceding methods fails or is not applicable, then	Configure a fallback authentication method, if necessary.
Re-authenticate after	Select the length of the session, after which users must authenticate again.

7. Click **Save**.

What to do next

You can now update the access policy configured for Windows 10 device type. The authentication method selected continues to be Certificate (Cloud deployment), but remove any fallback authentication methods that were configured.