

(Legacy) Setting Up Resources in VMware Workspace ONE Access

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

MAR 2022

VMware Workspace ONE Access

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

<https://docs.vmware.com/>

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

Copyright © 2015 - 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 Setting Up Resources in VMware Workspace ONE Access** 7
- 2 Providing Access to Web Applications in Workspace ONE Access** 10
 - Adding a Web Application to Your Workspace ONE Access Catalog 12
 - Assigning Users and Groups to a Web Application in Workspace ONE Access 16
 - Editing Web Applications in Workspace ONE Access 17
 - Copying a Web Application in Workspace ONE Access 18
 - Exporting and Importing a Web Application in Workspace ONE Access 19
 - Deleting a Web Application from the Workspace ONE Access Catalog 19
 - Managing Categories for Applications in Workspace ONE Access 20
 - Adding Multiple Tenants of Web Apps to Workspace ONE Access 20
 - Adding OpenID Connect Applications to Workspace ONE Access 22
 - Add an OpenID Connect Application to Workspace ONE Access 23
 - Using Provisioning Adapters with Workspace ONE Access 25
 - Managing Web Apps Settings in Workspace ONE Access 26
- 3 Using Virtual Apps Collections in Workspace ONE Access** 27
 - About Workspace ONE Access Virtual Apps Collections 28
 - Creating Virtual Apps Collections in Workspace ONE Access 29
 - Editing Virtual Apps Collections in Workspace ONE Access 31
 - Syncing Virtual Apps Collections in Workspace ONE Access 32
 - Monitoring Virtual Apps Collections in Workspace ONE Access 35
 - Deleting Virtual Apps Collections in Workspace ONE Access 37
 - Configuring Password Caching for Virtual Apps (Workspace ONE Access Cloud Only) 38
- 4 Providing Access to VMware Horizon Desktops and Applications in Workspace ONE Access** 39
 - Deployment Scenario for Integrating Horizon with Workspace ONE Access 40
 - High-Level Horizon-Workspace ONE Access Integration Design 41
 - About Integrating Independent Horizon Pods with Workspace ONE Access 44
 - Requirements for Integrating Horizon Pods with Workspace ONE Access 44
 - About Integrating Horizon Cloud Pod Architecture (CPA) Deployments with Workspace ONE Access 45
 - Requirements for Integrating Horizon Pod Federations with Workspace ONE Access 50
 - Configuring Horizon Pods and Pod Federations in Workspace ONE Access 51
 - Set up Your Workspace ONE Access Environment for Horizon Integration 52
 - Configure Horizon Pods and Pod Federations in Workspace ONE Access 53
 - Configure SAML Authentication in Horizon for Workspace ONE Access Integration 60

- Setting Client Access FQDNs for Horizon Virtual Apps in Workspace ONE Access 61
- Launching Horizon Resources Through Validating Gateways 64
- Viewing Horizon Desktop and Application Pool Information in Workspace ONE Access 66
- Viewing User and Group Assignments for Horizon Desktop and Application Pools in Workspace ONE Access 66
- Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access 67
- Allowing Users to Reset Their Horizon Desktops from the Workspace ONE Catalog 68
- Viewing Launch Options for Horizon Desktops and Applications in Workspace ONE Access 69
- Launching Horizon Desktops and Applications Integrated with Workspace ONE Access 71

- 5 Providing Access to VMware Horizon Cloud Service Desktops and Applications in Workspace ONE Access 73**
 - Integrating Workspace ONE Access with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker or Horizon Cloud Service on IBM Cloud 74
 - Deployment Scenario for Horizon Cloud Integration with Workspace ONE Access 75
 - Integrating Multiple Horizon Cloud Instances with Workspace ONE Access 77
 - Prerequisites for Integrating Workspace ONE Access with Horizon Cloud 78
 - Configure Horizon Cloud Tenant in Workspace ONE Access 80
 - Configure SAML Authentication in the Horizon Cloud Tenant for Workspace ONE Access Integration 83
 - Viewing Horizon Cloud Desktop and Application Pool Information in Workspace ONE Access 85
 - Viewing User and Group Assignments for Horizon Cloud Desktops and Applications 86
 - Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access 87
 - Allowing Users to Reset Horizon Cloud Desktops from the Workspace ONE Catalog 88
 - Launching Horizon Cloud Desktops and Applications Integrated with Workspace ONE Access 88

- 6 Providing Access to VMware ThinApp Packages in Workspace ONE Access 90**
 - Integrating VMware ThinApp Packages with Workspace ONE Access 91
 - Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository 91
 - Create a Network Share for ThinApp Packages 97
 - Configuring ThinApp Packages in Workspace ONE Access 98
 - Entitle Workspace ONE Access Users and Groups to ThinApp Packages 101
 - Distributing and Managing ThinApp Packages 103
 - Offline Grace Period for ThinApp Packages Integrated with Workspace ONE Access 107
 - Updating Managed ThinApp Packages After Deployment in Workspace ONE Access 107
 - Update a ThinApp Package Managed by Workspace ONE Access 109
 - Obtain the AppID and VersionID values of a Managed ThinApp Package 109
 - Create the Updated ThinApp Package 110
 - Copy an Updated ThinApp Package to the Network Share 112
 - Make Existing ThinApp Packages Compatible with Workspace ONE Access 114
 - Change the ThinApp Packages Share Folder in Workspace ONE Access 116

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access 117

7 Configuring Workspace ONE Access Desktop 118

Command-Line Installer Options for Workspace ONE Access Desktop 119

Install the Windows Application with Identical Settings to Multiple Systems 124

Add Workspace ONE Access Desktop Installer Files to Workspace ONE Access Virtual Appliances 125

Using the Workspace ONE Access Command-Line hws-desktop-ctrl.exe Application 126

8 Providing Access to Citrix-Published Resources in VMware Workspace ONE Access 128

Components Required for Citrix Integration with Workspace ONE Access 131

Synchronization of Citrix-published Resources and Assignments to Workspace ONE Access 132

Launch of Citrix-published Applications and Desktops Integrated with Workspace ONE Access 133

Configuring Citrix Server Farms in Workspace ONE Access 136

Configuring Citrix Resource Launch in Workspace ONE Access 140

Configuring Citrix Resource Launch for Internal Networks in Workspace ONE Access 141

Configuring Citrix Resource Launch for External Networks with NetScaler Gateway 142

Configure Network Range for NetScaler Gateway in Workspace ONE Access 143

Configuring Workspace ONE Access Settings for Citrix Integration 144

Managing Categories for Citrix-Published Resources Integrated with Workspace ONE Access 144

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access 145

Viewing User and Group Assignments for Citrix-Published Resources in Workspace ONE Access 146

Launching Citrix-Published Resources Integrated with Workspace ONE Access 147

9 Providing Access to Third-Party Managed Applications in Workspace ONE Access 149

Add an Application Source to Workspace ONE Access Catalog 150

Entitle Users to the Application Source in Workspace ONE Access 151

Add Applications Managed by the Application Source to Workspace ONE Access 152

10 Troubleshooting Workspace ONE Access Resource Configuration 154

Troubleshooting Launch Errors in Workspace ONE Access 154

Troubleshooting ThinApp Integration with Workspace ONE Access 154

Troubleshooting VMware Horizon Integration with Workspace ONE Access 157

Troubleshooting Citrix-Published Resources Integration with Workspace ONE Access 158

Resource Not Available Error while Launching XenApp 7.x Desktops 158

Unable to Launch Desktop from Citrix XenDesktop Farm on Windows 7 159

Sync Issues if Published Applications or Desktops in a Site Do Not Contain Valid Users 159

Citrix Entitlements do not Appear in Workspace ONE Access 159

Citrix Delivery Groups Not Synced to Workspace ONE Access 160

Setting Up Resources in VMware Workspace ONE Access

1

You can integrate Web apps and Virtual Apps with VMware Workspace ONE® Access™ (formerly known as VMware Identity Manager™) to make these apps and desktops available to end users in the VMware Workspace ONE® Intelligent Hub app and portal. Workspace ONE Access provides multi-factor authentication, conditional access, and single sign-on to the apps.

You can integrate the following types of resources with Workspace ONE Access:

- Web apps
- Virtual apps
 - VMware Horizon® applications and desktops
 - Citrix-published resources
 - VMware Horizon® Cloud Service™ applications and desktops

See [Chapter 5 Providing Access to VMware Horizon Cloud Service Desktops and Applications in Workspace ONE Access](#) for information on the types of Horizon Cloud Service environments supported.

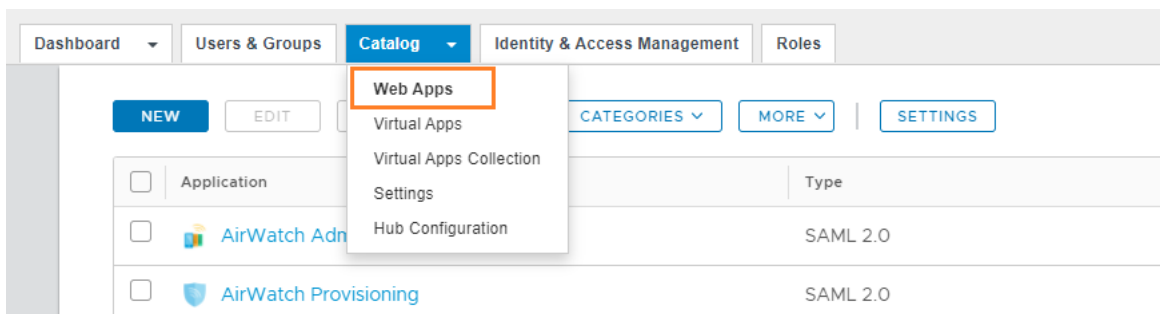
- VMware ThinApp® packaged applications

Note Integration with ThinApp packaged applications is only supported with the legacy VMware Identity Manager connector (Linux) version 2018.8.1.0.

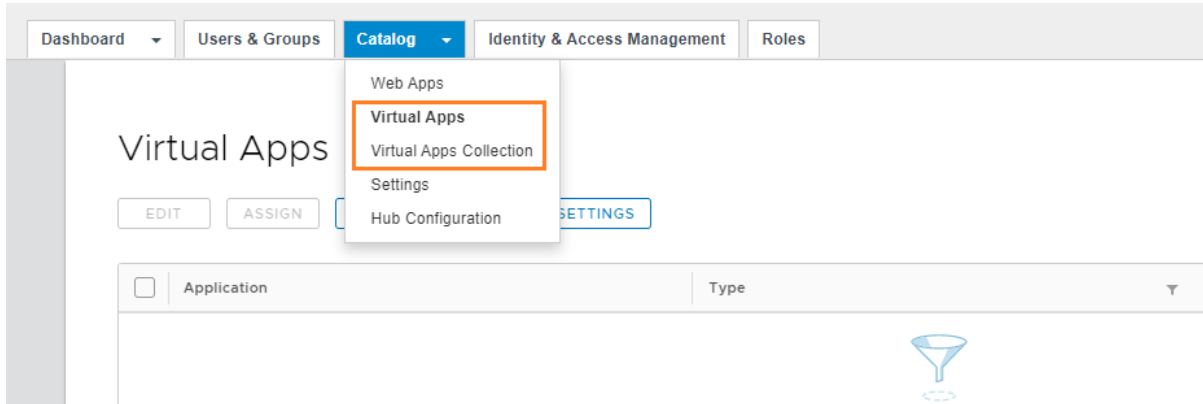
Except for Web applications, each resource type requires you to integrate Workspace ONE Access with another product or component.

You integrate these resources from the **Catalog** tab in the Workspace ONE Access console.

- To integrate Web applications, you use the **Catalog > Web Apps** tab.



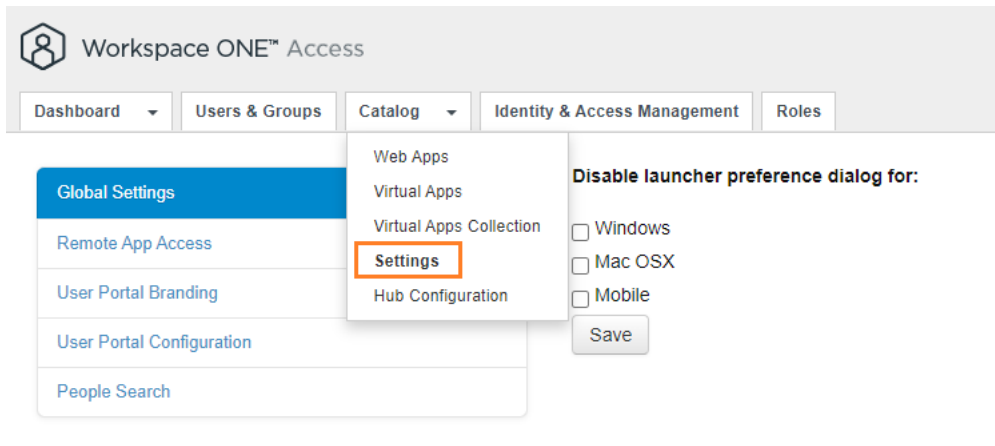
- To integrate and manage Horizon desktops and applications, Citrix-published resources, or ThinApp packaged applications, you use the **Catalog > Virtual Apps Collections** and **Catalog > Virtual Apps** tabs. You configure the integrations in the **Catalog > Virtual Apps Collections** page and view the synced resources in the **Catalog > Virtual Apps** page.



- To integrate Horizon Cloud, you either use the Horizon Cloud console or configure virtual apps collections in Workspace ONE Access, based on the type of Horizon Cloud environment that you have.

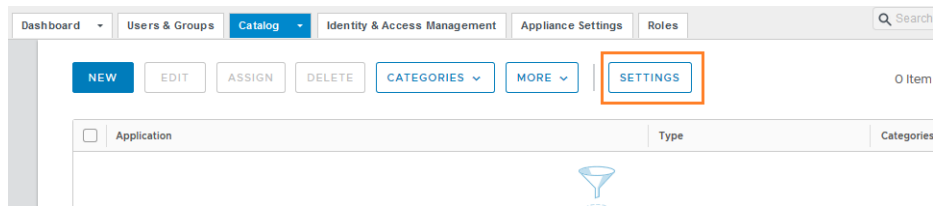
You can manage settings for integrated resources from the following pages.

- Global settings are available on the **Catalog > Settings** tab.

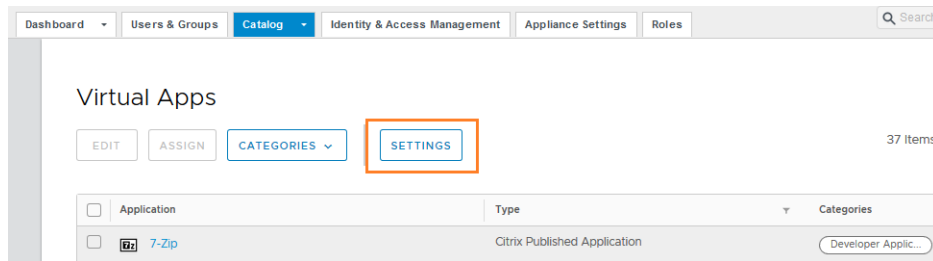


For information about global settings, see the *VMware Workspace ONE Access Administration* guide.

- Settings for Web applications are available from the **Settings** button on the **Catalog > Web Apps** tab.



- Settings for Horizon, ThinApp, and Citrix-published resources are available from the **Settings** button on the **Catalog > Virtual Apps** tab.



You can also manage settings for individual applications by clicking the application in the **Catalog > Web Apps** or **Catalog > Virtual Apps** page and clicking **Edit**.

Providing Access to Web Applications in Workspace ONE Access

2

You can add Web applications to the Workspace ONE Access catalog and assign them to users and groups to provide users access to these applications from the Workspace ONE Intelligent Hub app and portal. You configure single sign-on (SSO) to the applications by using a federation protocol such as SAML 2.0 to configure the applications.

Access policies can be applied on the applications to control user access based on criteria such as the user's network range or device type. You can create access policies for a single application, a set of applications, or all applications in your catalog. When you add an application to the catalog, you select the access policy to use.

You can also set up an approval flow so that users must request access to an application and the request must be approved before they can use the application.

The following types of Web applications can be added to the catalog:

- SAML 2.0 applications
- SAML 1.1 applications
 - SAML 1.1 is an older SAML authentication standard. For better security, implement SAML 2.0.
- WS-Federation 1.2 (supported for Office 365 only)
- OpenID Connect applications
- Applications that do not use a federation protocol
- Applications associated with third-party identity providers such as Okta, Ping, and ADFS.
 - To add these applications, you must first configure the third-party identity provider as an application source in Workspace ONE Access. See

[Chapter 9 Providing Access to Third-Party Managed Applications in Workspace ONE Access](#) for information.

Before setting up Web applications in the catalog, take into account the following considerations.

- If you configure the Web application to use a federation protocol, use a supported protocol. Configuring the Web application to use a federation protocol is not a requirement.
- The users you plan to entitle to the Web application must be registered users of that application, or you plan to configure the provisioning adapter for the application, if available, to provision Workspace ONE Access users in the application.

- If the Web application is a multitenant application, the service points to your instance of the application.

Role Requirements for Managing Web Applications

The following roles can manage Web applications:

- Super Admin
- Custom administrator role that has the following configuration:

Service: Catalog

Actions: Manage Web Applications, Manage App Sources, Manage Third-Party Apps, as applicable

Resources: All resources or specific resources as applicable

To assign applications to users and groups, the role must include the Manage Entitlements action.

For more information about roles, see "Managing Administrator Roles" in *VMware Workspace ONE Access Administration*.

Additional Information on Integrating Specific Web Applications

In addition to the information in this document, instructions on configuring SAML-based single sign-on from Workspace ONE Access to specific Web applications, such as Office 365 and Google Apps, are available. See [VMware Workspace ONE Access Integrations Documentation](#).

Information on provisioning adapters is included in those documents, if applicable.

This chapter includes the following topics:

- [Adding a Web Application to Your Workspace ONE Access Catalog](#)
- [Assigning Users and Groups to a Web Application in Workspace ONE Access](#)
- [Editing Web Applications in Workspace ONE Access](#)
- [Copying a Web Application in Workspace ONE Access](#)
- [Exporting and Importing a Web Application in Workspace ONE Access](#)
- [Deleting a Web Application from the Workspace ONE Access Catalog](#)
- [Managing Categories for Applications in Workspace ONE Access](#)
- [Adding Multiple Tenants of Web Apps to Workspace ONE Access](#)
- [Adding OpenID Connect Applications to Workspace ONE Access](#)
- [Using Provisioning Adapters with Workspace ONE Access](#)
- [Managing Web Apps Settings in Workspace ONE Access](#)

Adding a Web Application to Your Workspace ONE Access Catalog

You can add Web applications to your Workspace ONE Access catalog by either selecting applications from the cloud application catalog or creating new applications. You can then assign these applications to users so that they can access their applications from the Workspace ONE Intelligent Hub app and portal.

The cloud application catalog contains commonly-used enterprise Web applications. These applications are partially configured and you must provide additional information to complete the application record. You might also need to work with your Web application account representatives to complete other required setup.

Many of the applications in the cloud application catalog use SAML 2.0 or 1.1 to exchange authentication and authorization data to enable single sign-on from Workspace ONE to the Web application.

When you create a new application, you need to enter all the configuration information for the application. The configuration varies based on the type of application you are adding. For applications with no federation protocol, you only require a Target URL.

Applications from any third-party identity providers that you have configured as application sources in Workspace ONE Access are added as new applications.

While adding an application, you also select an access policy to control user access to the application. A default access policy is available and you can also create new ones from the **Identity & Access Management > Manage > Policies** page. See *Workspace ONE Access Administration* for information about access policies.

Prerequisites

- Obtain the configuration information for the application.
- Create an access policy if you do not want to use the default access policy. You can create access policies from the **Identity & Access Management > Manage > Policies** page.
- Create categories if you want to group applications into categories. A predefined Recommended category is available. You can create categories from the **Catalog > Web Apps** page by clicking **Categories** and typing the category name in the text box.
- Create or sync user groups, if required.

For users that are synced from your enterprise directory, you create groups in the enterprise directory and sync them to Workspace ONE Access. To update the list of groups to sync, go to the **Identity & Access Management > Manage** page, select the directory, click **Sync Settings**, and select the **Groups** tab.

For local users, you can create groups from the **Users & Groups > Groups** tab.

Procedure

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

2 Click **New**.

The New SaaS Application wizard appears.

3 On the **Definition** page, select an application from the cloud application catalog or create a new one.

- To select an application from the cloud application catalog, either type its name in the search box or click "**or browse from catalog**" and select it from the list of applications.

The fields on the Definition and Configuration pages are partially populated.

- To create a new application, enter its name in the **Name** field.

Important To add Office 365 applications, select them from the cloud application catalog.

4 Complete the remaining fields on the **Definition** page.

Option	Description
Name	Enter a unique name for the application.
Description	(Optional) Enter a description of the application.
Icon	(Optional) Upload an icon for the application. Icons in PNG, JPG, and ICON file formats, up to 4MB, are supported. The icon must be a minimum of 180 x 180 pixels. If the icon is too small, it does not display. In that case, the Workspace ONE icon is displayed.
Category	(Optional) To add the application to a category, select it from the drop-down menu. Categories must already be created. A predefined Recommended category is available. Select this category if you want the application to appear in the Recommended list of apps in the Workspace ONE Intelligent Hub app and portal. (Legacy Workspace ONE app and portal only) If you want the app to appear in users' Bookmarks tab, select the Recommended category and in the Catalog > Settings > User Portal Configuration page, select Show recommended apps in Bookmarks tab .

5 Click **Next**.

6 On the **Configuration** page, enter the application configuration details.

For applications that are added from the cloud application catalog, some fields are pre-populated with information specific to each Web application. Some of the pre-populated items are editable, while others are not. The information required varies from application to application.

For applications that are being added as new applications, the fields vary based on the authentication type you select.

For information about specific fields, click the information icon next to the field.

Option	Description
Single Sign-On	<p>Authentication Type</p> <p>For applications that are added from the cloud application catalog, the authentication type is preselected. For new applications, select the authentication type if applicable. If the application does not use a federation protocol, select Web Application Link.</p> <p>The following options are available:</p> <ul style="list-style-type: none">■ SAML 2.0 If the Web application supports SAML 2.0, an XML-based standard for the secure exchange of authentication and authorization information, select this option to enable single sign-on from Workspace ONE Access to the application.■ SAML 1.1 If the Web application supports SAML 1.1, select this option to enable single sign-on from Workspace ONE Access to the application.■ WSFed 1.2 (Supported for Office 365 only) Do not select the WSFed 1.2 option while creating a new Web application. The WS-Federation 1.2 authentication type is only supported for Office 365 applications. To add Office 365 applications, select them from the cloud application catalog. The authentication type will be preselected.■ OpenID Connect If the application supports OpenID Connect, an authentication protocol based on the OAuth 2.0 protocol, select this option to enable single sign-on from Workspace ONE Access to the application.■ Any third-party identity providers configured as application sources in Workspace ONE Access, for example, Okta. Select this option to add an application from an application source. Application sources appear in the list only if they are already configured in the Web Apps Settings page. When you select an application source, you only need to enter the target URL of the application as the rest of the configuration is already completed in the application source.■ Web Application Link Select this option if the application does not use a federation protocol. You only need to enter the target URL of the application. You must enter a valid URL that starts with http:// or https://. <p>Configuration</p> <p>The fields that appear vary based on the selected authentication type. Click the information icon for a description of each field.</p> <p>If you selected an application source or Web Application Link, you only need to enter the target URL of the application. For Web Application Link, you must enter a valid URL that starts with http:// or https://.</p>
Application Parameters	<p>For applications added from the cloud application catalog, parameters may be listed. If a parameter is listed and does not have a default value, enter a value to allow the application to launch. If a default value is provided, you can edit the value.</p>

Option	Description
	<p>For new applications, add the required parameters.</p> <hr/> <p>Note This section does not appear when OpenID Connect, an application source, or Web Application Link is selected as the authentication type.</p>
Advanced Properties	<p>Advanced properties include options to sign and encrypt SAML assertions and responses, and an option to enable authentication failure notification to send a SAML response to the service provider when authentication fails. The properties you can configure vary based on the selected authentication type. Click the information icon for a description of each field.</p> <hr/> <p>Note This section does not appear when OpenID Connect, an application source, or Web Application Link is selected as the authentication type.</p>
Open in VMware Browser	<p>Select this option if you want the Intelligent Hub app to open the application in the VMware Browser, which provides a secure alternative to the native Web browser.</p>

7 Click **Next**.

8 On the **Access Policies** page, select the access policy to manage user access to the application.

The default_access_policy_set is selected by default.

9 On the **Summary** page, review your selections and click **Save**, or click **Save & Assign** to assign the application to users and groups.

If you do not assign the application to any users and groups at this time, you can do so later by selecting the application in the **Catalog > Web Apps** page and clicking **Assign**.

10 If you clicked **Save & Assign**, assign the application to users and groups.

a Add users and groups by typing the name in the search box and selecting from the results.

b Select the deployment type for each user and group.

Regardless of whether you select **User Activated** or **Automatic**, the application appears in the Apps tab in the Intelligent Hub app or portal. Users can run the application from the Apps tab or mark it as favorite and run it from the Favorites tab. If you plan to set up an approval flow for the application, select **User Activated**.

c Click **Save**.

Results

The application is added to the catalog and appears in the list of applications in the **Catalog > Web Apps** tab.

Assigning Users and Groups to a Web Application in Workspace ONE Access

After you add Web applications to your Workspace ONE Access catalog, you can assign them to users and groups. Users can view and launch the applications from the Workspace ONE Intelligent Hub portal or app.

If you remove a user's entitlement to an application, the user cannot see or launch the application.

In many cases, the most effective way to entitle users is to assign Web applications to a group of users.

Note You can assign an application to only 50 users or groups. To assign it to more users or groups, add the users or groups to an existing group.

Prerequisites

Create or sync user groups, if required.

For users that are synced from your enterprise directory, you create groups in the enterprise directory and sync them to Workspace ONE Access. To update the list of groups to sync, go to the **Identity & Access Management > Manage** page, select the directory, click **Sync Settings**, and select the **Groups** tab.

For local users, you can create groups from the **Users & Groups > Groups** tab.

Procedure

- 1 Log in to the Workspace ONE Access console.

2 Entitle users to a Web application.

Method	Description
Access a Web application and assign it to users or groups	<ul style="list-style-type: none">a Select the Catalog > Web Apps tab.b Click the Web application.c Click Assign.d Select users and groups by typing the name in the search box and selecting from the results.e Select the deployment type for each user and group. Regardless of whether you select User Activated or Automatic, the application is added to the Apps tab in the Intelligent Hub app and portal. Users can run the application from the Apps tab or mark it as favorite to run it from the Favorites tab. However, if you want to set up an approval flow for the application, select User Activated.f Click Save.
Access a user or group and add Web application entitlements to that user or group.	<ul style="list-style-type: none">a Click the Users & Groups tab.b Click the Users tab or the Groups tab.c Click the name of a user or group.d Click the Apps tab, then click Add Entitlement.e In the Application Type drop-down list, select Web Applications.f Select the check boxes next to the Web applications to which you want to entitle the user or group.g In the DEPLOYMENT column, select how to activate each Web application. Regardless of whether you select User Activated or Automatic, the application is added to the Apps tab in the Intelligent Hub app and portal. Users can run the application from the Apps tab or mark it as favorite to run it from the Favorites tab. However, if you want to set up an approval flow for the application, select User Activated.h Click Save.

Results

The selected user or group is now entitled to use the Web application.

Editing Web Applications in Workspace ONE Access

You can edit Web applications that you have added to your Workspace ONE Access catalog to change the application definition, configuration, access policy, or user assignments. Edit applications from the **Catalog > Web Apps** tab in the Workspace ONE Access console.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click the application you want to edit.
- 3 Click **Edit**.

- 4 Follow the Edit SaaS Application wizard to modify the application as required.

The process is the same as creating a new application. See [Adding a Web Application to Your Workspace ONE Access Catalog](#).

Copying a Web Application in Workspace ONE Access

You can make a copy of a Web application in your Workspace ONE Access catalog and modify it to create a new application. Copying an application is useful when you want to add another application with a similar configuration or when you are adding multiple tenants of an application.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click the application you want to copy.
- 3 Click **Copy**.
- 4 Follow the Copy SaaS Application wizard to configure the new application.
 - a Ensure that you enter a new name for the copied application. By default, the name is changed to ***applicationName_Copy***.
 - b Modify the configuration as required.

The process is the same as creating a new application. See [Adding a Web Application to Your Workspace ONE Access Catalog](#).
 - c Click **Save**.
- 5 On the **Summary** page, review your selections and click **Save**, or click **Save & Assign** to assign the application to users and groups. User and group assignments from the original application are not copied to the new application.

If you do not assign the application to any users and groups at this time, you can do so later by selecting the application in the **Catalog > Web Apps** page and clicking **Assign**.

- 6 If you clicked **Save & Assign**, assign the application to users and groups.
 - a Add users and groups by typing the name in the search box and selecting from the results.
 - b Select the deployment type for each user and group.

Regardless of whether you select **User Activated** or **Automatic**, the application is added to the Apps tab in the Intelligent Hub app and portal. Users can run the application from the Apps tab or mark it as favorite to run it from the Favorites tab. However, if you want to set up an approval flow for the application, select **User Activated**.
 - c Click **Save**.

Exporting and Importing a Web Application in Workspace ONE Access

When you have added a Web application to your Workspace ONE Access catalog, you can export it from one Workspace ONE Access instance and import it into another instance. For example, you can import an application from your staging environment into your production environment without having to recreate the application.

This process involves exporting the application bundle from one Workspace ONE Access instance and importing it into the other. The application might not require any changes in Workspace ONE Access, especially if you thoroughly tested it in the original environment. However, you must update the application configuration at the service provider end to specify the new Workspace ONE Access environment details, such as the identity provider URL and SAML metadata.

Procedure

- 1 Log in to the console of the Workspace ONE Access instance from which to export a Web application.
- 2 Select the **Catalog > Web Apps** tab.
- 3 Click the application you want to export.
- 4 Click **Export**.

The application bundle is downloaded to your system as a zip file.

- 5 Log in to the console of the Workspace ONE Access instance in which to import the Web application.
- 6 Select the **Catalog > Web Apps** tab.
- 7 Click **More > Import**.
- 8 Select the application zip file and click **Open**.

The application is uploaded.

Deleting a Web Application from the Workspace ONE Access Catalog

You can delete Web applications from the Workspace ONE Access catalog that you no longer need to provide to your users. When you delete an application, it is no longer available to any user in the Workspace ONE Intelligent Hub app or portal.

To add the application back, you will need to recreate it in the catalog.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click the application you want to delete.

- 3 Click **Delete**.

Managing Categories for Applications in Workspace ONE Access

You can group Web applications that are in your Workspace ONE Access catalog into categories to make it easier for users to find the applications in the Intelligent Hub app or portal. For example, you can create a category named Benefits and assign your payroll, insurance, and 401K applications to it.

In addition to any categories that you create, a predefined **Recommended** category is also available. Select this category for applications that you want to add to the Recommended apps list in the Workspace ONE Intelligent Hub app and portal.

(Legacy Workspace ONE app and portal only) You can also use the **Recommended** category to place specific applications directly in users' Bookmarks pages. You do this by selecting the **Recommended** category for the applications and then selecting **Show recommended apps in Bookmarks** in the **Catalog > Settings > User Portal Configuration** page.

You can select categories for applications in various ways.

- Select categories while adding an application to the catalog, if the categories are already created.
- Edit an application to select categories.
- Apply categories to multiple applications at the same time from the **Catalog > Web Apps** tab.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click **Categories**.
- 3 In the text box that appears, type a name for the new category and select **Add Category** *newCategoryName*.
- 4 Assign applications to the category.
 - a In the **Catalog > Web Apps** tab, select the applications you want to add to the category.
 - b Click the **Categories** drop-down menu and select the category you created.

Adding Multiple Tenants of Web Apps to Workspace ONE Access

Workspace ONE Access supports adding multiple tenants of a service provider to a Workspace ONE Access instance. If you have multiple tenants of an app such as Office 365 that might be used by different lines of business in your organization, you can add all the tenants to a single instance of Workspace ONE Access. This enables you to manage SSO and access to all the tenants from one location.

To add multiple tenants, you add multiple copies of the app to the Workspace ONE Access catalog and then modify the configuration of each. Map each copy of the app to a different tenant of the service provider. Each tenant can have one or more domains. You also need to entitle users to the appropriate copy of the app.

When users log into the Workspace ONE Intelligent Hub app or portal and click the app to which they are entitled, the correct app is launched. When users log into the service provider directly, the service provider redirects to Workspace ONE Access for authentication and Workspace ONE Access authenticates the user and launches the correct app based on user entitlements.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click **New**.
- 3 Select the app from the cloud application catalog by either typing its name in the search box or clicking "**browse from the catalog**" and selecting it.

The fields on the Definition and Configuration pages are partially populated.

- 4 Follow the wizard to configure the app and click **Save**.
- 5 Create a copy of the app by doing one of the following:
 - Create a new app by clicking **New** in the **Catalog > Web Apps** page and adding the app from the cloud application catalog.
 - Copy the app by clicking the app in the **Catalog > Web Apps** page, then clicking **Copy**. Edit fields such as the name and description so that the new app can be easily identified.
- 6 Configure each copy of the app for the appropriate tenant.
 - Map each copy of the app to a different service provider tenant.
 - Ensure that users are unique across all service provider domains and tenants.

Note If the users are not unique, ensure that the service provider POST URLs, that is, the Assertion Consumer Service URLs that you enter in the Workspace ONE Access console, are unique across tenants.

- 7 Configure user entitlements for each copy of the app. Entitle users to the appropriate tenant.
 - a In the **Catalog > Web Apps** tab, click the copy of the app that corresponds to the tenant.
 - b Click **Assign**.
 - c Select users and groups by typing the names in the search box and selecting from the results.

- d Select the deployment type for each user and group.

Regardless of whether you select the User Activated or Automatic option, the application is added to the Apps page in the Intelligent Hub app and portal. Users can run the application from the Apps page or mark it as a favorite and run it from the Favorites page. However, if you want to set up an approval flow for the app, you must select User Activated for the app.

- e Click **Save**.

Adding OpenID Connect Applications to Workspace ONE Access

You can add applications that use the OpenID Connect authentication protocol to the Workspace ONE Access catalog and manage them like any other application in the catalog. You can apply an access policy to each application to specify how users are authenticated based on criteria such as network range and device type. After you add the application, you assign it to users and groups.

To add an OpenID Connect application, you specify the application's target URL, redirect URL, client ID, and client secret.

When you add an OpenID Connect application to the catalog, an OAuth 2.0 client is automatically created in Workspace ONE Access for the application. The client is created with the configuration information you specify while adding the application, which includes the target URL, redirect URL, client ID, and client secret. All other parameters use default values. These include:

- Grant type: authorization_code, refresh_token
- Scope: admin, openid, user
- Display user grant: false
- Access token time-to-live (TTL): 3 hours
- Refresh token time-to-live (TTL): Enabled and set to 90 days
- Refresh token idle time-to-live (TTL): 4 days

You can view the OAuth 2.0 client for the application on the **Clients** tab of the Remote App Access page. Select the **Catalog > Settings** tab, click **Remote App Access** in the left pane, and click the client ID to view the configuration information.

Caution Do not delete the OAuth 2.0 client associated with the application or the application will no longer be available to users.

When you delete the application from the catalog, the OAuth 2.0 client is also deleted.

Authentication Flow when Application is Accessed from Workspace ONE

When a user clicks the application in Workspace ONE, the authentication flow is as follows:

- 1 The user clicks the application in Workspace ONE.
- 2 Workspace ONE Access redirects the user to the target URL.
- 3 The application redirects the user to Workspace ONE Access with an authorization request.
- 4 Workspace ONE Access authenticates the user based on the authentication policy that you specified for the application.
- 5 Workspace ONE Access checks whether the user is entitled to the application.
- 6 Workspace ONE Access sends the authorization code to the redirect URL.
- 7 Using the authorization code, the application requests the access token.
- 8 Workspace ONE Access sends the ID token, access token, and refresh token to the application.

Authentication Flow when Application is Accessed Directly from Service Provider

When a user accesses the application directly from the service provider, the authentication flow is as follows:

- 1 The user clicks the application.
- 2 The user is redirected to Workspace ONE Access for authentication.
- 3 Workspace ONE Access authenticates the user based on the authentication policy that you specified for the application.
- 4 Workspace ONE Access checks whether the user is entitled to the application.
- 5 Workspace ONE Access sends an ID token to the service provider.

Add an OpenID Connect Application to Workspace ONE Access

You can add applications that use the OpenID Connect authentication protocol to the Workspace ONE Access catalog from the **Catalog > Web Apps** tab. To add an OpenID Connect application, you need the application's target URL, redirect URL, client ID, and client secret.

Prerequisites

- Obtain the target URL, redirect URL, client ID, and client secret for the application.
- Create an access policy if you do not want to use the default access policy. You can create access policies from the **Identity & Access Management > Manage > Policies** page.
- Create categories, if required. You can create categories from the **Catalog > Web Apps** page by clicking **Categories** and typing the category name in the text box.

- Create user groups, if required. You can create groups from the **Users & Groups > Groups** tab.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Web Apps** tab.
- 2 Click **New**.
- 3 In the Definition page of the New SaaS Application wizard, enter the required information.

Option	Description
Name	Enter a unique name for the application.
Description	(Optional) Enter a description of the application.
Icon	(Optional) Upload an icon for the application. Icons in PNG, JPG, and ICON file formats, up to 4MB, are supported. The icon must be a minimum of 180 x 180 pixels. If the icon is too small, it does not display. In that case, the Workspace ONE icon is displayed.
Category	(Optional) To add the application to a category, select it from the drop-down menu. Categories must already be created. A predefined Recommended category is also available. Select this category if you want the application to appear in the Recommended apps list in the Workspace ONE Intelligent Hub app and portal. (Legacy Workspace ONE app and portal only) If you want the app to appear in the users' Bookmarks page, select the Recommended category and in the Catalog > Settings > User Portal Configuration page, select Show recommended apps in Bookmarks tab .

- 4 Click **Next**.
- 5 In the Configuration page, enter the required configuration information.

Option	Description
Authentication Type	Select OpenID Connect.
Target URL	The application URL to which users will be sent when they click the app in the Intelligent Hub app or portal.
Redirect URL	The URL to which Workspace ONE Access will send the authorization code.
Client ID	The Client Identifier that the app will include in the authentication requests made to Workspace ONE Access. The Client ID must be unique per tenant.
Client Secret	The secret that the app will use to identify itself in the authentication requests made to Workspace ONE Access.
Open in VMware Browser	Select this option if you want the Intelligent Hub app to open the application in the VMware Browser, which provides a secure alternative to the native Web browser.

- 6 Click **Next**.

- 7 In the Access Policies page, select the access policy to manage user access to the application
The default_access_policy_set is selected by default. For information about creating and managing access policies, see *Workspace ONE Access Administration*.
- 8 On the Summary page, review your selections and click **Save**, or click **Save & Assign** to assign the application to users and groups.

If you do not assign the application to any users and groups at this time, you can do so later by selecting the application in the **Catalog > Web Apps** page and clicking **Assign**.
- 9 If you clicked **Save & Assign**, assign the application to users and groups.
 - a Add users and groups by typing the name in the search box and selecting from the results
 - b Select the deployment type for each user and group.

Regardless of whether you select **User Activated** or **Automatic**, the application appears in the Apps tab in the Intelligent Hub app and portal. Users can run the application from the Apps tab or mark it as a favorite and run it from the Favorites tab. If you plan to set up an approval flow for the application, select **User Activated**.
- 10 Click **Save**.
- 11 To enable additional scopes, such as Email or Profile, or to edit attributes such as token Time-To-Live (TTL) on the OAuth 2.0 client that was created for the application, follow these steps.
 - a Select the **Catalog > Settings** tab.
 - b Click **Remote App Access**.
 - c Find the client for the application based on the **Client ID** that you entered in step 5, and click the link.
 - d To edit the scope, click **Edit** in the **SCOPE** box, make your changes, and click **Save**.
 - e To edit other attributes, click **Edit** in the **CLIENT CONFIGURATION** box, make your changes, and click **Save**.

Results

The application is added to the catalog. To edit the application configuration at any time, select the application in the **Catalog > Web Apps** page and click **Edit**.

Using Provisioning Adapters with Workspace ONE Access

Provisioning provides automatic application user management from a single location. Provisioning adapters allow Web applications to retrieve specific information from the Workspace ONE Access service as required. For example, when automatic user provisioning to Google Apps is enabled, required user account information, such as the user name, first name, and last name can be retrieved from the Workspace ONE Access service.

If provisioning is enabled for a Web application, when you entitle a user to the application in the Workspace ONE Access service, the user is provisioned in the Web application.

You configure the provisioning adapter for an application when you add the application to the catalog from the **Catalog > Web Apps** tab.

The Workspace ONE Access service currently includes provisioning adapters for the following applications:

- Google Apps
- Office 365
- Socialcast

Managing Web Apps Settings in Workspace ONE Access

Settings for Web applications are available on the **Catalog > Web Apps > Settings** page in the Workspace ONE Access console. You can set up an approval flow for applications, manage SAML metadata, and configure third-party identity providers as application sources.

Setting	Description
Approvals	<p>When you set up approvals, users need to request access to applications before they can use the applications from the catalog.</p> <p>For information about setting up approvals, see <i>Workspace ONE Access Administration</i>.</p>
SAML Metadata	<p>You can download the self-signed Workspace ONE Access SAML signing certificate and SAML metadata from the Download SAML Metadata tab. If you want to obtain a certificate from a third-party Certificate Authority (CA), you can generate a Certificate Signing Request (CSR) from the Generate CSR tab, obtain the certificate, and upload it on the same tab.</p> <p>For more information about managing SAML metadata, see "Managing the Catalog" in <i>Workspace ONE Access Administration</i>.</p>
Application Sources	<p>You can configure certain third-party identity providers such as OKTA or ADFS as application sources and then add the associated applications to the catalog.</p> <p>For information about setting up application sources, see Chapter 9 Providing Access to Third-Party Managed Applications in Workspace ONE Access.</p>

Using Virtual Apps Collections in Workspace ONE Access

3

In addition to Web applications, you can integrate VMware Horizon applications and desktops, Citrix-published applications and desktops, and ThinApp packaged applications with Workspace ONE Access to provide end users access to these resources from the Workspace ONE Intelligent Hub app or portal. To integrate these resources, you create virtual apps collections in the Workspace ONE Access console.

To create and manage all types of virtual apps collections except ThinApp, you must install the Virtual App service, which is a component of Workspace ONE Access Connector 21.08 and later. See [Installing Workspace ONE Access Connector 21.08](#) for information.

If you are upgrading from Workspace ONE Access Connector 19.03, a migration path is available to migrate your existing Horizon on-premises and Citrix virtual apps collections to the Virtual App service. Migration is not available for ThinApp integrations. See [Migrating to VMware Workspace ONE Access Connector 21.08](#) for information.

Note

- Integration with ThinApp packaged applications is only supported with the legacy VMware Identity Manager connector (Linux) version 2018.8.1.0. The Virtual App service does not support ThinApp integration.
- You can also integrate Horizon Cloud with Workspace ONE Access to make Horizon Cloud applications and desktops available in the Intelligent Hub app and portal. See [Chapter 5 Providing Access to VMware Horizon Cloud Service Desktops and Applications in Workspace ONE Access](#) for information on the types of Horizon Cloud environments supported and how they are integrated with Workspace ONE Access. The Virtual App service is not required for any Horizon Cloud integration.

This chapter includes the following topics:

- [About Workspace ONE Access Virtual Apps Collections](#)
- [Creating Virtual Apps Collections in Workspace ONE Access](#)
- [Editing Virtual Apps Collections in Workspace ONE Access](#)
- [Syncing Virtual Apps Collections in Workspace ONE Access](#)
- [Monitoring Virtual Apps Collections in Workspace ONE Access](#)
- [Deleting Virtual Apps Collections in Workspace ONE Access](#)

- [Configuring Password Caching for Virtual Apps \(Workspace ONE Access Cloud Only\)](#)

About Workspace ONE Access Virtual Apps Collections

To integrate Horizon desktops and applications, Citrix-published resources, and ThinApp packaged applications with the Workspace ONE Access service, you create virtual apps collections. All these types of integrations except ThinApp require you to install the Virtual App service, which is a component of Workspace ONE Access connector 21.08 and later.

Note Integration with ThinApp packaged applications is only supported with the legacy VMware Identity Manager connector (Linux) version 2018.8.1.0.

A virtual apps collection contains the configuration information for an integration, including the type of resource, the servers from which to sync resources, the Virtual App service instance to use for sync, and the sync schedule.

You can create a single virtual apps collection or multiple collections for any type of resource except ThinApp packages for which you can only create a single collection. For example, to integrate a deployment of two Citrix XenApp farms, you can set up two separate virtual apps collections in Workspace ONE Access. This allows for easier management of the configuration and faster sync as each collection is synced separately.

You can also use different Virtual App service instances for each collection to distribute the sync load.

The Virtual Apps Collections page, accessed by navigating to **Catalog > Virtual Apps Collections** in the Workspace ONE Access console, provides a central location for managing all your resources integrations. You can create and edit collections, monitor the sync status of all collections, view alerts, and sync manually from this page.

Virtual Apps Collections

NEW EDIT SYNC ▾ DELETE

Name	Source Type	Sync Frequency	Sync Status	⌂	Last Attempt Sync
<input type="radio"/> Horizon Apps	Horizon	Manual	Completed More		Apr 15, 2021, 3:56:33 PM

1 - 1 of 1 item(s)

Benefits of Using Virtual Apps Collections

The virtual apps collections feature provides the following benefits:

- A central location from which to manage all resource integrations
 - Manage all types of resources
 - Manage the configuration and sync settings for each collection
 - Monitor the sync status of all collections

- Ability to sync smaller sets of data by setting up multiple collections for a large resource integration. For example, you can create separate collections for each Horizon pod or each XenApp farm.
- Ability to set up separate collections for different domains. Multiple domains do not need a trust relationship if you use separate collections for each domain.

Requirements for Virtual Apps Collections

The virtual apps collection feature has the following requirements:

- Install the Virtual App service, which is a component of Workspace ONE Access connector 21.08 and later, for any integration except ThinApp.
- Role requirements
 - To access the Virtual Apps Collections page initially, use a Super Admin role.
In a new installation, when you select the **Catalog > Virtual Apps Collections** tab for the first time, an information page appears and you click **Get Started** to display the Virtual Apps Collections page. This initial getting started flow requires a Super Admin role.
 - Subsequently, you can manage virtual apps collections with any role that can perform the following actions in the Catalog service:
 - Manage Desktop Apps (to create, edit, or delete Horizon and Citrix virtual apps collections)
 - Manage ThinApp (to create, edit, or delete ThinApp collections)
 - To save the Network Ranges page for Horizon and Citrix collections, you must use the Super Admin role. The Network Ranges page specifies Client Access FQDNs to direct user requests to the appropriate servers.

Creating Virtual Apps Collections in Workspace ONE Access

You can create one or more virtual apps collections in the Workspace ONE Access console for each type of integration, such as Horizon, ThinApp, or Citrix.

Prerequisites

- Install the Virtual App service, a component of Workspace ONE Access connector 21.08 and later.

Note The Virtual App service does not support integration with ThinApp packaged applications. Integration with ThinApp is only supported with the legacy VMware Identity Manager connector (Linux) version 2018.8.1.0.

- The following administrator roles are required:
 - To get started with virtual apps collections, use the Super Admin role. See [About Workspace ONE Access Virtual Apps Collections](#) for more information.

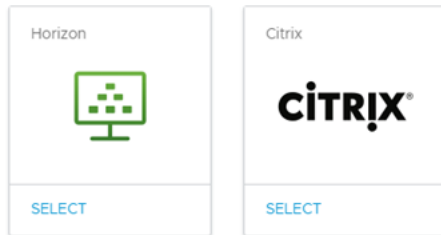
- To create, edit, or delete Horizon or Citrix virtual apps collections, use any role that can perform the Manage Desktop Apps action in the Catalog service.
- To create, edit, or delete ThinApp collections, use any role that can perform the Manage ThinApp action in the Catalog service.
- To edit and save the Network Ranges page for Horizon and Citrix virtual apps collections, use the Super Admin role.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 If an information page appears, review the information and click **Get Started**, otherwise click **New**.
- 4 Select the type of resource to integrate.

Select the Source Type

Select the source type to use to create the virtual apps collection.



- 5 Follow the New Collection wizard to create the collection.

The configuration information for each type of integration is different.

- For a Horizon on premises integration, see [Configure Horizon Pods and Pod Federations in Workspace ONE Access](#) for more information.
- For a Citrix integration, see [Configuring Citrix Server Farms in Workspace ONE Access](#) for more information.
- For a ThinApp integration, see [Configuring ThinApp Packages in Workspace ONE Access](#) for more information.

Some settings, such as the following, appear for all source types.

Option	Description
Connector	Select the connectors to use to sync this collection. You can add multiple connectors and arrange them in failover order. Only connectors that have the Virtual App service component installed appear in the list.
Sync Frequency	Select when and how frequently you want to sync the resources in the collection. The sync frequency can range from hourly to weekly. If you do not want to set up an automatic sync schedule, select the Manual option. If you select Manual , you must sync the collection manually after you create it and whenever you want to sync updates from the source server. For more information about sync, see Syncing Virtual Apps Collections in Workspace ONE Access .
Activation Policy	Select how you want to make resources in this collection available to users in the Workspace ONE Intelligent Hub portal and app. If you intend to set up an approval flow, select User-Activated , otherwise select Automatic . With both the User-Activated and Automatic options, the resources are added to the Apps tab. Users can run the resources from the Apps tab or mark them as favorites and run them from the Favorites tab. However, to set up an approval flow for any of the apps, you must select User Activated for that app. The activation policy applies to all user entitlements for all the resources in the collection. You can modify the activation policy for individual users or groups per resource, from the user or group page in the Users & Groups tab.

What to do next

The resources in the new collection are not yet synced. If you set up a sync schedule for the collection, the resources are synced at the next scheduled time. If you selected the Manual option for sync, you must sync the resources manually by selecting the collection in the Virtual Apps Collections page and clicking **Sync > Sync with safeguards** or **Sync > Sync without safeguards**.

Editing Virtual Apps Collections in Workspace ONE Access

You can edit all virtual apps collections, for all types of integrations, from the Virtual Apps Collections page in the Workspace ONE Access console. You can modify both configuration settings and sync settings from this page.

Prerequisites

- The following administrator roles are required:
 - To create, edit, or delete Horizon and Citrix virtual apps collections, use any role that can perform the Manage Desktop Apps action in the Catalog service.
 - To create, edit, or delete ThinApp collections, use any role that can perform the Manage ThinApp action in the Catalog service.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the virtual apps collection to edit and click **Edit**.
- 3 In the Edit Virtual Apps Collection wizard, edit the virtual apps collection and save your changes.

You can change the following settings:

- The name of the virtual apps collection
- The connectors used to sync the collection
- The source server or path, and related settings
- Sync settings such as the sync frequency or sync safeguards
- Other settings, as applicable to the type of integration

Note In a Horizon virtual apps collection, you cannot modify the FQDN of a Horizon pod that was previously added. Remove the pod from the collection and add it again.

What to do next

As a best practice, sync the virtual apps collection after editing it. Go to the **Catalog > Virtual Apps Collections** page, select the collection, and select **Sync > Sync with safeguards** or **Sync > Sync without safeguards**.

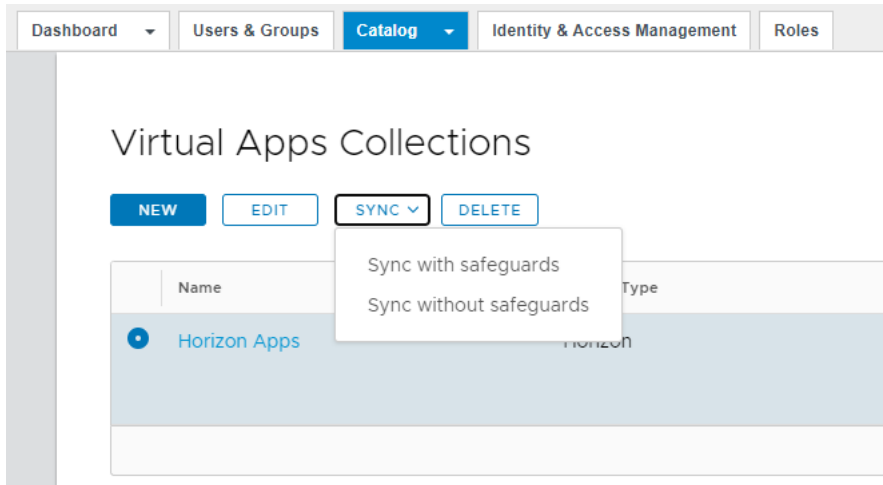
Syncing Virtual Apps Collections in Workspace ONE Access

Syncing a virtual apps collection propagates applications, desktops, and assignments from the source server to the Workspace ONE Access service. You can sync a collection at any time from the Virtual Apps Collections page in the Workspace ONE Access console. You can also set up a sync schedule. Additionally, you can configure sync safeguards to help prevent unintended changes.

Syncing a Virtual Apps Collection Manually

When you want to sync applications, desktops, and assignments from the source server to the Workspace ONE Access service immediately, you can start the sync process manually. Virtual apps collections that do not have a sync schedule set must always be synced manually.

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the virtual apps collection to sync, then select **Sync > Sync with safeguards** or **Sync > Sync without safeguards**, based on your preference.



For information about sync safeguards, see [Managing Sync Safeguard Thresholds](#).

Workspace ONE Access compares applications, desktops, and assignments between the source server and the Workspace ONE Access service. If there are changes in the source that need to be propagated to Workspace ONE Access, the sync process starts. The process might take some time to complete, depending on the number of applications, desktops, and assignments that require syncing.

For information about viewing sync results, see [Monitoring Virtual Apps Collections in Workspace ONE Access](#).

Setting up a Sync Schedule

You can set up a sync schedule for a virtual apps collection so that applications, desktops, and assignments are synced automatically from the source server to the Workspace ONE Access service at regular intervals. When you set a schedule, changes in the source server are reflected in Workspace ONE Access without requiring a manual sync.

You can set up a sync schedule while creating a virtual apps collection or any time later.

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collection** tab.
- 2 Select the virtual apps collection for which you want to set a schedule, and click **Edit**.
- 3 In the Edit wizard, click **Configuration** in the left pane.
- 4 In the **Sync** section, configure the sync frequency.
 - You can configure the sync frequency to **Weekly**, **Daily**, or **Hourly**, and specify the time of day to sync.

For example:

Sync

Sync Frequency

Daily

Sync Time

05 : 30 UTC

- If you do not want to set a sync schedule, set the sync frequency to **Manual**. If the sync frequency is set to **Manual**, you must click the **Sync** button on the Virtual Apps Collections page every time you want to sync the collection.

Sync

Sync Frequency

Manual

For information about viewing sync results, see [Monitoring Virtual Apps Collections in Workspace ONE Access](#).

Managing Sync Safeguard Thresholds

Workspace ONE Access sets sync safeguard thresholds for all virtual apps collections by default to help prevent unintended changes when the collection syncs. Sync safeguards limit the number of changes that can be made to applications, desktops, and assignments during sync. You can modify these thresholds at any time.

Sync safeguards are ignored the first time a virtual apps collection syncs to Workspace ONE Access but are applied to every subsequent sync.

Workspace ONE Access sets a default threshold of 10% for each of the following actions:

- Add applications
- Add desktops
- Add assignments
- Delete applications
- Delete desktops
- Delete assignments

During sync, Workspace ONE Access compares the applications, desktops, and assignments in Workspace ONE Access to the ones on the source server and calculates the number of changes required. If the changes exceed the threshold for any of the categories, Workspace ONE Access cancels the sync process and you receive an error.

For example, if the threshold for **Add Applications** is set to 10%, and 4 additional applications need to be synced to a virtual apps collection that currently includes 20 applications, sync safeguards will prevent the sync process from succeeding because the changes exceed 10%.

To sync the collection, you must either manually sync the collection with the **Sync > Sync without safeguards** command or raise the safeguard thresholds so that the next scheduled sync succeeds. The **Sync without safeguards** command ignores the safeguards thresholds that are set for the collection and syncs all the applications, desktops, and assignments that require syncing.

You can set up sync safeguards while creating a virtual apps collection or any time later.

- 1 In the Workspace ONE Access console, select **Catalog > Virtual Apps Collections**.
- 2 Select the virtual apps collection, then click **Edit**.
- 3 In the left pane of the Edit wizard, click **Configuration**.
- 4 Scroll to the **Safeguards Thresholds Limits** section and set the thresholds for the actions that are listed.
- 5 Click **Next**, then click **Save**.

The updated settings apply the next time the collection is synced.

Monitoring Virtual Apps Collections in Workspace ONE Access

You can monitor the sync status of all your virtual apps integrations from the Virtual Apps Collections page in the Workspace ONE Access console. For each virtual apps collection, you can view the time the resources were last synced, whether the sync was successful or not, which resources and assignments were synced, and whether any alerts occurred during the sync.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.

All collections, for all types of resource integrations, appear on the page.

Virtual Apps Collections

[NEW](#) [EDIT](#) [SYNC](#) [DELETE](#)

Name	Source Type	Sync Frequency	Sync Status	Last Attempt Sync
<input type="radio"/> Horizon Apps	Horizon	Manual	Completed More	Apr 15, 2021, 3:56:33 PM

1 - 1 of 1 item(s)

2 View the information for each collection.

To view	See
The sync schedule that is set for the collection	<p>The Sync Frequency column.</p> <p>If you did not set an automatic sync schedule, the column displays Manual. With a Manual setting, you must sync the virtual apps collection manually each time you want to propagate any changes in resources or assignments from the source servers to Workspace ONE Access.</p>
The time of the last sync attempt	<p>The Last Sync Attempt column.</p>
The status of the last sync	<p>The Sync Status column displays one of the following states:</p> <ul style="list-style-type: none">■ <code>Not yet synced</code> The virtual apps collection has never been synced.■ <code>Started</code> The sync process has started.■ <code>Failed to start sync</code> The sync process cannot start because a previous sync is in progress.■ <code>Completed</code> The sync process is complete.■ <code>Failed</code> The sync process did not succeed. For example, if a network issue prevented the Virtual App service from reaching the server from which to sync resources, sync could not succeed.

To view	See
---------	-----

Desktops, applications, and entitlements that were added or deleted in the last sync

- 1 Click **More** in the **Sync Status** column.
- 2 Click the information icon.

Name	Source Type	Sync Frequency	Sync Status	Last Attempt Sync
Horizon Apps	Horizon	Manual	Completed 	Apr 15, 2021, 3:55:57 PM

The Sync Action Summary dialog box lists the number of applications, desktops, and assignments that were added, deleted, or updated in the sync run. For example:

Sync Action Summary

Sync Time: Mar 11, 2021, 2:32:12 AM


Applications	Desktops	Assignments
8 added	4 added	35 added
0 updated	0 updated	0 updated
0 deleted	0 deleted	0 deleted

CLOSE

- 3 To view the names of the applications, desktops, or assignments, click the links.

Alerts

- 1 Click **More** in the **Sync Status** column.
- 2 Click the alert icon.

Name	Source Type	Sync Frequency	Sync Status	Last Attempt Sync
Horizon Apps	Horizon	Manual	Completed 	Apr 15, 2021, 3:55:57 PM

The Sync Alerts dialog box displays alerts that occurred during sync. For example, if assignments were synced for a user who does not exist in Workspace ONE Access, an alert appears.

Sync Alerts

- Could not entitle user with Reason: User not synced in workspace. to resource Hzc3-Ded-Pool.
- Could not entitle user with Reason: User not synced in workspace. to resource Hzc3-Ded-Pool.

Deleting Virtual Apps Collections in Workspace ONE Access

You can delete a virtual apps collection from Workspace ONE Access when you no longer need to provide your users any of the apps and desktops from that virtual apps collection.

When you delete a collection, all applications and desktops synced by the collection are deleted. When you delete a Horizon or Citrix collection, the corresponding policies configured in network ranges are also deleted. When you delete a Horizon or Horizon Cloud collection, the federation artifact is also deleted.

Prerequisites

- To delete Horizon and Citrix-published virtual apps collections, use an administrator role that can perform the Manage Desktop Apps action in the Catalog service.

- To delete ThinApps collections, use an administrator role that can perform the Manage ThinApps action in the Catalog service.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the collection you want to delete and click **Delete**.

Configuring Password Caching for Virtual Apps (Workspace ONE Access Cloud Only)

You can enable password caching in the Workspace ONE Access console to provide single sign on for users running Horizon, Horizon Cloud, and Citrix virtual apps from the Workspace ONE catalog. Once users' passwords are cached, they are not required to enter their passwords again while running virtual apps in the same login session.

When the password caching option is enabled, users' passwords are cached either when they first log in or when they first run a virtual app, based on the authentication methods configured.

- If a user logs into Workspace ONE using password authentication, the password is cached at login.
- If a user logs into Workspace ONE using a non-password authentication method such as certificate or third-party IDP, the user is required to enter a password the first time they launch a Horizon, Horizon Cloud, or Citrix app. The password is then cached.

Note Users are not prompted for passwords for Horizon or Horizon Cloud integrations that have True SSO configured.

The password caching option was introduced in the Workspace ONE Access Cloud 2006 release in June 2020 with the following defaults:

- The option is turned on for existing Workspace ONE Access tenants that have Horizon without True SSO, Horizon Cloud without True SSO, or Citrix integrations configured.
- The option is turned off for all other existing tenants and for new tenants.

Important For Horizon and Horizon Cloud integrations, setting up True SSO instead of password caching to provide a single sign on experience is recommended.

Procedure

- 1 In the Workspace ONE Access console, navigate to the **Identity & Access Management > Setup > Preferences** page.
- 2 Select or deselect the **Enable Password Caching** option, based on your preferences.

Providing Access to VMware Horizon Desktops and Applications in Workspace ONE Access

4

Integrating VMware Horizon[®] with the Workspace ONE Access service lets you provide users the ability to access their assigned Horizon desktops and applications from the Workspace ONE Intelligent Hub app or portal. You can integrate independent Horizon pods, which consist of Horizon Connection Server instances, and pod federations, which contain multiple pods and can span multiple sites and data centers.

You deploy and manage desktop and application pools in the Horizon Console. You also create user assignments for Active Directory users and groups in Horizon, not in Workspace ONE Access. You must sync these users and groups to the Workspace ONE Access service from Active Directory before setting up the integration with Horizon.

To integrate Horizon pods and pod federations with Workspace ONE Access, you create one or more virtual apps collections in the Workspace ONE Access console. The collections contain the configuration information for the pods and pod federations, sync settings, and other settings. You then sync the collection, which propagates Horizon resources and assignments to Workspace ONE Access.

In the Workspace ONE Access console, you can view the Horizon desktops and applications. You can also view user and group assignments for these desktops and applications.

End users can run their assigned desktops and applications from the Intelligent Hub app or portal. They can access the desktops and applications over HTML in a browser or over a supported display protocol in the Horizon Client.

Supported VMware Horizon Versions and Features

Workspace ONE Access supports the following VMware Horizon versions:

- Horizon 8
- Horizon 7

It supports the following VMware Horizon features:

- Integration with independent Horizon pods
- Integration with pod federations, created using the Cloud Pod Architecture feature

- HTML Access

Important If you integrate Horizon 7.13 or later versions with Workspace ONE Access, end users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers. See the [VMware Horizon HTML Access](#) documentation for information.

- Certificate SSO

See the VMware Product Interoperability Matrix for the latest support information.

This chapter includes the following topics:

- [Deployment Scenario for Integrating Horizon with Workspace ONE Access](#)
- [High-Level Horizon-Workspace ONE Access Integration Design](#)
- [About Integrating Independent Horizon Pods with Workspace ONE Access](#)
- [About Integrating Horizon Cloud Pod Architecture \(CPA\) Deployments with Workspace ONE Access](#)
- [Configuring Horizon Pods and Pod Federations in Workspace ONE Access](#)
- [Setting Client Access FQDNs for Horizon Virtual Apps in Workspace ONE Access](#)
- [Launching Horizon Resources Through Validating Gateways](#)
- [Viewing Horizon Desktop and Application Pool Information in Workspace ONE Access](#)
- [Viewing User and Group Assignments for Horizon Desktop and Application Pools in Workspace ONE Access](#)
- [Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access](#)
- [Allowing Users to Reset Their Horizon Desktops from the Workspace ONE Catalog](#)
- [Viewing Launch Options for Horizon Desktops and Applications in Workspace ONE Access](#)
- [Launching Horizon Desktops and Applications Integrated with Workspace ONE Access](#)

Deployment Scenario for Integrating Horizon with Workspace ONE Access

To integrate your on-premises VMware Horizon deployment with the Workspace ONE Access service, make sure that you set up all the required components and follow the high-level deployment considerations listed here.

You need the following components:

- A Workspace ONE Access tenant or on-premises instance
- A Workspace ONE Access Virtual App service instance, installed on premises. The Virtual App service is a component of Workspace ONE Access connector 21.08 and later.

You can download the connector from the Workspace ONE Access product page on <https://my.vmware.com>.

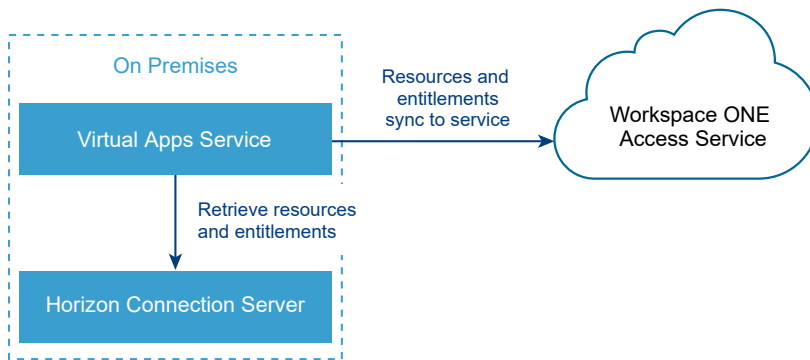
- A VMware Horizon deployment on premises

While deploying the on-premises components, ensure that all instances of the Virtual App service can communicate with the Horizon Connection Server instances.

All communication between the Workspace ONE Access service and the on-premises components is through the connector. The connector and the service communicate over a communication channel that is automatically set up during installation.

The following diagram depicts a Workspace ONE Access-Horizon integration.

Figure 4-1. Workspace ONE Access and Horizon Integration

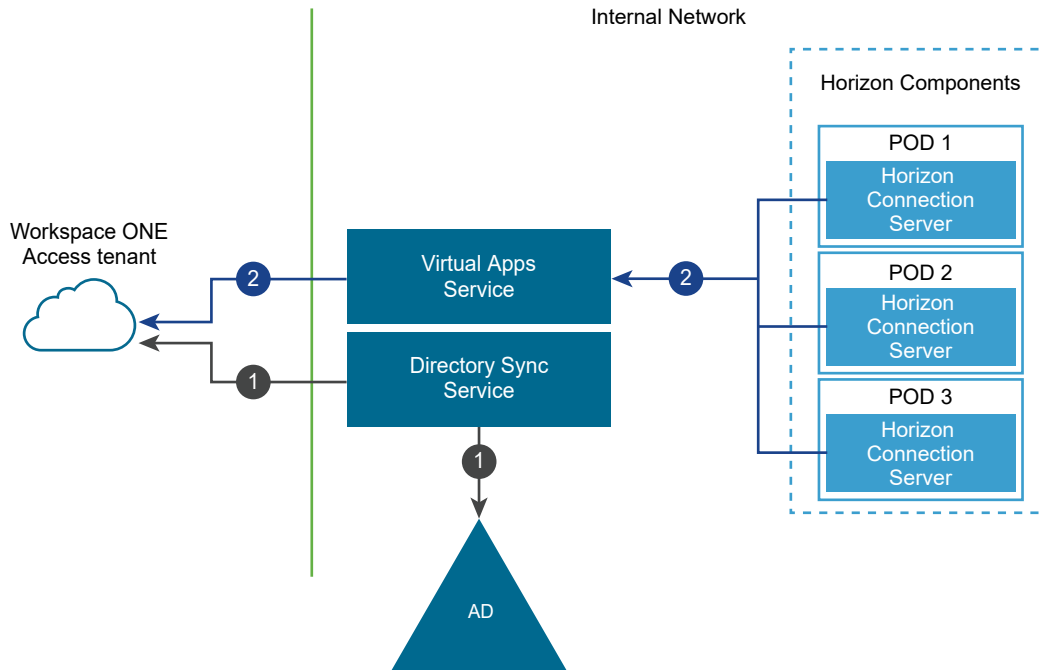


High-Level Horizon-Workspace ONE Access Integration Design

The synchronization and launch architecture diagrams depict how Workspace ONE Access synchronizes on-premises Horizon resources and user assignments from the Horizon Connection Server to the Workspace ONE Access service and how it launches these resources from Workspace ONE.

Horizon Resources and Assignments Synchronization

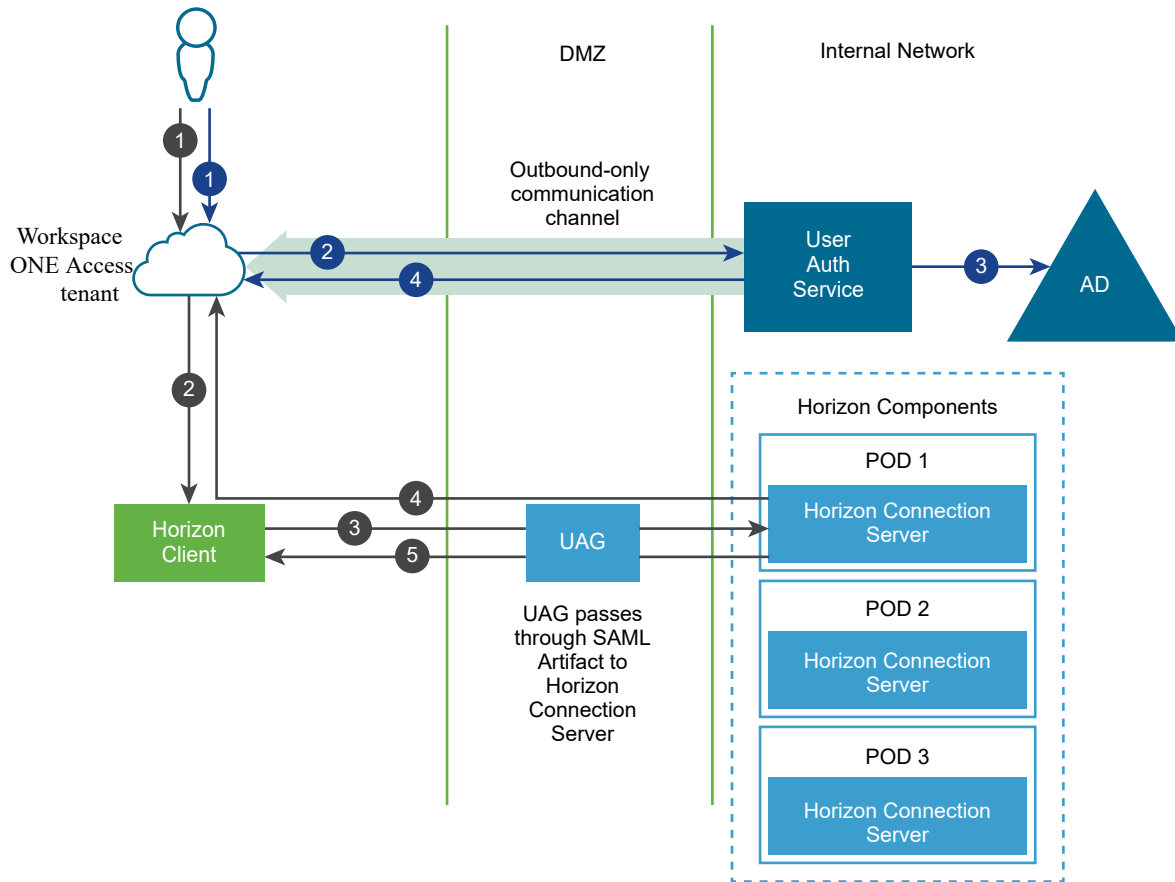
Figure 4-2. Synchronization Architecture Diagram



- 1 The Directory Sync service syncs users and groups from Active Directory to the Workspace ONE Access service.
- 2 The Virtual App service syncs Horizon resources and assignments from the Horizon Connection Server to the Workspace ONE Access service.

Horizon Applications and Desktops Launch

Figure 4-3. Launch Architecture Diagram



The blue arrows in the diagram depict the authentication flow.

- 1 A user enters Active Directory credentials to log into the Workspace ONE Intelligent Hub app or portal.
- 2 The Workspace ONE Access service sends encrypted credentials to the User Auth service.
- 3 The User Auth service verifies the credentials with Active Directory.
- 4 The User Auth service sends an OK message to the Workspace ONE Access service, allowing the user to log in.

The black arrows in the diagram depict the launch flow.

- 1 The user launches a Horizon resource from the Workspace ONE Intelligent Hub app or portal.
- 2 The Workspace ONE Access service creates a launch URL with the SAML artifact and passes it to the Horizon Client.
- 3 The Horizon Client connects to the Horizon Connection Server through Unified Access Gateway (UAG).

- 4 The Horizon Connection Server resolves the SAML artifact with the Workspace ONE Access service to get the SAML assertion and validates it.
- 5 The Horizon Connection server renders the Horizon resource to the end user through the Horizon Client.

About Integrating Independent Horizon Pods with Workspace ONE Access

To integrate Horizon pods with Workspace ONE Access, you create one or more virtual apps collections in the Workspace ONE Access console. The virtual apps collections contain the configuration information for the Horizon Connection Servers, sync settings, and other settings relevant to the integration.

Before you perform any integration tasks in the Workspace ONE Access console, you must set up Horizon. You create and configure desktop and application pools in Horizon Console, not in the Workspace ONE Access console. You also set assignments for Active Directory users and groups in Horizon Console.

Integrating Horizon pods with Workspace ONE Access involves the following high-level tasks.

- Deploy and configure Horizon servers.
- Deploy Horizon desktop and application pools, with entitlements set for Active Directory users and groups.
- Sync Active Directory users and groups who are entitled to application and desktop pools in Horizon Connection Server instances to the Workspace ONE Access service using the Directory Sync service.
- Create one or more virtual apps collections for the Horizon pods in Workspace ONE Access.
- Configure SAML authenticator on the Horizon Connection Server. You must always use the Workspace ONE Access FQDN on the Authenticator configuration page.

Requirements for Integrating Horizon Pods with Workspace ONE Access

While setting up the Horizon pods that you plan to integrate with Workspace ONE Access through virtual apps collections, make sure that you meet the requirements listed here.

- Deploy Horizon Connection Servers on the default port 443 or on a custom port.
- Verify that you have a DNS entry and an IP address that can be resolved during reverse lookup for each Horizon Connection Server in your setup. Workspace ONE Access requires reverse lookup for the Horizon Connection Servers, Horizon Security Server, and the load balancer. If reverse lookup is not properly configured, the Workspace ONE Access integration with Horizon fails.
- Ensure that the Horizon Connection Servers have valid certificates signed by a trusted Certificate Authority (CA). If you have not obtained CA-signed certificates and are using self-

signed certificates temporarily for testing purposes, you must upload the root certificates to the Virtual App service trust store using the Workspace ONE Access connector installer, and then restart the Virtual App service. See [Set up Your Workspace ONE Access Environment for Horizon Integration](#) for more information.

- Deploy and configure Horizon desktop and application pools with entitlements set for Active Directory users and groups. Ensure that users have the correct entitlements.
- While configuring desktop pools, ensure that in Remote Settings, you set the **Automatically log off after disconnect** option to 1 or 2 minutes instead of **immediately**.
- You can create pools in any access group in the Horizon environment. Ensure that the admin user account that you use to sync Horizon assignments to Workspace ONE Access has admin permissions on the Horizon root access group so that pools and resources from all access groups can be synced to Workspace ONE Access.
- Extending the SAML metadata expiration period on the Horizon Connection Servers to 1 year is recommended. See [Change the Expiration Period for Service Provider Metadata on View Connection Server](#) for information.
- If you integrate Horizon 7.13 or later versions with Workspace ONE Access, end users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers. See the [VMware Horizon HTML Access](#) documentation for information.

About Integrating Horizon Cloud Pod Architecture (CPA) Deployments with Workspace ONE Access

In addition to integrating independent Horizon pods with Workspace ONE Access, you can integrate Horizon Cloud Pod Architecture (CPA) deployments.

Figure 4-4. Integrating Horizon Pod Federations with Workspace ONE Access On Premises

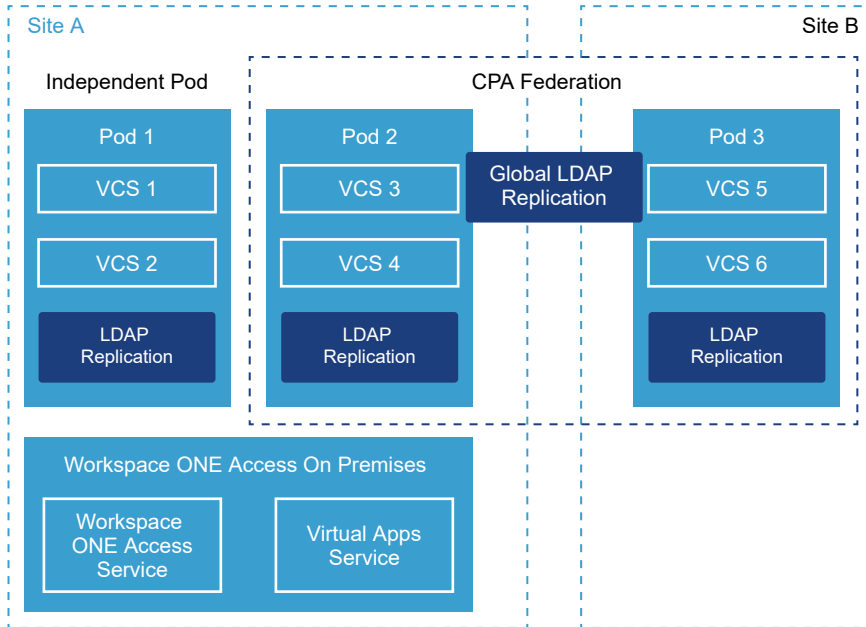
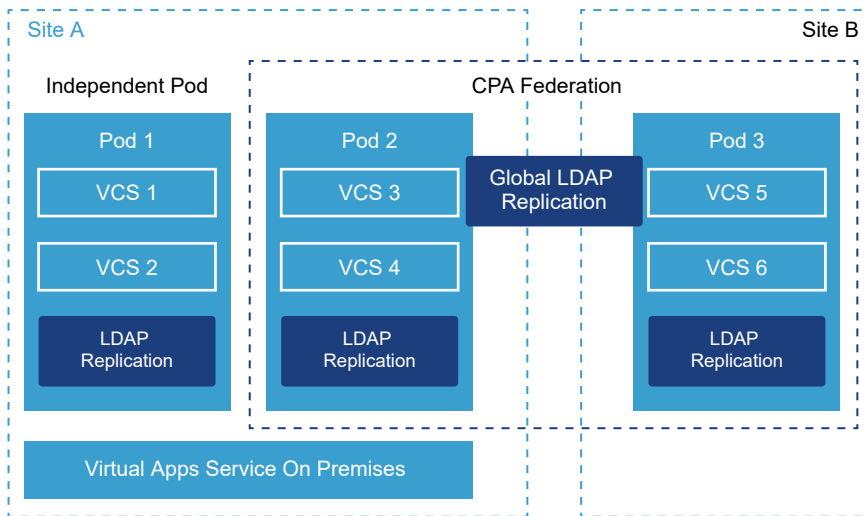


Figure 4-5. Integrating Horizon Pod Federations with the Workspace ONE Access Cloud Service



The Horizon Cloud Pod Architecture feature links together multiple Horizon pods to form a single large desktop and application brokering and management environment called a pod federation. A pod federation can span multiple sites and data centers.

You can integrate one or more pod federations with the Workspace ONE Access service. Note that pod federations are created and managed in Horizon, and that user and group entitlements to the pod federation's desktops and application pools are set in Horizon. You sync the resources and entitlements to Workspace ONE Access.

Pod federations have global entitlements, which let you entitle users to desktops and applications that can be accessed from any pod in the pod federation. A global entitlement can consist of resources from multiple pods in the federation. For example, a global desktop entitlement might contain desktop pools from three different pods in three different data centers. Individual pods in the pod federation can also have local entitlements configured. You can sync both global and local entitlements to Workspace ONE Access.

Integrating a pod federation with the Workspace ONE Access service involves the following high-level tasks in the Workspace ONE Access console:

- Add all the pods that form the pod federation, specifying Horizon Connection Server details for each.

While Workspace ONE Access can sync global entitlements from any one of the pods in the pod federation, it needs to connect to each pod to sync metadata required for SAML authentication. It also needs to connect to the pods to sync local entitlements, if applicable.

- Add the pod federation details and specify the global launch URL. The global launch URL, typically the global load balancer URL, is used to launch globally-entitled desktops and applications.

You can customize the global launch URL for specific network ranges, for example for internal and external access.

- Sync resources and entitlements from the pod federation to the Workspace ONE Access service.
- Customize the global launch URL by setting client access URLs for specific network ranges. These URLs are used to launch globally-entitled resources from the pod federation. By default, the global launch URL you specify while adding the federation is used as the global launch URL for all network ranges.
- Specify client access URLs for each pod in the pod federation that has local entitlements configured. These URLs are used to launch locally-entitled desktops and applications from the pod. A client access URL can be a Horizon Connection Server URL, a Security Server URL, or a load balancer URL. Client access URLs are set for specific network ranges. By default, the Horizon Connection Server you specify while adding the pod is used as the client access URL for all network ranges.

When you integrate a pod federation with the Workspace ONE Access service, the service does the following:

- Syncs all global entitlements from the pod federation.
- Syncs local entitlements, if selected, from the pods that are part of the pod federation.
- Syncs metadata from all the Horizon Connection Servers in the pod federation.
- Allows end users to access their Horizon applications and desktops from the Workspace ONE Intelligent Hub app or portal.

End users access their Horizon applications and desktops from the Intelligent Hub app or portal. All the resources to which they are entitled, whether through global entitlements or local entitlements, are displayed. Applications and desktops are launched in the Horizon Client or in a browser. When a user launches a locally-entitled application or desktop, it is launched from the Horizon Connection Server to which the user connects. Globally-entitled resources are launched from the Horizon Connection Server in which the resource is located.

Sample Cloud Pod Architecture Deployment

The following diagrams show a sample cloud pod architecture deployment and how it is integrated with the Workspace ONE Access service.

Figure 4-6. Cloud Pod Architecture Deployment with Workspace ONE Access On Premises

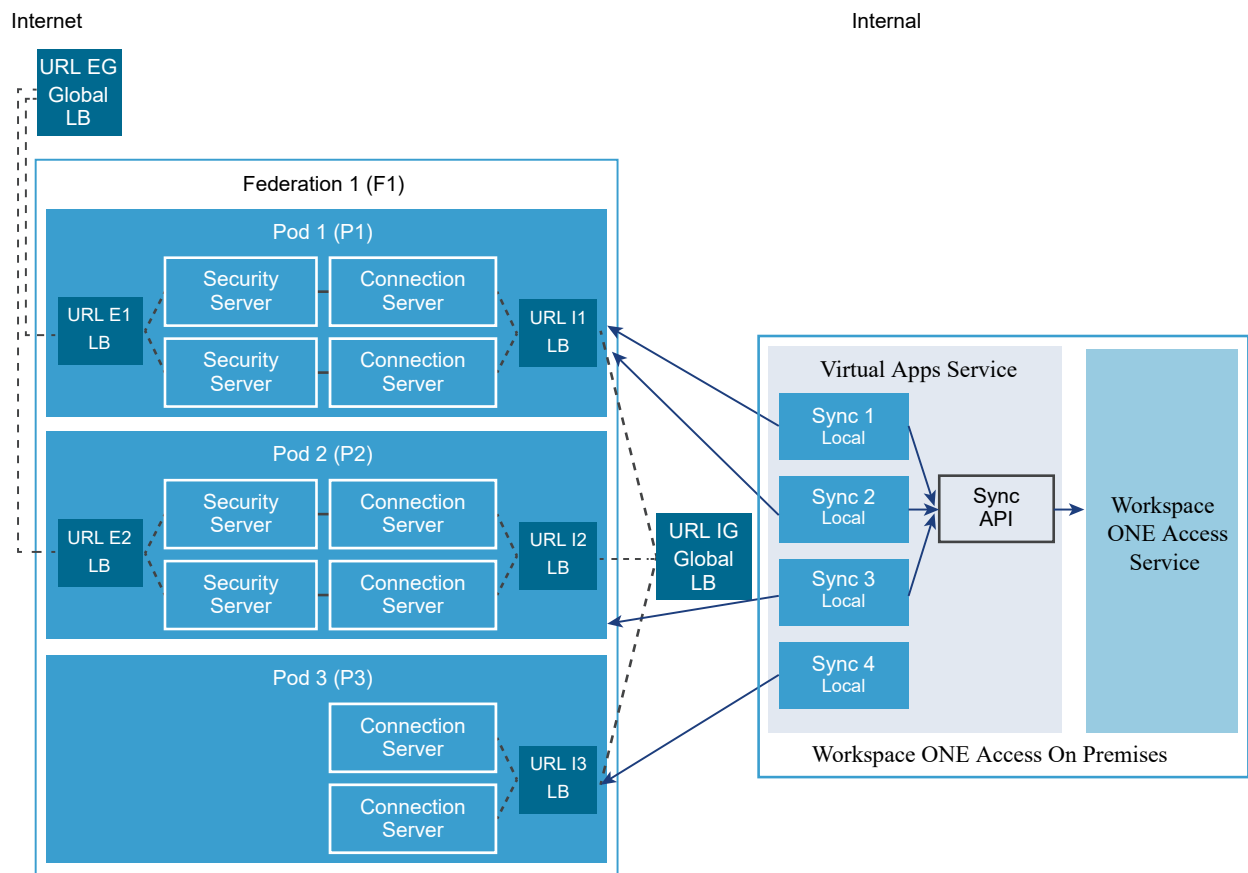
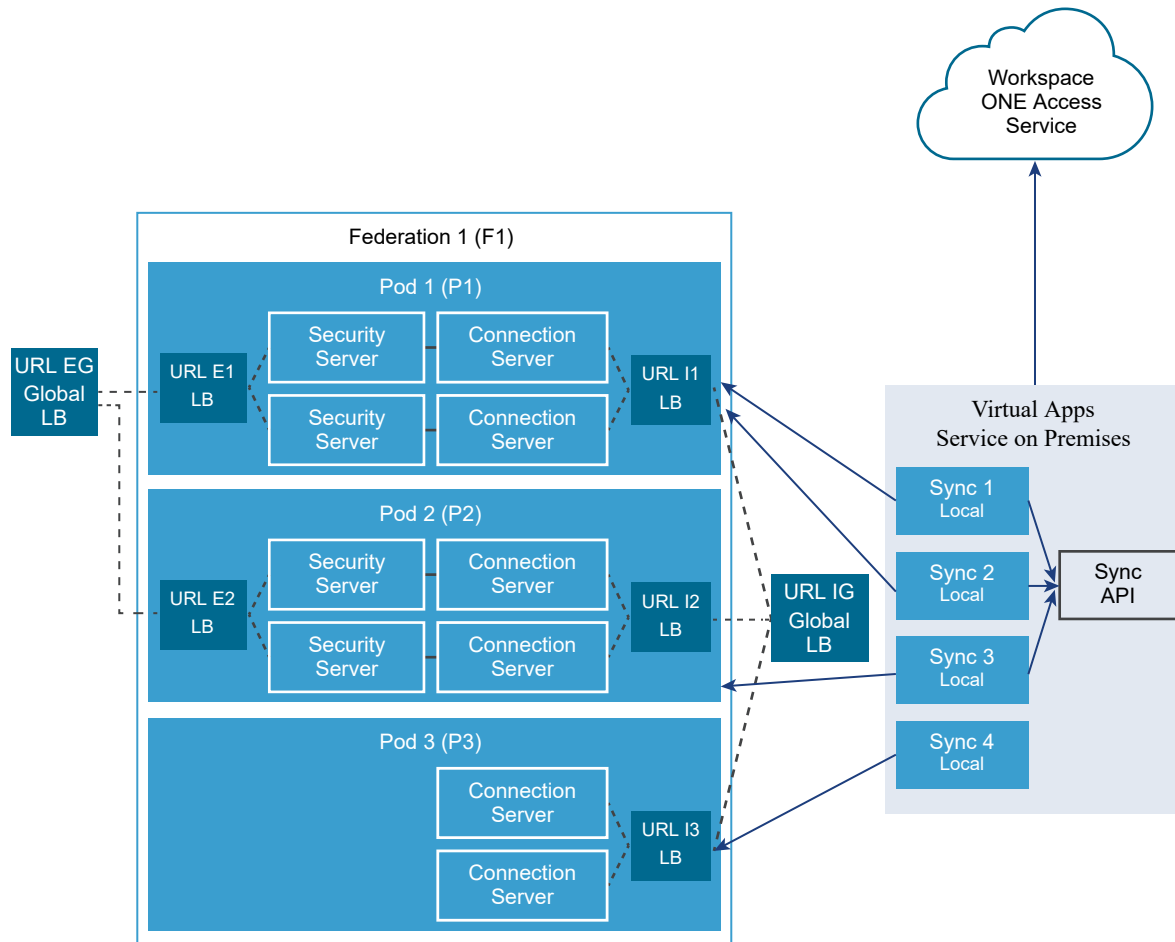


Figure 4-7. Cloud Pod Architecture Deployment with Workspace ONE Access Cloud Service



This diagram depicts a sample pod federation deployment. A pod federation, named Federation 1, is created in Horizon 6. It has three pods, Pod 1, Pod 2, and Pod 3. Pod 1 and Pod 2 are configured with Security Server instances for each Horizon Connection Server and an external load balancer for external access, and with an internal load balancer for internal access. Pod 3 is configured for only internal access with an internal load balancer. The pod federation as a whole has an external global load balancer and an internal global load balancer.

Desktop and application pools are deployed on the pods. Global entitlements are configured for Federation 1 and local entitlements are also configured for the individual pods.

Federation 1 is integrated with the Workspace ONE Access service. The Workspace ONE Access service syncs global entitlements as well as local entitlements from Federation 1. Because global entitlements are replicated in each pod, it syncs global entitlements from Pod 1. It also syncs local entitlements from Pod 1, Pod 2, and Pod 3.

End users can view all the desktops and applications to which they are entitled, whether through global entitlements or local entitlements, in the Intelligent Hub app or portal. When a user launches a desktop or application, if it is part of a global entitlement, the launch request goes to the external or internal global load balancer, URL EG or URL IG, based on the network range of the user. If the resource is from a local entitlement, the launch request goes to the internal or external load balancer of the pod on which the resource is deployed, based on the network range of the user. For example, for a resource on Pod 2, the request goes to URL I2 or URL E2.

Requirements for Integrating Horizon Pod Federations with Workspace ONE Access

To integrate Horizon pod federations with Workspace ONE Access, make sure that you meet the requirements listed here.

- Workspace ONE Access supports the Cloud Pod Architecture feature for both applications and desktops.
- You can integrate a maximum of 10 pod federations with the Workspace ONE Access service. Each federation can contain up to 7 pods.
- Deploy Horizon Connection Server instances on the default port 443 or on a custom port.
- Verify that you have a DNS entry and an IP address that can be resolved during reverse lookup for each Horizon Connection Server instance in your environment. Workspace ONE Access requires reverse lookup for Horizon Connection Server, Security Server, and load balancer instances. If reverse lookup is not properly configured, the Workspace ONE Access integration with Horizon fails.
- The Workspace ONE Access Virtual App service must be able to reach all the Horizon Connection Server instances in the pod federation.
- Ensure that the Horizon Connection Servers have valid certificates signed by a trusted Certificate Authority (CA). If you have not obtained CA-signed certificates and are using self-signed certificates temporarily for testing purposes, you must upload the root certificates to the Virtual App service trust store using the Workspace ONE Access connector installer, and then restart the Virtual App service. See [Set up Your Workspace ONE Access Environment for Horizon Integration](#) for more information.
- SAML authentication must be configured in Horizon, with the Workspace ONE Access service specified as the identity provider. You must use the service's fully-qualified domain name as part of the URL. Configuring SAML authentication on all the Horizon Connection Server instances in the pod federation is recommended. See [Configure SAML Authentication in Horizon for Workspace ONE Access Integration](#) for more information.

Extending the SAML metadata expiration period on the Horizon Connection Server instances to 1 year is recommended. See [Change the Expiration Period for Service Provider Metadata on View Connection Server](#) for information.

- Deploy application and desktop pools in the Horizon pods.
 - While configuring desktop pools, ensure that in Remote Settings, you set the **Automatically log off after disconnect** option to 1 or 2 minutes instead of **immediately**.
 - You can create pools in any access group in the Horizon environment. Ensure that the admin user account that you use to sync Horizon assignments to Workspace ONE Access has admin permissions on the Horizon root access group so that pools and resources from all access groups can be synced to Workspace ONE Access.

If you add or remove application or desktop pools after integrating with Workspace ONE Access, for the changes to appear in the Workspace ONE Access service, you must sync again.

- You must create the pod federation, by initializing the Cloud Pod Architecture feature from one of the pods and joining all the other pods to the federation, before integrating with the Workspace ONE Access service. Global entitlements are replicated to pods when they join the federation.

If you join or remove a pod from the pod federation after you integrate the pod federation with the Workspace ONE Access service, you must edit the pod federation details in the Workspace ONE Access console to add or remove the pod, save your changes, and sync again.

- In your Horizon environment, create global entitlements in the pod federation to entitle Active Directory users or groups to desktops and applications.
- (Optional) Create local entitlements on the pods, if required.
- In Horizon 7 versions prior to 7.13, to enable end users to launch desktops or applications in a Web browser, select the HTML Access option for the global entitlement.

If you integrate Horizon 7.13 or later versions with Workspace ONE Access, end users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers. See the [VMware Horizon HTML Access](#) documentation for information.

For more information about configuring Horizon, see the VMware Horizon documentation.

Configuring Horizon Pods and Pod Federations in Workspace ONE Access

To configure Horizon pods and pod federations in Workspace ONE Access, you set up your Workspace ONE Access environment, create one or more virtual apps collections for the integration, specify Client Access FQDNs for specific network ranges, and configure SAML authentication in Horizon.

Set up Your Workspace ONE Access Environment for Horizon Integration

After setting up your Horizon environment, you must set up your Workspace ONE Access environment before integrating the Horizon pods and pod federations with the Workspace ONE Access service.

Using valid certificates signed by a trusted Certificate Authority (CA) for the Horizon Connection Servers is strongly recommended. If you have not obtained CA-signed certificates and are using self-signed certificates temporarily for testing purposes, you must upload the root certificates to the Virtual App service trust store.

Prerequisites

To sync users and groups from Active Directory to Workspace ONE Access, you must install the Directory Sync service component of the Workspace ONE Access connector.

Procedure

- 1 If the Horizon Connection Servers have self-signed certificates, upload the root certificates to the Virtual App service truststore.
 - a On the server on which the Virtual App service is installed, run the Workspace ONE Access connector installer again.
 - b On the **Welcome** page, click **Next**.
 - c On the **Program Maintenance** page, select **Add/Remove Services** and click **Next**.
 - d Click **Next** until the **Install Trusted Root Certificates** page appears.
 - e On the **Install Trusted Root Certificates** page, click **Browse** and upload the certificate.
 - f Save your changes and close the installer.
 - g Restart the VMware Virtual App Service.
- 2 Ensure that the distinguishedName attribute is mapped to the Active Directory attribute distinguishedName.
 - a Log in to the Workspace ONE Access console.
 - b Navigate to the **Identity & Access Management > Directories** page.
 - c Select the directory that contains the users and groups with Horizon entitlements.
 - d On the directory page, click **Sync Settings**, then select the **Mapped Attributes** tab.
 - e Verify that the **distinguishedName** attribute is mapped to the Active Directory **distinguishedName** attribute.

- 3 Sync all users and groups with global or local entitlements in Horizon from Active Directory to the Workspace ONE Access service.
 - a To view current users and groups, click the **Users & Groups** tab.
 - b Select the **Identity & Access Management > Directories** tab.
 - c Select the appropriate directory.
 - d Click **Sync Settings**, review the directory settings, and make changes if needed.
 - e On the directory page, click **Sync** to sync the directory.

Note Users must have the `userPrincipalName` and `distinguishedName` attributes set. If the `userPrincipalName` or `distinguishedName` attribute is not set for a user, the user might not be able to run desktops and applications.

- 4 If applicable, establish a connection to multi-domains or trusted multi-forest domains in Active Directory. See *Directory Integration with VMware Workspace ONE Access* for information.

Configure Horizon Pods and Pod Federations in Workspace ONE Access

Configure Horizon pods and pod federations in the Workspace ONE Access console to sync resources and assignments to the Workspace ONE Access service.

To configure the pods and pod federations, you create one or more virtual apps collections in the **Catalog > Virtual Apps Collections** page and enter configuration information such as the Horizon Connection Servers from which to sync resources and entitlements, pod federation details, the Workspace ONE Access Virtual App service to use for sync, and administrator settings such as the default launch client.

After you add the pods and pod federations, you configure client access FQDNs for specific network ranges so that end users connect to the correct servers when they launch apps and desktops.

You can add all the Horizon pods and pod federations in one collection or you can create multiple collections, based on your needs. For example, you might choose to create separate collections for each pod federation or each pod for easier management and to distribute the sync load across multiple connectors. Or you may choose to include all pods and pod federations in one collection for test purposes and have another identical collection for your production environment.

Important If you change any settings or the SAML configuration on the Horizon server after setting up the integration, and you want to propagate the changes to the Workspace ONE Access service immediately, edit the virtual apps collection page in the Workspace ONE Access console and click **Save**. Otherwise, updates are propagated at the next sync.

Prerequisites

- Set up Horizon according to [Requirements for Integrating Horizon Pods with Workspace ONE Access](#) and [Requirements for Integrating Horizon Pod Federations with Workspace ONE Access](#).
- Set up Workspace ONE Access according to [Set up Your Workspace ONE Access Environment for Horizon Integration](#).
- For each Horizon pod that you want to configure in Workspace ONE Access, ensure that you have the Horizon Connection Server administrator user name and password. The user must have the Administrators role in Horizon.
- To perform this procedure in Workspace ONE Access, you must use an administrator role that includes the Manage Desktop Apps action in the Catalog service.
- At the end of this procedure, you are redirected to the Network Ranges page to configure Client Access FQDNs. To edit and save the Network Ranges page, you require a Super Admin role. You can choose to perform that step separately.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 If an information page appears, review the information and click **Get Started**, otherwise click **New**.
- 4 Select **Horizon** as the source type.
- 5 In the New Horizon Collection wizard, enter the following information in the Connector page.

Option	Description
Name	Enter a unique name for the Horizon virtual apps collection.
Connector	Select the connectors to use to sync this collection. You can add multiple connectors and arrange them in failover order. Only connectors that have the Virtual App service installed appear in the list.

- 6 Click **Next**.

7 In the Pod and Federation page, click **Add a Pod** and enter the pod information.

If the pod has multiple Horizon Connection Server instances, enter the information for any of the instances.

Option	Description
Horizon Connection Server	Enter the fully qualified host name of any one of the Horizon Connection Server instances within the pod. For example, connectionserver.horizondomain.com . The domain name must match the domain name to which the Horizon Connection Server instance is joined. Important If the pod has multiple Horizon Connection Server instances, you need to add only one of the instances. VMware Workspace ONE Access pulls the information for all the instances within the pod.
Username	Enter the Horizon Connection Server administrator user name. The user must have the Administrators role in Horizon.
Password	Enter the Horizon Connection Server administrator password.
Smart Card Authentication	Select this option if users will use smart card authentication instead of passwords to sign in to the Horizon Connection Server.
True SSO	Select this option only if True SSO is enabled for the Horizon Connection Server. This option only applies to Horizon versions that support the True SSO feature. When this option is enabled, users logged into the Workspace ONE app or portal with a non-password authentication method such as SecurID will not be prompted for a password when they launch their Windows desktops.
Sync Local Assignments	Select this option to sync local entitlements from the Horizon Connection Server, in addition to global assignments.

For example:

Add A Pod

Horizon Connection Server * ⓘ
pod2.example.com

Username * ⓘ
admin

Password * ⓘ

Smart Card Authentication ⓘ
 Disabled

True SSO ⓘ
 Disabled

Sync Local Assignments ⓘ
 Enabled

- 8 Click **Add**.
- 9 To add more pods, click **Add a Pod** and enter the information for each pod.
- 10 If the **Cloud Pod Architecture** option is enabled in Horizon for any of the pods that you added, follow these steps to add the pod federation information.
 - a Set the **Have you enabled Cloud Pod Architecture for any of the pods added above option** to **Yes**.
 - b Click **Add a federation**.

- c Enter the pod federation information, then click **Add**.

Option	Description
Federation Name	The name of the pod federation.
Default Client Access FQDN	<p>The fully qualified domain name (FQDN) of the server to which to direct clients accessing global entitlements on this pod federation. This value is typically the global load balancer of the pod federation deployment.</p> <p>For example, federationA.example.com.</p> <p>The Default Client Access FQDN is used to set an initial, default value for the View CPA Federation - Client Access FQDN text box for all network ranges that are currently configured. After creating the collection, go to the collection's Network Ranges tab to customize the View CPA Federation - Client Access FQDN value for each network range.</p> <p>After creating the collection, if you want to update the pod federation's Client Access FQDN, go to the Network Ranges tab and edit the Client Access FQDN value in the View CPA Federation section for each network range. Editing the Default Client Access FQDN value in the Edit Horizon Collection wizard does not update the value in the network ranges.</p> <hr/> <p>Note If you create a network range after creating the collection, make sure that you go to the collection's Network Ranges tab, select the new network range, and add a Client Access FQDN value in the View CPA Federation section. Otherwise, clients using that network range will not be able to access their Horizon desktops and apps.</p>
Horizon Pods	<p>Select all the pods that belong to the pod federation. The Available Pods column displays the pods that you added to the collection. When you select a pod, it is added to the Selected Pods column. You can arrange the pods in the Selected Pods column in failover order.</p> <hr/> <p>Important You must add all the pods that belong to the pod federation to the virtual apps collection and select them here.</p>

For example:

Add A Federation

Federation Name * ⓘ

Horizon Pod Federation A

Default Client Access FQDN * ⓘ

federationA.example.com

Sets the initial value for all existing network ranges. After the collection is created, use the collection's Network Ranges tab to update the Client Access FQDNs. Editing the value here does not update the network ranges.

Horizon Pods

Select one or more pods and arrange them in failover order. At least one pod is required.

Available Pods	Selected Pods
Choose the pods that are associated with the cloud pod federation. <input checked="" type="checkbox"/> pod2.example.com	Selected pods appear here. Arrange them in failover order. pod2.example.com ×

d To add another pod federation, click **Add a federation** and enter the pod federation information.

11 In the Configuration page, enter the following information.

Option	Description
Sync Frequency	Select how often you want to sync applications, desktops, and assignments from the Horizon servers to Workspace ONE Access. You can set up an automatic sync schedule or choose to sync manually. To set a schedule, select the interval such as daily or weekly and select the time of day to run the sync. If you select Manual , you must click Sync > Sync with safeguards or Sync > Sync without safeguards on the virtual apps collection page after you create the collection and whenever there is a change in the Horizon resources or assignments. For more information about sync, see Syncing Virtual Apps Collections in Workspace ONE Access .
Sync Duplicate Apps	Set to No if you want to prevent duplicate applications from being synced from multiple servers. When Workspace ONE Access is deployed in multiple data centers, the same resources are set up in the multiple data centers. Setting this option to No prevents duplication of the desktop or application pools in the Intelligent Hub catalog.

Option	Description
Safeguard Thresholds Limits	<p>Configure sync safeguard thresholds if you want to limit the number of changes that can be made to applications, desktops, and assignments when the virtual apps collection syncs. If any of the thresholds is met, sync is cancelled.</p> <p>By default, Workspace ONE Access sets the threshold for all categories to 10%.</p> <p>Sync safeguards are ignored the first time a collection syncs and are applied to all subsequent syncs.</p> <p>For more information about sync safeguards, see Syncing Virtual Apps Collections in Workspace ONE Access.</p>
Activation Policy	<p>Select how you want to make resources in this collection available to users in the Workspace ONE Intelligent Hub app and portal. If you intend to set up an approval flow, select User-Activated, otherwise select Automatic.</p> <p>With both the User-Activated and Automatic options, the resources are added to the Apps tab. Users can run the resources from the Apps tab or mark them as favorites and run them from the Favorites tab. However, to set up an approval flow for any of the apps, you must select User Activated for that app.</p> <p>The activation policy applies to all user assignments for all the resources in the collection. You can modify the activation policy for individual users or groups per resource, from the user or group page in the Users & Groups tab.</p>
Default Launch Client	<p>Select the default client for end users accessing Horizon desktops and applications from the Intelligent Hub app or portal.</p> <p>None: No default preference is set at the administrator level. If this option is set to None and the end user does not set a preference either, the Horizon Default display protocol setting is used to determine how to launch the desktop or application.</p> <p>Browser: Horizon desktops and applications are launched in a web browser by default. End user preferences, if set, override this setting.</p> <p>Native: Horizon desktops and applications are launched in the Horizon Client by default. End user preferences, if set, override this setting.</p> <p>This setting applies to all users for all resources in this collection.</p> <p>The following order of precedence, listed from highest to lowest, applies to the default launch client settings:</p> <ol style="list-style-type: none"> End user preference setting, set in Intelligent Hub. Administrator Default Launch Client setting for the collection, set in the Workspace ONE Access console. Horizon Remote Display Protocol > Default display protocol setting for the desktop or application pool, set in Horizon Console. For example, when the display protocol is set to PCoIP, the application or desktop is launched in the Horizon Client. <hr/> <p>Important If you integrate Horizon 7.13 or later versions with Workspace ONE Access, end users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers. See the VMware Horizon HTML Access documentation for information.</p>

12 In the Summary page, review your selections, then click **Save & Configure**.

The **Network Ranges** tab appears.

13 In the **Network Ranges** tab, edit each network range and specify Client Access FQDNs for Horizon pods and pod federations so that end users accessing Horizon applications and desktops from that network range connect to the correct server.

See [Setting Client Access FQDNs for Horizon Virtual Apps in Workspace ONE Access](#) for more information on configuring network ranges.

What to do next

The Horizon collection is created and appears in the **Catalog > Virtual Apps Collections** page. Resources in the collection are not yet synced. You can either wait for the next scheduled sync or sync the collection manually from the **Catalog > Virtual Apps Collections** page.

Configure SAML Authentication in Horizon for Workspace ONE Access Integration

After you create a Horizon virtual apps collection in Workspace ONE Access, log in to Horizon Console and configure SAML authentication on the Horizon Connection Server instances to allow users to launch Horizon desktops and applications using single sign-on. When SAML authentication is configured, users logged into the Intelligent Hub app or portal can launch their remote Horizon desktops and applications without going through a second login procedure.

You must configure SAML authentication on at least one Horizon Connection Server instance in a pod. The best practice is to configure SAML authentication on all instances in the pod.

If SAML authentication is not configured on some of the Horizon Connection Server instances in a pod, Workspace ONE Access uses the other instances for sync. However, make sure that any instance that does not have SAML authentication configured is not used for launch, otherwise users cannot launch Horizon desktops or applications. Do not use the instance as the Client Access FQDN or, if the Client Access FQDN points to a load balancer, as one of the nodes on the load balancer.

If none of the Horizon Connection Server instances in the pod have SAML authentication configured, sync fails.

Note You do not need to configure SAML authentication if your organization uses smart card authentication to view resources using a third-party identity provider.

Procedure

- 1 Log in to Horizon Console as a user that has the Administrators role.
- 2 Configure SAML authentication on the Horizon Connection Server instances.

See the relevant version of the [VMware Horizon documentation](#) for information.

Ensure that you specify the FQDN of the Workspace ONE Access service when you configure the SAML Authenticator.

Important The Horizon and Workspace ONE Access servers must be in time sync. If the servers are not in time sync, when users access a Horizon application or desktop, an invalid SAML message occurs.

What to do next

Important If you change any settings or SAML configuration on the Horizon server, and you want to propagate the changes to the Workspace ONE Access service immediately, edit the virtual apps collection page in the Workspace ONE Access console and click **Save**. Otherwise, updates are propagated at the next sync.

Setting Client Access FQDNs for Horizon Virtual Apps in Workspace ONE Access

As part of integrating Workspace ONE Access and Horizon, you specify Client Access FQDNs for network ranges so that users connect to the correct Horizon server based on their network range. Additionally, you can filter users by specifying user groups for each network range.

When you create a Horizon virtual apps collection, the wizard guides you to the Network Ranges tab to configure the Client Access FQDNs for the pods and pod federation in the collection. After creating the collection, you can edit the Client Access FQDNs at any time from the Network Ranges tab.

All network ranges in your tenant must have Client Access FQDNs set for Horizon pods and pod federations. If a network range does not have a Client Access FQDN defined, users accessing Horizon resources through that network range cannot launch their assigned applications and desktops. Make sure that whenever you create new network ranges, you also edit the virtual apps collections to add Client Access FQDNs for Horizon pods and pod federations to the new network range.

You can configure Client Access FQDNs in Workspace ONE Access in the following ways:

- Use only network ranges to direct users to the appropriate Client Access FQDNs.

Create multiple network ranges and specify Client Access FQDNs for each network range. Do not select any user groups for the network ranges. All users will be directed to Client Access FQDNs based on the network range from which they are accessing their assigned Horizon apps and desktops.

For example, you can create separate network ranges for internal and external access and specify the appropriate Client Access FQDNs for each range.
- Use both network ranges and groups to direct users to the appropriate Client Access FQDNs.

Create multiple network ranges and specify Client Access FQDNs for each range. Also select user groups for the network ranges. For users to be able to launch Horizon apps and desktops from a Client Access FQDN, their client IP address must match the network range and they must belong to at least one of the groups selected for the network range. If no groups are selected for a network range, all users whose client IP address matches the network range can launch apps and desktops from that network range's Client Access FQDN.

For example, you can create separate network ranges for internal and external access and filter users for each range based on whether they belong to a permanent employee group or a temporary employee group.

Note If you do not want to create multiple network ranges, you can configure user groups on the default **ALL RANGES** network range for each virtual apps collection. Only users that belong to one of the selected groups will be able to launch Horizon apps and desktops from the **ALL RANGES** Client Access FQDN.

For example, you can create different virtual apps collections for pods in different regions, create user groups by region, and select the appropriate user groups for the **ALL RANGES** network range for each collection.

If you configure overlapping network ranges, Workspace ONE Access applies the following rules to find the best match for the user:

- If the user's client IP address matches multiple ranges and no groups are specified for any of the network ranges, then the network range that was created most recently is used to determine the Client Access FQDN for the user.
- If the user's client IP address matches multiple network ranges and the user's groups match only one of those network ranges, then the network range that matches both the client IP address and groups is used to determine the Client Access FQDN for the user.
- If the client IP address matches multiple network ranges and the user belongs to one or more groups in all those network ranges, then the network range that has the most user group matches will be used to determine the Client Access FQDN for the user.
- If the client IP address matches multiple network ranges and the number of user groups that match is identical across multiple network ranges, then the network range that was created most recently is used to determine the Client Access FQDN for the user.

Prerequisites

A Super Admin role, or a custom role that can perform the Manage Settings action in the Identity and Access Management service, is required to create and edit network ranges.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Click the Horizon virtual apps collection, then select the **Network Ranges** tab.
- 3 Click the network range to edit or create a new network range, if necessary.

- 4 If you are creating a new network range, enter a name, optional description, and the IP range.
- 5 (Optional) In the **Group Membership** section, select the user groups that you want to associate with this network range.

If you select groups, to launch Horizon applications and desktops from the Client Access FQDN associated with this network range, users must belong to at least one of the groups and their client IP address must match the network range.

If you do not select any groups, all users whose client IP address matches the network range can launch Horizon applications and desktops from the Client Access FQDN associated with this network range.

For example:

Assign Pods to Network Ranges

Network Ranges

Name *

Description

IP Ranges ⓘ To

Group Membership

Groups ⓘ

- 6 Scroll to the **Pod and Federation** section.

The Pod section lists all the Horizon pods in the collection that have the Sync Local Assignments option enabled. The CPA Federation section lists the pod federations in the collection, if any.

Pod	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT ⓘ
pod1.example.com	<input type="text" value="pod1.example.com"/>	<input type="text" value="443"/>	No <input type="checkbox"/>	<input type="button" value="ADD"/>

View CPA Federation	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT
Fed	<input type="text" value="pod2.example.com"/>	<input type="text" value="443"/>	No <input type="checkbox"/>	<input type="button" value="ADD"/>

- 7 Edit the **Pod** section for each pod and enter the appropriate values for this network range.

Option	Description
Client Access FQDN	The fully qualified domain name (FQDN) of the server to which to direct clients accessing local entitlements on this pod, when the requests come from this network range. This value can be a Horizon Connection Server, Unified Access Gateway, load balancer, or reverse proxy FQDN. For example: internal1b.example.com The Client Access FQDN for a pod is used to launch locally entitled resources from the pod.
Port	The server port.
Wrap Artifact in JWT	See Launching Horizon Resources Through Validating Gateways .
Audience in JWT	See Launching Horizon Resources Through Validating Gateways .

- 8 Edit the **CPA Federation** section for each pod federation and enter the appropriate values for this network range.

Option	Description
Client Access FQDN	The fully qualified domain name (FQDN) of the server to which to direct clients accessing global entitlements on this pod federation, when the requests come from this network range. This value is typically the global load balancer of the pod federation deployment. For example: global1b.example.com The Client Access FQDN for a pod federation is used to launch globally entitled resources.
Port	The server port.
Wrap Artifact in JWT	When the Workspace ONE Access service is integrated with a validating gateway, such as F5, this option must be enabled to authenticate Horizon resources assigned to users. See Launching Horizon Resources Through Validating Gateways .
Audience in JWT	See Launching Horizon Resources Through Validating Gateways .

- 9 Click **Save**.
- 10 Repeat these steps to edit the other network ranges, if necessary.

Important Verify that each network range in your environment has a Client Access FQDN set. If a network range is missing the Client Access FQDN, users accessing resources through that network range cannot launch their Horizon desktops and applications.

Launching Horizon Resources Through Validating Gateways

When the Workspace ONE Access service is integrated with a validating gateway, such as F5, the Wrap Artifact in JWT setting must be enabled in the Workspace ONE Access service to authenticate Horizon resources assigned to users.

When Wrap Artifact in JWT is enabled to authenticate a Horizon resource launch request, the Workspace ONE Access service generates a digitally signed JWT token that includes the SAML artifact to allow for verification.

This JWT token is sent to the validating gateway in the DMZ. The gateway validates the JWT token from Workspace ONE Access and extracts the SAML artifact value from the token. The gateway forwards the request with the real SAML artifact value to the Horizon Connection Server. The Connection Server verifies the request and the user is signed in to the Horizon resource.

If Wrap Artifact in JWT is not enabled, the validating gateway does not pass the artifact to the Horizon Connection Server for validation and authentication fails.

Prerequisites

- The validating gateway must be configured with the following Workspace ONE Access details.
 - SSL Certificate
 - OAuth2 client ID and secret
 - Workspace ONE Access validation endpoint URL
- A Super Admin role is required in Workspace ONE Access to perform this procedure.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click the Horizon collection to edit, then click **Edit Network Range**.
- 4 Click the network range of IP addresses that the Horizon resource can use.

The Pod section lists all the Horizon pods that you added to the collection that have the Sync Local Entitlements option selected. See [Configure Horizon Pods and Pod Federations in Workspace ONE Access](#) for steps to configure the Client Access FQDNs for pods and pod federations.

- 5 In the Pod section, enable the **Wrap Artifact in JWT** option on the Horizon environment that is configured.

Pod	Client Access FQDN ⓘ	Port	Wrap Artifact in JWT ⓘ	Audience in JWT ⓘ
pod2vcs1.hs.trcint.com	<input type="text" value="pod2vcs1.hs.trcint.com"/>	443 ⌵	Yes <input checked="" type="checkbox"/>	<input type="text" value="ADD"/>

- 6 If more than one validating gateway can process requests, create unique identifiers and add the names to the **Audience in JWT** text box.

This audience name is configured in the validating gateway setup and is used to verify that this gateway is the intended audience. If the audience in JWT does not match the audience name configured here, the request is rejected.

7 Click **Save**, then click **Finish** in the Network Ranges page.

What to do next

The unique audience names that you add here must also be added to the validating gateway configuration.

Viewing Horizon Desktop and Application Pool Information in Workspace ONE Access

After integrating Workspace ONE Access and Horizon, you can view details about the Horizon desktop and application pools that are synced to Workspace ONE Access from the Horizon servers.

Procedure

- 1 In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
- 2 Click the icon in the **Type** column heading and select either **Horizon Desktop** or **Horizon Application**, or both, to view all Horizon desktop and application pools.

You can also search for a specific pool by name.

- 3 Click the desktop or application name.

The **Definition** section in the application page lists information synced from Horizon, including the following:

- Application UUID
- External ID
- Pool name
- Supported client types
- Horizon Connection Server from which the pool is synced

Note From this page, you can also edit Workspace ONE Access settings for the application, such as categories, access policies, and licensing.

Viewing User and Group Assignments for Horizon Desktop and Application Pools in Workspace ONE Access

In the Workspace ONE Access console, you can view user and group assignments for Horizon desktop and application pools. These assignments are set in Horizon and synced to Workspace ONE Access. You cannot edit the assignments from Workspace ONE Access.

Prerequisites

- To see the latest updates, manually sync resources and assignments from the Horizon Connection Server instances to Workspace ONE Access from the **Catalog > Virtual Apps Collections** page.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 View user and group assignments for Horizon desktop and application pools.

Option	Action
List users and groups assigned to a specific Horizon desktop or application pool	<ol style="list-style-type: none">a Click the Catalog > Virtual Apps tab.b (Optional) Click the icon in the Type column heading and search for the pool by name or select Horizon Desktop or Horizon Application to view all Horizon desktop or application pools.c Click the desktop or application.d Click View Assignments. All users and groups to whom the application is assigned are listed.
List Horizon desktop and application pools assignments for a specific user or group	<ol style="list-style-type: none">a Click the Users & Groups tab.b Click the Users tab or the Groups tab.c Click the name of an individual user or group.d Click the Apps tab. Horizon desktop and application pool assignments for the user or group are listed.

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access

The default access policy set applies to all applications and desktops in your Workspace ONE Access catalog. You can also set access policies for individual applications or desktops, which override the default access policy.

You can configure application policies for desktops and applications from the application configuration page or from the Policies page in the Workspace ONE Access console.

For detailed information on access policies and how they are applied, see the *Workspace ONE Access Administration Guide*.

Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
 - a In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
 - b Click the application.

- c Click **Edit**.
Certain fields on the application page are now editable.
 - d In the **Access Policies** section, select the access policy for the application.
 - e Click **Save** at the top of the page.
- 2 To apply an access policy to one or more applications and desktops from the Policies page, follow these steps.
- a In the Workspace ONE Access console, navigate to the **Identity & Access Management > Policies** page.
 - b Click a policy to edit or click **Add Policy** to create a new policy.
 - c In the Definition page of the wizard, in the **Applies to** section, select the applications and desktops to which you want to apply the policy.
 - d In the **Applies to** section, select the applications to which you want to apply the policy.
 - e Save your changes.

Allowing Users to Reset Their Horizon Desktops from the Workspace ONE Catalog

You can configure Horizon and Workspace ONE Access to provide users the ability to reset an unresponsive Horizon desktop from the Workspace ONE Intelligent Hub app or portal.

You configure this setting in the Horizon Console, not in the Workspace ONE Access console. The configuration applies to both Horizon and Workspace ONE Access. In the Workspace ONE Access console, you can view whether a specific desktop is resettable or not.

The option to reset desktops from Workspace ONE Access is supported for:

- Horizon 7.x or later pods
- Dedicated and floating Horizon desktops

Prerequisites

- Configure Horizon to allow users to reset their desktops. See the documentation for VMware Horizon.
- For Horizon desktops to be resettable by users, the client access FQDNs for the respective pods must have trusted certificates. If the URLs have root-signed or self-signed certificates, configure Workspace ONE Access to trust those certificates. See *VMware Workspace ONE Access Installation and Configuration* for information about adding a root certificate.

Procedure

- ◆ (Optional) Verify that Workspace ONE Access lists the desktop as resettable by users.
 - a In the Workspace ONE Access console, select the **Catalog > Virtual Apps** tab.
 - b (Optional) Click the icon in the **Type** column heading and search for the desktop by name or select **Horizon Desktop** to view all Horizon desktops.
 - c Click the desktop.
 - d In the **Definition** section of the page, verify that the **Reset Allowed** setting is set to **Enabled**.

If it is set to **Disabled**, Horizon is not configured to allow users to reset the desktop.

What to do next

If a Horizon desktop becomes unresponsive, administrators or users can reset the desktop by using the **Reset** command.

Viewing Launch Options for Horizon Desktops and Applications in Workspace ONE Access

Users can launch Horizon desktops and applications from the Workspace ONE Intelligent Hub app or portal in Horizon Client or a Web browser, based on how the desktop or application is configured in Horizon. If a desktop or application is only configured for Horizon Client, users must install Horizon Client on their systems.

The Horizon HTML Access feature enables Horizon administrators to configure a desktop or application for browsers. This configuration is done in Horizon and no configuration is required in Workspace ONE Access. See the [VMware Horizon HTML Access](#) documentation for information.

In Horizon 7 versions prior to 7.13, the **Allow HTML Access to desktop and applications on this farm** setting determines whether users in Workspace ONE Access have the option to launch desktops or applications from that farm in a browser.

In Horizon 7.13 and later versions, HTML Access is enabled by default for all resources in a farm. End users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers.

Workspace ONE Access also supports all the display protocols that Horizon supports for Horizon Client. For Horizon 7, Workspace ONE Access supports the Blast protocol in addition to PCoIP and RDP for Horizon Client 4.0. When Workspace ONE Access users launch a desktop or application in Horizon Client, it uses the protocol that is set in Horizon.

Note In Horizon, in addition to setting the default display protocol, administrators can specify whether users are allowed to choose a display protocol. If you want to support versions of Horizon Client that do not support the default protocol, allowing users to choose the display protocol is recommended. Otherwise, the application or desktop cannot be launched.

For information about configuring the display protocols and launch options, see the Horizon documentation.

In the Workspace ONE Access console, you can check the launch options that a Horizon desktop or application supports.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Click the **Catalog > Virtual Apps** tab.
- 3 (Optional) Click the icon in the **Type** column heading and select either **Horizon Desktop** or **Horizon Application**, or both, to view all Horizon desktop and application pools.

You can also search for a specific pool by name.

- 4 Click the desktop or application name.

In the Definition section, the **Supported client types** field displays the launch options that are set in Horizon.

Definition

Name	Version
Paint	1.0
Type	UUID
Horizon Application	af1d2877-7e32-356e-8ade-6705e58ee91d
Pool Name (CN)	External ID (SID)
CN=Paint,OU=Applications,DC=vdi,DC=vmware,DC=int	Application/YmJmZThiMzYlZDIiYS00MjRkLWE5MWhlNTNiY2JiZDQyM... Copy
Connection Server	Supported Client Types
pod2vcs1.hs.trcint.com	NATIVE, BROWSER
Reset Allowed	Categories
Disabled	—

The value can be **NATIVE** or **BROWSER**, or both. If only **NATIVE** is listed, the desktop or application can only be launched in Horizon Client. Users must install Horizon Client on their systems before starting the application from the Hub catalog. If **BROWSER** is listed, users can start the application or desktop in a browser. If both are specified, users can select how they want to start the application.

Note In Horizon 7 versions prior to 7.13, the **Allow HTML Access to desktop and applications on this farm** option must be enabled for the **BROWSER** option to appear in the **Supported client types** list.

Note In Horizon 7.13 and later, HTML Access must be installed on the Horizon Connection servers for browser launch to work.

Launching Horizon Desktops and Applications Integrated with Workspace ONE Access

When you integrate Horizon pods and pod federations with Workspace ONE Access, users can launch their assigned Horizon desktops or applications from the Workspace ONE Intelligent Hub app or portal.

Based on how an application or desktop is configured in Horizon, it can be launched in Horizon Client or in a browser. For applications or desktops that can only be launched in Horizon Client, users must install Horizon Client on their systems. For applications and desktops that can be launched in either Horizon Client or a browser, users can select the launch method.

Users can also set their default launch preference from their Account page in the Intelligent Hub portal. This user preference overrides any default launch preference set at the administrator level.

Note Users cannot set a default launch preference in the Intelligent Hub app.

Prerequisites

- Based on how the application or desktop is configured in Horizon, users might need to install Horizon Client. For supported Horizon Client versions, see the [VMware Product Interoperability Matrix](#).
- If you integrate Horizon 7.13 or later versions with Workspace ONE Access, end users always see the option in Intelligent Hub to launch applications and desktops in a browser. However, if HTML Access is not installed on the Horizon Connection servers, browser launch fails. For Horizon 7.13 and later versions, you must install HTML Access on the Horizon Connection servers. See the [VMware Horizon HTML Access](#) documentation for information.

Procedure

- 1 Log in to the Intelligent Hub app or portal.

- 2 Click the three dots on the desktop or application you want to launch and select **Launch from Client**, **Launch from Browser**, or **Launch from Chrome Client**. The **Launch from Chrome Client** option appears when you are running Intelligent Hub on a Chromebook.

Results

The application or desktop starts.

If the user chose the **Browser** option, the application or desktop is started in a browser. The browser window also displays an HTML Access sidebar.

Beginning with Horizon 2006, all running applications and desktops that are launched directly from the Hub catalog (and not from the sidebar) appear in the Running list in the HTML Access sidebar. The following exceptions apply:

- If the **Clean Up Credential When Tab Closed for HTML Access** setting is enabled in Horizon, only the last-opened Horizon desktop session appears in the sidebar. This limitation does not apply to application sessions.
- Only the same type of sessions, sessions with the **Multi-Session Mode** setting selected or sessions with the **Multi-Session Mode** setting deselected, appear in the sidebar.

Note When a user launches an application or desktop, Workspace ONE Access refreshes the SAML metadata from the Horizon Connection Server instances. However, if the application or desktop does not launch, sync the Horizon resources to Workspace ONE Access again. Navigate to the **Catalog > Virtual Apps Collections** page, select the collection, and click **Sync > Sync with safeguards** or **Sync > Sync without safeguards**.

Providing Access to VMware Horizon Cloud Service Desktops and Applications in Workspace ONE Access

5

You can integrate your Horizon Cloud Service tenant with your Workspace ONE Access tenant to provide users the ability to access Horizon Cloud desktops and applications from the Workspace ONE Intelligent Hub app and portal. This lets you provide users a single place to access all their applications securely from multiple devices.

Types of Horizon Cloud-Workspace ONE Access Integrations

There are two methods for integrating Horizon Cloud with Workspace ONE Access. The type of integration method you use depends on the type of Horizon Cloud environment that you have.

- Horizon Cloud Service on Microsoft Azure with Universal Broker environments

For these environments, you set up the integration between Horizon Cloud and Workspace ONE Access in the Horizon Cloud administration console. Horizon Cloud assignments are pulled into the Intelligent Hub catalog directly from Horizon Cloud when users log into the Hub portal. Assignments do not have to be synced to Workspace ONE Access first.

This integration method is available for Workspace ONE Access Cloud only. A Workspace ONE Access connector is required to sync users and groups from Active Directory to your Workspace ONE Access tenant.

For information about using this integration method, see [Horizon Cloud Environment with Universal Broker - Integrate the Tenant with Workspace ONE Access and Intelligent Hub Services](#) in the Horizon Cloud Service documentation.

- Horizon Cloud Service on Microsoft Azure with Single-Pod Broker environments, and Horizon Cloud Service on IBM Cloud environments

For these environments, you integrate Horizon Cloud with Workspace ONE Access by creating a Virtual Apps collection in the Workspace ONE Access console and syncing user entitlements from your Horizon Cloud tenant to your Workspace ONE Access tenant. Administrators can view Horizon Cloud desktops and applications in the Workspace ONE Access console. End users access their desktops and apps from the Intelligent Hub app or portal.

A Workspace ONE Access connector is required to sync resources and entitlements from Horizon Cloud to your Workspace ONE Access tenant as well as to sync users and groups from Active Directory to your Workspace ONE Access tenant.

Important Only Workspace ONE Access connector version 19.03.0.1 supports integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and Horizon Cloud Service on IBM Cloud.

For information about using this integration method, follow the requirements and procedures described in this document. Also see [A Horizon Cloud Environment with Single-Pod Brokering – Integrating the Environment's Horizon Cloud Pods in Microsoft Azure with Workspace ONE Access](#) in the Horizon Cloud Service on Microsoft Azure documentation.

This chapter includes the following topics:

- [Integrating Workspace ONE Access with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker or Horizon Cloud Service on IBM Cloud](#)
- [Viewing Horizon Cloud Desktop and Application Pool Information in Workspace ONE Access](#)
- [Viewing User and Group Assignments for Horizon Cloud Desktops and Applications](#)
- [Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access](#)
- [Allowing Users to Reset Horizon Cloud Desktops from the Workspace ONE Catalog](#)
- [Launching Horizon Cloud Desktops and Applications Integrated with Workspace ONE Access](#)

Integrating Workspace ONE Access with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker or Horizon Cloud Service on IBM Cloud

The process for integrating Workspace ONE Access with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker or Horizon Cloud Service on IBM Cloud includes creating one or more virtual apps collection in the Workspace ONE Access console and syncing Horizon Cloud assignments to Workspace ONE Access with the Workspace ONE Access connector. You must also configure SAML authentication to enable trust between the Horizon Cloud tenant and the Workspace ONE Access service.

Important Only Workspace ONE Access connector version 19.03.0.1 supports this integration.

Desktop and application pools, also known as assignments, are configured in the Horizon Cloud environment. You also set user and group entitlements in the Horizon Cloud tenant, not in the Workspace ONE Access service. You must sync these users and groups to the Workspace ONE Access service from Active Directory before integrating Workspace ONE Access with your Horizon Cloud tenant.

To integrate Horizon Cloud with Workspace ONE Access, you create one or more virtual apps collections in the Workspace ONE Access console. The virtual apps collections contain the configuration information for the Horizon Cloud tenants as well as sync settings.

You can set up a sync schedule for each virtual apps collection to regularly sync assignments from the Horizon Cloud tenants to the Workspace ONE Access service.

After you integrate the Horizon Cloud tenant with Workspace ONE Access, you can see the Horizon Cloud desktops and applications in the Workspace ONE Access console. You can also view user and group entitlements.

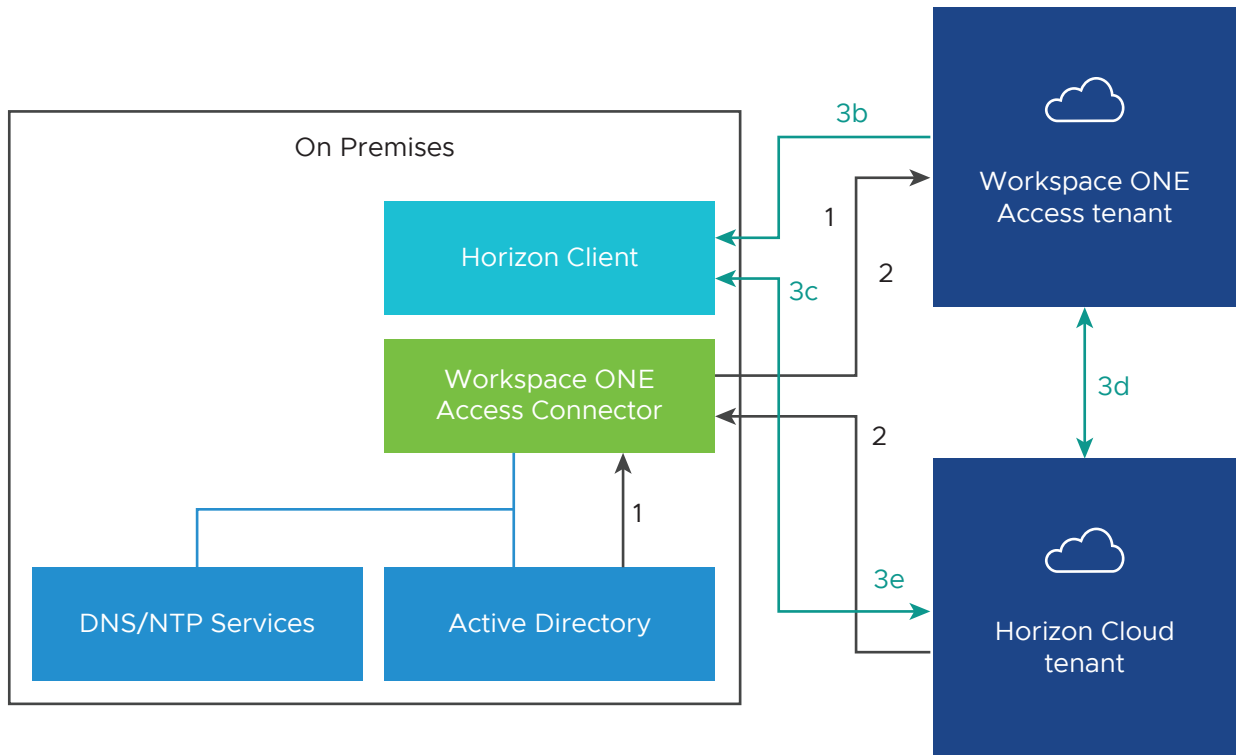
End users can launch their entitled desktops and applications from the Workspace ONE Intelligent Hub portal or app. These desktops and applications can be accessed in a browser or in the VMware Horizon[®] Client[™]. Horizon Client versions 3.4 and later are supported.

Deployment Scenario for Horizon Cloud Integration with Workspace ONE Access

To integrate Workspace ONE Access with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker or Horizon Cloud Service on IBM Cloud, you need a Horizon Cloud tenant, a Workspace ONE Access tenant, and a Workspace ONE Access connector. You must install the connector on premises with line-of-sight to the Horizon Cloud tenant.

Important Only Workspace ONE Access connector version 19.03.0.1 supports this integration.

Figure 5-1. Horizon Cloud Integration with Workspace ONE Access



- 1 The Workspace ONE Access connector syncs user and group information from Active Directory to the Workspace ONE Access tenant.
- 2 The connector syncs Horizon Cloud user and group entitlements from the Horizon Cloud tenant to the Workspace ONE Access tenant.
- 3 The end user accesses a desktop or application as follows:
 - a The end user logs into the Intelligent Hub app or portal and clicks on a desktop or application.
 - b The Workspace ONE Access service generates a launch URL and passes it to the Horizon Client. The launch URL includes a SAML artifact ID.
 - c The Horizon Client accesses the launch URL.
 - d The Horizon Cloud tenant receives the request and validates the SAML artifact ID with the Workspace ONE Access service.
 - e If the SAML artifact ID is validated by the Workspace ONE Access service, the desktop or application is streamed to the Horizon Client by the Horizon Cloud tenant.

About the Workspace ONE Access Connector Requirement

Before you can integrate your Horizon Cloud tenant with Workspace ONE Access, you must install the Workspace ONE Access connector on premises. The connector is required to sync resources and entitlements from Horizon Cloud to your Workspace ONE Access tenant as well as to sync users and groups from Active Directory to your Workspace ONE Access tenant.

Install Workspace ONE Access connector version 19.03.0.1. See *Installing and Configuring VMware Identity Manager Connector 19.03 (Windows)* for information.

Important Do not install a later version as later versions do not support integration with these types of Horizon Cloud Service environments.

After you install and configure the connector, create a directory in your Workspace ONE Access tenant and sync the Active Directory users and groups that have Horizon Cloud desktop and application entitlements.

Integrating Multiple Horizon Cloud Instances with Workspace ONE Access

You can integrate multiple Horizon Cloud tenants with a single instance of Workspace ONE Access so that Horizon Cloud resources and entitlements from all the tenants can be synced to a single location, authentication and access policies can be centrally managed, and end users with entitlements in different tenants can be served from a single portal or app.

Important This topic applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and with Horizon Cloud Service on IBM Cloud, using Workspace ONE Access connector 19.03.0.1.

While integrating multiple Horizon Cloud tenants, take into account the following considerations.

- A single Workspace ONE Access connector can sync resources and entitlements from multiple Horizon Cloud tenants to the Workspace ONE Access service.
- Each Horizon Cloud tenant might provide entitlements for users in different Active Directory instances and domains. Ensure that you add all the relevant directories and domains to Workspace ONE Access so all users with entitlements in any of the Horizon Cloud tenants are synced to Workspace ONE Access.
- If the tenant appliances have self-signed certificates, you must upload the self-signed certificate as a trusted root certificate in Workspace ONE Access. When you integrate multiple Horizon Cloud tenants, you must ensure that all the certificates have the same root certificate as only one root certificate can be uploaded to Workspace ONE Access.
- Workspace ONE Access cannot access and sync entitlements from a tenant on which two-factor authentication is enabled.

- In Workspace ONE Access, you can add all the Horizon Cloud tenants in one configuration, called a virtual apps collection, or create multiple configurations. When all the Horizon Cloud tenants are added to one configuration, if Workspace ONE Access cannot access one of the tenants, it creates an alert and continues to sync resources and entitlements from the other tenants.
- Ensure that you configure SAML authentication in each Horizon Cloud tenant that you integrate with Workspace ONE Access.

Prerequisites for Integrating Workspace ONE Access with Horizon Cloud

Before you integrate your Horizon Cloud tenant with Workspace ONE Access, ensure that you meet the prerequisites listed in this topic. This information applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and Horizon Cloud Service on IBM Cloud environments, using Workspace ONE Access connector 19.03.0.1.

- Verify that you have the following components:
 - A Workspace ONE Access tenant
 - A Workspace ONE Access connector installed on premises

Install Workspace ONE Access connector version 19.03.0.1. See *Installing and Configuring VMware Identity Manager Connector 19.03 (Windows)* for information.

Important Do not install a later version as later versions do not support integration with these types of Horizon Cloud Service environments.

- One or more Horizon Cloud tenants that can be accessed by the Workspace ONE Access connector
- Verify that each Horizon Cloud tenant meets the following requirements.
 - The tenant name must be a fully qualified domain name (FQDN), not just a host name. For example, `server-tal.example.com` instead of `server-tal`.
 - The tenant appliances must have valid, signed certificates issued by a CA. The certificate must match the FQDN of the tenant appliance. If the tenant appliances have self-signed certificates, you must upload the root certificate as a trusted root certificate on the Workspace ONE Access connector, using the connector admin pages at `https://connectorFQDN:8443/cfg/login`. When you integrate multiple Horizon Cloud tenants, you must ensure that all the certificates have the same root certificate as only one root certificate can be uploaded to Workspace ONE Access.
- If the Workspace ONE Access connector is using an outbound proxy server, the proxy server must have a valid, CA-signed certificate. If the proxy server has a self-signed certificate, you must upload its root certificate as a trusted root certificate on the connector, using the connector admin pages at `https://connectorFQDN:8443/cfg/login`.

- Ensure that the Horizon Cloud tenants and the Workspace ONE Access service are in time sync. If they are not in time sync, an invalid SAML error can occur when users run Horizon Cloud desktops and applications.
- Create and configure desktop and application pools, also known as assignments, in the Horizon Cloud tenant administration console. You can create the following types of pools in the Horizon Cloud tenant:
 - Dynamic desktop pool, also known as floating desktop assignment
 - Static desktop pool, also known as dedicated desktop assignment
 - Session-based pool with desktops, also known as session desktop assignment
 - Session-based pool with applications, also known as remote application assignment

For more information about the types of pools, see the Horizon Cloud documentation.

- Set user and group entitlements to Horizon Cloud desktops and applications in the Horizon Cloud tenant administration console.

Note Only entitlements for users that belong to a registered group are synced. Users who do not belong to any group will not see their entitlements in Workspace ONE Access.

- In the Workspace ONE Access console, ensure that users and groups with Horizon Cloud entitlements are synced from Active Directory to Workspace ONE Access using directory sync.

Follow these guidelines:

- If you are integrating multiple Horizon Cloud tenants, ensure that you add all the relevant directories and domains to Workspace ONE Access so that users with entitlements in any of the Horizon Cloud tenants are synced to Workspace ONE Access.
- sAMAccountName must be set as the directory search attribute for the directory in Workspace ONE Access.
- Ensure that the distinguishedName attribute is mapped to the Active Directory attribute distinguishedName.

- 1 In the Workspace ONE Access console, navigate to the **Identity & Access Management > Directories** page.
- 2 Select the directory that contains the users and groups with Horizon Cloud entitlements.
- 3 On the directory page, click **Sync Settings**, then select the **Mapped Attributes** tab.
- 4 Verify that the **distinguishedName** attribute is mapped to the Active Directory **distinguishedName** attribute.

Note Users must have the distinguishedName attribute set. If the distinguishedName attribute is not set for a user, the user might not be able to run desktops and applications.

Configure Horizon Cloud Tenant in Workspace ONE Access

To integrate Horizon Cloud tenants with the Workspace ONE Access service, you create a virtual apps collection in the Workspace ONE Access console, which contains Horizon Cloud tenant information as well as sync settings, and sync resources and entitlements from the Horizon Cloud tenant to the Workspace ONE Access service.

If you have multiple Horizon Cloud tenants, you can create separate virtual apps collections for each tenant or configure all the tenants in a single collection, based on your needs. Each collection syncs separately.

Note This topic applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and with Horizon Cloud Service on IBM Cloud, using Workspace ONE Access connector 19.03.0.1.

Prerequisites

- Verify that you meet the prerequisites described in [Prerequisites for Integrating Workspace ONE Access with Horizon Cloud](#). See also [Integrating Multiple Horizon Cloud Instances with Workspace ONE Access](#).
- You must use an administrator role that can perform the Manage Desktop Apps action in the Catalog service.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click **New**.
- 4 Select **Horizon Cloud** as the source type.
- 5 In the New Horizon Cloud Virtual Apps Collection wizard, enter the following information in the Connector page.

Option	Description
Name	Enter a unique name for the Horizon Cloud collection.
Connector	Select the connector that you want to use to sync this collection. To select the connector, select the directory that is associated with it. If you have set up a cluster of connectors, all the connector instances appear in the Host list and you can arrange them in failover order for this collection. Important After you create the collection, you cannot select a different directory.

- 6 Click **Next**.

- 7 In the Tenant page, click **Add a Tenant** and enter your Horizon Cloud tenant information.

Important Do not use non-ASCII characters when you enter your domain information.

Option	Description
Host	Fully-qualified domain name of your Horizon Cloud tenant host. For example: tenant1.example.com
Port	Port number of your Horizon Cloud tenant host. For example: 443
Admin User	User name for your Horizon Cloud tenant administrator account. For example: tenantadmin
Admin Password	Password for your Horizon Cloud tenant administrator account.
Admin Domain	Active Directory NETBIOS domain name in which the Horizon Cloud tenant administrator resides.
Domains to Sync	Active Directory NETBIOS domain names for syncing Horizon Cloud resources and entitlements. Note This field is case-sensitive. Ensure that you use the proper case when you enter the names.
Assertion Consumer Service URL	The URL to which to post the SAML assertion. This URL is typically the Horizon Cloud tenant's floating IP address or hostname, or the Unified Access Gateway URL. For example, https://mytenant.example.com .
True SSO	Select this option only if True SSO is enabled for the Horizon Cloud tenant. When this option is enabled, users logged into the Intelligent Hub portal or app with a non-password authentication method such as SecurID will not be prompted for a password when they launch their Windows desktops.
Custom ID Mapping	<p>You can customize the user ID that is used in the SAML response when users launch Horizon Cloud applications and desktops. By default, User Principal Name is used. You can choose to use other name ID formats such as sAMAccountName or email address and customize the value.</p> <p>Name ID Format: Select the name ID format, such as Email address or User Principal Name. The default value is Unspecified (username).</p> <p>Name ID Value: Click Select from suggestions and pick from a predefined list of values or click Custom value and enter the value. This value can be any valid Expression Language (EL) expression such as \${user.userName}@\${user.domain}. The default value is \${user.userPrincipalName}.</p> <p>Note Ensure that the attributes you use in the expression are mapped attributes in the VMware directory. You can view mapped attributes in the directory's Sync Settings tab. In the above example, <code>userName</code>, <code>userPrincipalName</code>, and <code>domain</code> are directory mapped attributes.</p> <p>The ability to select the name ID format is useful in scenarios such as the following:</p> <ul style="list-style-type: none"> When users from multiple sub-domains are synced, User Principal Name may not work. You can use a different name ID format such as sAMAccountName or email address to uniquely identify users. <p>Important Ensure that you use the same name ID format setting in Horizon Cloud and Workspace ONE Access.</p>

- 8 Click **Add**.
- 9 Add other tenants, if required, then click **Next**.
- 10 In the Configuration page, enter the following information.

Option	Description						
Sync Frequency	<p>Select how often you want to sync the resources in the collection.</p> <p>You can set up an automatic sync schedule or choose to sync manually. To set a schedule, select the interval such as daily or weekly and select the time of day to run the sync. If you select Manual, you must click Sync on the Virtual Apps Collections page after you set up the collection and whenever there is a change in your Horizon Cloud resources or entitlements.</p>						
Activation Policy	<p>Select how you want to make resources in this collection available to users in the Intelligent Hub portal and app. If you intend to set up an approval flow, select User-Activated, otherwise select Automatic.</p> <p>With both the User-Activated and Automatic options, the resources are added to the Apps page. Users can use the resources from the Apps page or mark them as favorites and run them from the Favorites page. However, to set up an approval flow for any of the apps, you must select User Activated for that app.</p> <p>The activation policy applies to all user entitlements for all the resources in the collection. You can modify the activation policy for individual users or groups per resource, from the user or group page in the Users & Groups tab.</p>						
Default Launch Client	<p>Select the default client for end users accessing Horizon Cloud desktops and apps from the Intelligent Hub portal or app.</p> <table border="1"><tbody><tr><td>None</td><td>No default preference is set at the administrator level. If this option is set to None and the end user does not set a preference either, the Horizon Cloud Default Protocol setting is used to determine how to launch the desktop or application.</td></tr><tr><td>Browser</td><td>Horizon Cloud desktops and applications are launched in a web browser by default. End user preferences, if set, override this setting.</td></tr><tr><td>Native</td><td>Horizon Cloud desktops and applications are launched in the Horizon Client by default. End user preferences, if set, override this setting.</td></tr></tbody></table> <p>This setting applies to all users for all resources in this collection.</p> <p>The following order of precedence, listed from highest to lowest, applies to the default launch client settings:</p> <ol style="list-style-type: none">a End user preference setting, set in Intelligent Hub.b Administrator Default Launch Client setting for the collection, set in the Workspace ONE Access console.c Horizon Cloud Default Protocol settings	None	No default preference is set at the administrator level. If this option is set to None and the end user does not set a preference either, the Horizon Cloud Default Protocol setting is used to determine how to launch the desktop or application.	Browser	Horizon Cloud desktops and applications are launched in a web browser by default. End user preferences, if set, override this setting.	Native	Horizon Cloud desktops and applications are launched in the Horizon Client by default. End user preferences, if set, override this setting.
None	No default preference is set at the administrator level. If this option is set to None and the end user does not set a preference either, the Horizon Cloud Default Protocol setting is used to determine how to launch the desktop or application.						
Browser	Horizon Cloud desktops and applications are launched in a web browser by default. End user preferences, if set, override this setting.						
Native	Horizon Cloud desktops and applications are launched in the Horizon Client by default. End user preferences, if set, override this setting.						

- 11 Click **Next**.
- 12 In the Summary page, review your selections, then click **Save**.

The collection is created and appears in the Virtual Apps Collections page.

- 13 To sync the resources and entitlements in the collection, select the collection in the Virtual Apps Collections page and click **Sync**.

Each time resources or entitlements change in Horizon Cloud, a sync is required to propagate the changes to Workspace ONE Access.

What to do next

Configure SAML authentication in the Horizon Cloud tenant to enable trust between the Workspace ONE Access service and the Horizon Cloud tenant.

Configure SAML Authentication in the Horizon Cloud Tenant for Workspace ONE Access Integration

After you create a virtual apps collection for the Horizon Cloud integration in the Workspace ONE Access console, configure SAML authentication in the Horizon Cloud tenant.

If you are integrating multiple Horizon Cloud tenants, ensure that you configure SAML authentication in all the tenants.

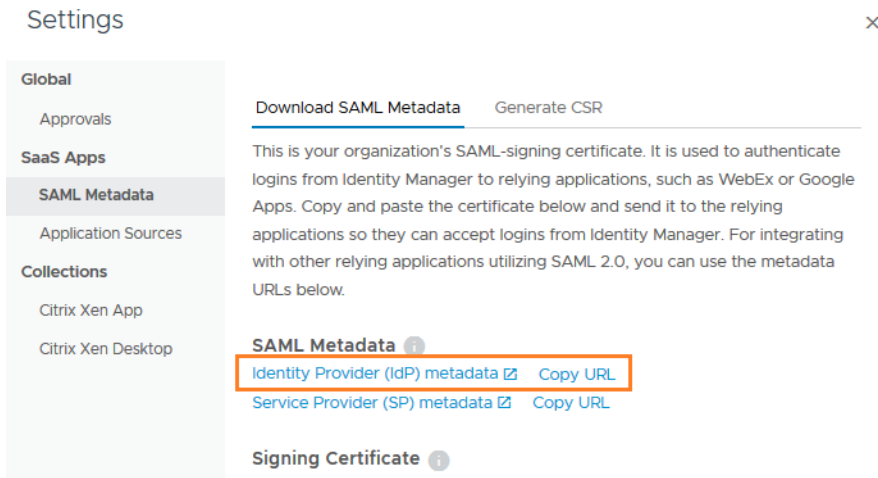
Note This topic applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and with Horizon Cloud Service on IBM Cloud, using Workspace ONE Access connector 19.03.0.1.

Important The Horizon Cloud tenant appliance and Workspace ONE Access must be in time sync. If they are not in time sync, when you try to launch Horizon Cloud desktops and applications, an invalid SAML message appears.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps** tab, then click **Settings**.
- 2 In the left pane, under **SaaS Apps**, click **SAML Metadata**.
- 3 In the **Download SAML Metadata** tab, click **Copy URL** next to the **Identity Provider (IdP) metadata** link.

The URL, which is in a format similar to `https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml`, is copied to your clipboard.



- 4 Log in to the Horizon Cloud tenant.
- 5 Navigate to **Settings > Identity Management**.
- 6 Click **New**.
- 7 Configure the required settings.

Option	Description
Identity Manager URL	The Workspace ONE Access IdP metadata URL you copied. The URL is typically in the following format: <code>https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml</code>
Timeout SSO Token	(Optional) The amount of time, in minutes, after which the SSO token times out.
Data Center	The Horizon Cloud data center name. Select the name from the drop-down list.
Tenant Address	The Horizon Cloud tenant address. Specify the floating IP address or hostname of the Horizon Cloud tenant appliance, or the Unified Access Gateway IP address or hostname. For example, mytenant.example.com.

On Horizon Cloud on Azure, the following settings appear.

Option	Description
VMware Identity Manager URL	The Workspace ONE Access IdP metadata URL you copied. The URL is typically in the following format: <code>https://VMwareIdentityManagerFQDN/SAAS/API/1.0/GET/metadata/idp.xml</code>
Timeout SSO Token	(Optional) The amount of time, in minutes, after which the SSO token times out.
Location	Select a location to filter the Node drop-down list to the nodes associated with that location.
Node	Select the node you are integrating with Workspace ONE Access.

Option	Description
Data Center	The Horizon Cloud data center name. Select the name from the drop-down list.
Tenant Address	The Horizon Cloud tenant address. Specify the floating IP address or hostname of the Horizon Cloud tenant appliance, or the Unified Access Gateway IP address or hostname. For example, mytenant.example.com.

8 Click **Save**.

If the integration is successful, the status is green.

9 To block user access except through Workspace ONE Access, click **Configure** and edit the settings.

Option	Description
Force Remote Users to Identity Manager	Select YES to block remote user access except through IDM. Option only displays if Identity Manager status is green.
Force Internal Users to Identity Manager	Select YES to block internal user access except through IDM. Option only displays if Identity Manager status is green.

Results

Your integration is complete. After you sync Horizon Cloud resources to Workspace ONE Access, you can view Horizon Cloud desktop and application pools in the Workspace ONE Access console and end users can launch the resources to which they are entitled from the Intelligent Hub portal or app.

Viewing Horizon Cloud Desktop and Application Pool Information in Workspace ONE Access

In the Workspace ONE Access console, you can view information about the synced Horizon Cloud desktop and application pools.

Note This topic applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and with Horizon Cloud Service on IBM Cloud, using Workspace ONE Access connector 19.03.0.1.

Procedure

- 1 In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
- 2 Click the icon in the **Type** column heading and select either **Horizon Cloud Desktop** or **Horizon Cloud Application**, or both, to view all Horizon Cloud desktop and application pools.
You can also search for a specific pool by name.

3 Click the desktop or application name.

The **Definition** section in the application page lists attributes synced from the Horizon Cloud tenant, such as the following:

- Application UUID
- Pool name, Pool ID, and Pool Domain
- Supported launch clients

See the Horizon Cloud documentation for information about these attributes.

Note From this page, you can also edit Workspace ONE Access settings for the application, such as categories, access policies, and licensing.

Viewing User and Group Assignments for Horizon Cloud Desktops and Applications

In the Workspace ONE Access console, you can view user and group assignments for Horizon Cloud desktop and application pools. These assignments are set in Horizon Cloud and synced to Workspace ONE Access. You cannot edit the assignments from Workspace ONE Access.

Prerequisites

To see the latest updates, manually sync resources and entitlements from the Horizon Cloud tenants to Workspace ONE Access from the **Catalog > Virtual Apps Collections** page.

Note This topic applies to Workspace ONE Access integration with Horizon Cloud Service on Microsoft Azure with Single-Pod Broker and with Horizon Cloud Service on IBM Cloud, using Workspace ONE Access connector 19.03.0.1.

Procedure

- 1 Log in to the Workspace ONE Access console.

2 View user and group assignments for Horizon Cloud desktop and application pools.

Option	Action
List users and groups assigned to a specific Horizon Cloud desktop or application pool	<ol style="list-style-type: none">Click the Catalog > Virtual Apps tab.(Optional) Click the icon in the Type column heading and search for the pool by name or select Horizon Cloud Desktop or Horizon Cloud Application to view all Horizon Cloud desktop or application pools.Click the desktop or application.Click View Assignments. All users and groups to whom the application is assigned are listed.
List Horizon desktop and application pools assignments for a specific user or group	<ol style="list-style-type: none">Click the Users & Groups tab.Click the Users tab or the Groups tab.Click the name of an individual user or group.Click the Apps tab. Horizon Cloud desktop and application pool assignments for the user or group are listed.

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access

The default access policy set applies to all applications and desktops in your Workspace ONE Access catalog. You can also set access policies for individual applications or desktops, which override the default access policy.

You can configure application policies for desktops and applications from the application configuration page or from the Policies page in the Workspace ONE Access console.

For detailed information on access policies and how they are applied, see the *Workspace ONE Access Administration Guide*.

Procedure

- To select an access policy for a specific application from the application configuration page, follow these steps.
 - In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
 - Click the application.
 - Click **Edit**.

Certain fields on the application page are now editable.
 - In the **Access Policies** section, select the access policy for the application.
 - Click **Save** at the top of the page.

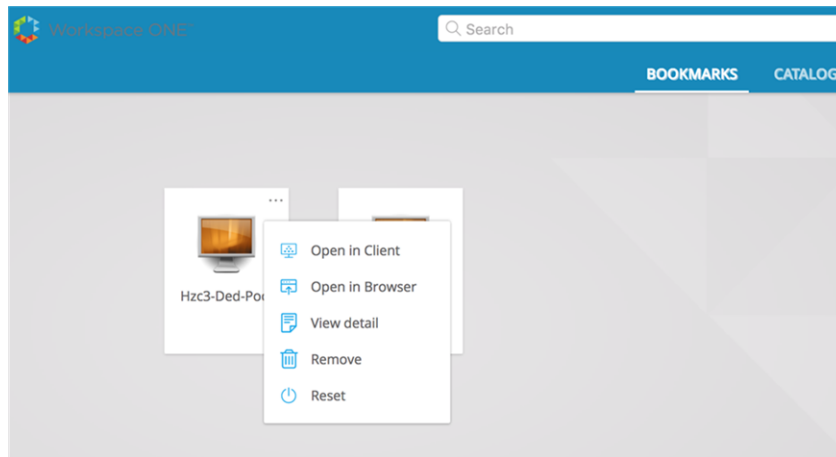
- 2 To apply an access policy to one or more applications and desktops from the Policies page, follow these steps.
 - a In the Workspace ONE Access console, navigate to the **Identity & Access Management > Policies** page.
 - b Click a policy to edit or click **Add Policy** to create a new policy.
 - c In the Definition page of the wizard, in the **Applies to** section, select the applications and desktops to which you want to apply the policy.
 - d In the **Applies to** section, select the applications to which you want to apply the policy.
 - e Save your changes.

Allowing Users to Reset Horizon Cloud Desktops from the Workspace ONE Catalog

Users can reset dedicated Horizon Cloud desktops from the Workspace ONE Intelligent Hub portal or app if the setting in Horizon Cloud allows it. The Reset option is useful when desktops become unresponsive.

The option to allow users to reset their desktops is configured in Horizon Cloud, not in Workspace ONE Access. Only dedicated Horizon Cloud desktops can be reset from Workspace ONE.

If Horizon Cloud allows users to reset desktops, the Reset option is available for the desktop in the Workspace ONE Intelligent Hub portal or app. The option does not appear for desktops for which reset is not allowed.



Launching Horizon Cloud Desktops and Applications Integrated with Workspace ONE Access

When you integrate your Horizon Cloud tenant with Workspace ONE Access, end users can run the Horizon Cloud desktops and applications that are assigned to them from the Workspace ONE Intelligent Hub portal or app.

Based on how an application or desktop has been configured in the Horizon Cloud tenant, it can be run in the Horizon Client or in a browser. For applications or desktops that are configured for the Horizon Client only, users must install the Horizon Client on their systems. For applications and desktops that are configured for both the Horizon Client and browsers, users can select the launch method.

Users can also set their default launch preference from their Account page in the Intelligent Hub portal. This user preference overrides any default launch preference set at the administrator level.

Note Users cannot set a default launch preference in the Intelligent Hub app.

Prerequisites

Based on how the application or desktop has been configured in the Horizon Cloud tenant, users might need to install the Horizon Client.

For supported Horizon Client versions, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedure

- 1 Log in to the Intelligent Hub app or portal.
- 2 Click the three dots on the desktop or application you want to launch and select **Launch from Client** or **Launch from Browser**.

Note Based on how the desktop or application is configured and based on your preference, you might need to install the Horizon Client on your system.

Providing Access to VMware ThinApp Packages in Workspace ONE Access

6

With Workspace ONE Access, you can centrally distribute and manage ThinApp packages. ThinApp packages are virtualized Windows applications, and are used on Windows systems. Entitled users who have the Workspace ONE Access Desktop application installed on their Windows systems can launch and use their entitled ThinApp packages on those Windows systems.

Important ThinApp integration is only available with the legacy VMware Identity Manager connector (Linux) version 2018.8.1.0.

In the ThinApp capture and build processes, you create a virtual application from a Windows application. That virtualized Windows application can run on a Windows system without that system having the original Windows application installed. The ThinApp package is the set of virtual application files generated by running the ThinApp capture and build processes on a Windows application. The package includes the primary data container file and entry point files to access the Windows application.

Not every ThinApp package is compatible with Workspace ONE Access. When you capture a Windows application, the default settings in the ThinApp capture-and-build process create a package that Workspace ONE Access cannot distribute and manage. You create a ThinApp package that Workspace ONE Access can distribute and manage by setting the appropriate parameters during the capture and build processes. See the VMware ThinApp documentation for detailed information on ThinApp features and the appropriate parameters to use to create a package compatible with Workspace ONE Access.

After you integrate Workspace ONE Access with your ThinApp repository, you can see in your catalog those ThinApp packages from the repository that Workspace ONE Access can distribute and manage. After you see the ThinApp packages in your Workspace ONE Access catalog, you can entitle users and groups to those ThinApp packages, and optionally configure license tracking information for each package.

This chapter includes the following topics:

- [Integrating VMware ThinApp Packages with Workspace ONE Access](#)
- [Entitle Workspace ONE Access Users and Groups to ThinApp Packages](#)
- [Distributing and Managing ThinApp Packages with Workspace ONE Access](#)

- [Updating Managed ThinApp Packages After Deployment in Workspace ONE Access](#)
- [Make Existing ThinApp Packages Compatible with Workspace ONE Access](#)
- [Change the ThinApp Packages Share Folder in Workspace ONE Access](#)
- [Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access](#)

Integrating VMware ThinApp Packages with Workspace ONE Access

To use Workspace ONE Access to distribute and manage applications packaged with VMware[®] ThinApp[®], you must have a ThinApp repository that contains the ThinApp packages, point to that repository, and sync the packages. After the sync process is finished, the ThinApp packages are available in your Workspace ONE Access catalog and you can entitle them to your Workspace ONE Access users and groups.

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package. To be managed by Workspace ONE Access, these packages must be enabled with the appropriate options. For example, in the ThinApp Setup Capture wizard, you select the **Manage with Workspace** check box. For more information about ThinApp features and how to enable your applications for management by Workspace ONE Access, see the VMware ThinApp documentation.

Typically, you perform the steps to connect the Workspace ONE Access connector to the repository and sync the packages as part of the overall setup and configuration of your Workspace ONE Access environment. The ThinApp repository must be a network share that is accessible to the connector using a Uniform Naming Convention (UNC) path. The connector synchronizes with this network share regularly to obtain the ThinApp package metadata that Workspace ONE Access requires to distribute and manage the packages. See [Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository](#).

The network share can be a Common Internet File System (CIFS) or a Distributed File System (DFS) share. The DFS share can be a single Server Message Block (SMB) file share or multiple SMB file shares organized as a distributed file system. CIFS and DFS shares running on NetApp storage systems are supported. DFS shares on Isilon storage systems are also supported.

Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository

When you capture and store ThinApp applications to distribute from Workspace ONE Access, you must meet certain requirements. These include requirements on the ThinApp packages as well as requirements on the network share repository.

Requirements on the ThinApp Packages

To create or repackage ThinApp packages that Workspace ONE Access can manage, you must use a version of ThinApp that Workspace ONE Access supports. Workspace ONE Access supports ThinApp 4.7.2 and later. For updated information about supported versions, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

You must have ThinApp packages that Workspace ONE Access can manage. In the ThinApp capture-and-build process, you can create packages that Workspace ONE Access can manage or ones that it cannot manage. For example, when you use the ThinApp Setup Capture wizard to capture an application, you can make a package that Workspace ONE Access can manage by selecting the **Manage with Workspace** check box. See the VMware ThinApp documentation for detailed information on ThinApp features and the appropriate parameters to use to create a package compatible with Workspace ONE Access.

For existing ThinApp packages, you can use the `relink - h` command to enable the packages for Workspace ONE Access. For information about how to convert existing ThinApp packages to packages that Workspace ONE Access can manage, see the *Workspace ONE Access Administration Guide*.

You must store the ThinApp packages on a network share that meets the requirements for the combination of network share type, repository access, and desired ThinApp package deployment mode for your organization's needs.

Requirements on the Network Share Repository

The ThinApp packages must reside on a network share, also known as the ThinApp package repository. The network share must be accessible using a Uniform Naming Convention (UNC) path from each system running the Workspace ONE Access Desktop application used to access the ThinApp packages. For example, a network share named `appshare` on a host named `server` is accessible using the UNC path `\\server\appshare`. The fully qualified hostname of the network share folder must be resolvable from the Workspace ONE Access connector.

The network share can be a Common Internet File System (CIFS) or a Distributed File System (DFS) share. The DFS share can be a single Server Message Block (SMB) file share or multiple SMB file shares organized as a distributed file system. CIFS and DFS shares running on NetApp storage systems are supported. DFS shares on Isilon storage systems are also supported.

The network share must meet the criteria appropriate for the type of access you configure Workspace ONE Access to use for accessing the ThinApp package repository: domain-based access or account-based access. The type of access determines the allowable combinations for the following items:

- Whether you use a CIFS network share or a DFS network share for the ThinApp package repository.
- Whether you must join the connector and the network share's host to the same Active Directory domain.

- Whether the user's Windows system must join the Active Directory domain to use the ThinApp packages.
- The ThinApp package installation mode that the installed Workspace ONE Access Desktop application is set to use for obtaining and running the virtualized applications on the Windows system on which the application is installed. The package installation mode that is used on the user's Windows system is set during the installation process when the Workspace ONE Access Desktop application is installed on that Windows system. This package installation mode determines the mode of ThinApp deployment used by that Windows system, download mode or streaming mode.

Access Type	Network Share Type	Requirements on Workspace ONE Access	Requirements for the User's Windows System
Domain-based access	<p>You can use a CIFS share for your ThinApp package repository when you use domain-based access.</p> <p>You cannot use a DFS share for domain-based access. If you have a DFS share, you must use account-based access.</p>	<p>You must join the connector to the Active Directory domain so it can join the Windows network share and access the packages.</p> <hr/> <p>Note Windows authentication is not required.</p> <hr/> <p>The network share must support authentication and file permissions that are based on computer accounts. The connector accesses the network share with the computer account of the connector in the domain.</p> <p>The network share's folder and file permissions must be configured such that the combination of permissions allows read access for the computer account of the connector in the domain.</p>	<p>The user's Windows system must join the Active Directory domain before that user can use their entitled ThinApp packages.</p> <p>The following systems must all be joined to the same domain:</p> <ul style="list-style-type: none"> ■ The user's Windows system ■ The Workspace ONE Access connector ■ The host of the network share drive with the ThinApp packages <p>When you use domain-based access, the following installation modes for the ThinApp packages are allowed.</p> <ul style="list-style-type: none"> ■ COPY_TO_LOCAL. With this installation mode, packages are downloaded to the client Windows system. This installation mode corresponds to using the ThinApp download mode for the virtualized application. The account that is used to log in to the client Windows system is the user account that is used to copy the packages from the network share to the client Windows system, and that account must have permissions to read the packages and copy the files from that network share. After the package is downloaded to the client Windows system and the user launches the package, the virtualized application runs locally on the client Windows system. ■ RUN_FROM_SHARE. With this installation mode, packages are not downloaded to the client Windows system. A user launches the packages using shortcuts on the local desktop and the virtualized applications run from the network share using ThinApp streaming mode. The account that is used to log in to the client Windows system is the user account that is used to run the packages from the network share, and that account must have permissions to read and execute files from that network share. <hr/> <p>Note RUN_FROM_SHARE is best suited for Windows systems that will always have connectivity to the ThinApp packages' network share. Windows systems that best fit that description are Horizon desktops, because they are always connected to their domain. Floating, or stateless, Horizon desktops best use RUN_FROM_SHARE to avoid the resource usage inherent in downloading the packages to the Windows system.</p>

Access Type	Network Share Type	Requirements on Workspace ONE Access	Requirements for the User's Windows System
Account-based access	<p>You can use either a CIFS share or a DFS share for your ThinApp package repository when you use account-based access.</p>	<p>You must configure the connector to use a share user account and password to access the network share and the packages.</p> <p>The share user account and password is any combination that has read access to the UNC path to the network share folder.</p> <p>You do not have to join the connector to the Active Directory domain to access the network share.</p> <hr/> <p>Note In the Workspace ONE Access console, you must complete the Join Domain page before you can use the ThinApp Packages page.</p> <hr/> <p>Note Account based access is required if you are using NetApp share.</p>	<p>By default, the COPY_TO_LOCAL installation mode is set as the default installation mode when you install the Workspace ONE Access Desktop application on a Windows system by running the graphical version of the client's installer program. To set a different installation mode as the default installation mode for the packages, you must run the client installation using the command line. See the Command-Line Installer Options for Workspace ONE Access Desktop .</p> <hr/> <p>Important HTTP_DOWNLOAD mode requires the IDP URL to be reachable from the user's Windows machine. RUN_FROM_SHARE and COPY_TO_LOCAL modes require the ThinApp share to be reachable from the user's Windows machine.</p> <hr/> <p>The user's Windows system does not have to join the Active Directory domain before that user can use their entitled ThinApp packages. Windows authentication is not required.</p> <p>The user's Windows system, the connector, and the host of the network share with the ThinApp packages do not have to be joined to the same Active Directory domain.</p> <p>With account-based access configured, the following installation modes for the ThinApp packages are allowed.</p> <ul style="list-style-type: none"> ■ If the user's Windows system is not joined to the domain, the client must use the HTTP_DOWNLOAD installation mode to obtain the virtualized application. This installation mode corresponds to using the ThinApp download mode for the virtualized application. <p>The connector uses the share user account to retrieve the packages from the repository.</p> <ul style="list-style-type: none"> ■ If the user joins the Windows system to the domain, the client can use either the COPY_TO_LOCAL installation mode or the RUN_FROM_SHARE installation mode to run the user's entitled ThinApp packages. The account that is used to log in to the client Windows system is the user account that is used to obtain the packages from the network share, and that account must have the appropriate permissions on the network share.

Access Type	Network Share Type	Requirements on Workspace ONE Access	Requirements for the User's Windows System
			<p>If the user's Windows system might be joined to the domain at some times and not joined to the domain at other times, you can install the client with the COPY_TO_LOCAL mode and the AUTO_TRY_HTTP option enabled, as long as the connector is configured for account-based access.</p> <p>With this configuration, the client first tries to use the COPY_TO_LOCAL mode to download the packages. If the Windows system is not joined to the domain at that time, that attempt to copy the packages fails. However, with the AUTO_TRY_HTTP option enabled, the client immediately makes an attempt to use HTTP to download the packages. This combination of COPY_TO_LOCAL and AUTO_TRY_HTTP is the default when you install the Workspace ONE Access Desktop application on a Windows system by running the graphical version of the client's installer program. The connector must be configured for account-based access for the attempt to download the packages using HTTP_DOWNLOAD mode to succeed.</p> <hr/> <p>Important HTTP_DOWNLOAD mode requires the IDP URL to be reachable from the user's Windows machine. RUN_FROM_SHARE and COPY_TO_LOCAL modes require the ThinApp share to be reachable from the user's Windows machine.</p>

In addition, the ThinApp packages repository must meet the following criteria according to the described situation.

- When your settings involve systems joining the Active Directory domain, make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the ThinApp packages. A disjoint namespace occurs when an Active Directory domain name is different from the DNS namespace that machines in that domain use.
- The network share's file and sharing permissions must be configured to provide read access and the ability to run applications to those users that you want to run the ThinApp applications using the COPY_TO_LOCAL or RUN_FROM_SHARE option.

For example, for the Active Directory user accounts of those users that you want to run the ThinApp applications in streaming mode, setting the Shared Folder permission to **Read** and the NTFS permission to **Read & Execute** provides read access and the ability to run the applications to those users.

The NTFS permission setting of **Read & Execute** is required to run a ThinApp application using the ThinApp streaming mode, which corresponds to the Workspace ONE Access Desktop application's RUN_FROM_SHARE installation mode. If your organization requires the NTFS permission set to **Read**, your users can use the ThinApp download mode for the

virtualized application. ThinApp download mode corresponds to installing the Windows client with either the COPY_TO_LOCAL installation mode or HTTP_DOWNLOAD installation mode. With either of those installation modes, the applications are downloaded to the Windows systems and launched locally.

Both CIFS and DFS network shares must have the ThinApp packages organized in individual subdirectories in a directory under the namespace, not subdirectories in the namespace itself, such as `\\server\appshare\thinapp1`, `\\server\appshare\thinapp2`, and so on. See [Create a Network Share for ThinApp Packages That Workspace ONE Access Manages](#).

Create a Network Share for ThinApp Packages That Workspace ONE Access Manages

If you want to enable the VMware ThinApp management capabilities of Workspace ONE Access and allow users to access ThinApp packages from the catalog, you must create a network share and store the ThinApp packages in that network share folder.

Workspace ONE Access obtains the metadata it needs about the ThinApp packages from the network file share.

Prerequisites

- Verify that the ThinApp packages meet Workspace ONE Access requirements.
- Verify that you have the appropriate access and permissions to create a network file share in your IT environment that meets Workspace ONE Access requirements for ThinApp packages.

Procedure

- 1 Create a network share that meets the Workspace ONE Access requirements for ThinApp packages.
- 2 In the network share, create a network share subfolder for each ThinApp package.

Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named `appshare` on a host named `server`, and the application is called `abceditor`, the subfolder for the ThinApp package is `\\server\appshare\abceditor`.

Note Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Workspace ONE Access. Non-ASCII characters are not supported.

- 3 For each ThinApp package, copy its files, such as its EXE and DAT files, to the subfolder that is named for that package's virtualized application.

After copying the files, you have a set of subfolders and files that are similar to these files:

- `\\server\appshare\abceditor\abceditor.exe`
- `\\server\appshare\abceditor\abceditor.dat`

What to do next

Configure Workspace ONE Access access to the ThinApp packages.

Configuring ThinApp Packages in Workspace ONE Access

To configure Workspace ONE Access to provide users access to ThinApp packages, you create a virtual apps collection which contains configuration information such as the path to the storage location of the packages, the connector to use for sync, and the sync schedule.

You can only create a single virtual apps collection for all your ThinApps integrations.

Prerequisites

- Create a network share with the appropriate configuration and store the ThinApp packages in the appropriate location in that network share. See [Create a Network Share for ThinApp Packages That Workspace ONE Access Manages](#).
- Verify that you have the UNC path to the network share folder where the ThinApp packages are located.
- If the connector is not already domain-joined, verify that you have an Active Directory domain name and the username and password of an account in that Active Directory that has the rights to join the domain. Even if you are using account-based access, the Workspace ONE Access console requires the completion of the Join Domain page for legacy Linux connectors before you can use the ThinApp Packages page.

To enable domain-based access, you must also join the connector to the same Active Directory domain to which the ThinApp package repository is joined. Verify that you have the Active Directory domain name for the domain that the network share uses and the username and password of an account in that Active Directory that has the rights to join the domain. The Active Directory account is used to join the connector to the domain.

- When enabling account-based access, verify that you have a username and password that has permission to read the network share. See [Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository](#).

Note Unless you want to restrict use of the ThinApp packages to domain-joined Windows systems for all runtime situations, you should enable account-based access in addition to domain-based access. This combination provides the most flexibility for supporting runtime situations where users need to use their entitled ThinApp packages without joining their Windows systems to the domain.

- You must use an administrator role that can perform the Manage ThinApps action in the Catalog service.

Procedure

- 1 (Legacy Linux connector only) If the connector is not already domain-joined, join it to the Active Directory domain.

Your Workspace ONE Access deployment can have multiple connector instances. The instance that you configure in this procedure will be the instance that synchronizes ThinApp packages with Workspace ONE Access.

- a Log in to the Workspace ONE Access console.
- b Select the **Identity & Access Management** tab.
- c Click **Setup**.
- d In the Connectors page, click **Join Domain** in the appropriate connector row.
- e On the Join Domain page, type the information for the Active Directory domain and click **Join Domain**.

Important Do not use non-ASCII characters when you enter the Active Directory (AD) domain name, AD username, or AD password. Non-ASCII characters are not supported in these entry fields in the Workspace ONE Access console.

Option	Description
AD Domain	Type the fully qualified domain name of the Active Directory. An example is HS . TRDOT . COM .
AD Username	Type the username of an account in the Active Directory that has permissions to join systems to that Active Directory domain.
AD Password	Type the password associated with the AD Username . This password is not stored by Workspace ONE Access.

The Join Domain page refreshes and displays a message that you are currently joined to the domain.

- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click **New**.
- 4 Select **ThinApp Package** as the source type.
- 5 In the New ThinApp Collection wizard, enter the following information in the Connector page.

Option	Description
Name	Enter a unique name for the ThinApp collection.
Connector	Select the connector that you want to use to sync this collection. To select the connector, select the directory that is associated with it. If you have set up a cluster of connectors, all the connector instances appear in the Host list and you can arrange them in failover order for this collection.

Important After you create the collection, you cannot select a different directory.

- 6 Click **Next**.
- 7 In the Configuration page, enter the required information.

Option	Description
Path	<p>The path to the shared folder where the ThinApp packages' folders are located, in the UNC path format <code>\\server\share\subfolder</code>. For example: <code>\\DirectoryHost\ThinAppFileShare</code>. For <i>DirectoryHost</i>, provide the host name, not the IP address.</p> <p>For both CIFS and DFS network shares, this path must be a directory under the namespace, and not the namespace itself.</p>
Enable Account Based Access	<p>Account based access is required in the following cases:</p> <ul style="list-style-type: none">■ For NetApp storage systems and other brands of DFS network shares■ If you are using HTTP download deployment mode■ If you want users to be able to use their entitled ThinApp packages on non-domain-joined Windows systems
Share User	<p>The username for a user account that has read access to the network share. The Share User is required to enable account based access to the stored ThinApp packages.</p>
Share Password	<p>The password associated with the Share User user account.</p>
Sync Frequency	<p>Select how often you want to sync the resources in the collection.</p> <p>You can set up an automatic sync schedule or choose to sync manually. To set a schedule, select the interval such as daily or weekly and select the time of day to run the sync. If you select Manual, you must click Sync on the Virtual Apps Collections page after you set up the collection and whenever there is a change in your Horizon Cloud resources or entitlements.</p>
Activation Policy	<p>Select how you want to make resources in this collection available to users in the Workspace ONE Intelligent Hub portal and app. If you intend to set up an approval flow, select User-Activated, otherwise select Automatic.</p> <p>With both the User-Activated and Automatic options, the resources are added to the Apps tab. Users can run the resources from the Apps tab or mark them as favorites to run them from the Favorites tab. However, to set up an approval flow for any of the apps, you must select User Activated for that app.</p> <p>The activation policy applies to all user entitlements for all the resources in the collection. You can modify the activation policy for individual users or groups per resource, from the user or group page in the Users & Groups tab.</p>

- 8 Click **Next**.
- 9 In the Summary page, review your selections, then click **Save**.

The collection is created and appears in the Virtual Apps Collections page. The applications are not synced yet.

- 10 To sync the applications in the collection, select the collection in the Virtual Apps Collections page and click **Sync**.

Each time ThinApp applications change, a sync is required to propagate the changes to Workspace ONE Access.

Results

Workspace ONE Access is now configured so that you can entitle groups and users to ThinApp packages, and those users can run their entitled ThinApp packages using the Workspace ONE Access Desktop application installed on their Windows systems.

What to do next

Entitle groups and users to ThinApp packages.

Entitle Workspace ONE Access Users and Groups to ThinApp Packages

After you integrate ThinApp packages with Workspace ONE Access, you can entitle users and groups to the Windows applications that are captured as ThinApp packages.

You can only entitle Workspace ONE Access users, users who are imported from your directory server, to ThinApp packages. When you entitle a user to a ThinApp package, the user sees the application and can start it from the Workspace ONE Access Desktop application on their system. If you remove the entitlement, the user cannot see or start the application.

Often, the most effective way to entitle users to ThinApp packages is to add a ThinApp package entitlement to a group of users. In certain situations entitling individual users to a ThinApp package is more appropriate.

Prerequisites

Set up a virtual apps collection for ThinApp packages from the **Catalog > Virtual Apps Collections** page. After you create the collection, sync the ThinApp packages to Workspace ONE Access. When the ThinApp packages are synced to your catalog, you can entitle them to your users and groups.

Procedure

- 1 Log in to the Workspace ONE Access console.

2 Entitle users to a ThinApp package.

Option	Description
Access a ThinApp package and entitle users or groups to it.	<ul style="list-style-type: none">a Click the Catalog > Virtual Apps tab.b (Optional) Click the icon in the Type column heading and select ThinApp Package to view all ThinApp packages. You can also search for a ThinApp package by name.c Click the package.d Click Assign.e Select users and groups by typing the name in the search box and selecting from the results.f Select the deployment type for each user and group. Regardless of whether you select User Activated or Automatic, the application is added to the Apps page in the Intelligent Hub portal or app. Users can run the application from the Apps page or mark it as favorite and run it from the Favorites page. However, if you want to set up an approval flow for the application, select User Activated.g Click Save.
Access a user or group and add ThinApp package entitlements to that user or group.	<ul style="list-style-type: none">a Click the Users & Groups tab.b Click the Users tab or the Groups tab.c Click the name of an individual user or group.d Click the Apps tab, then click Add Entitlement.e In the Application Type drop-down list, select ThinApp Packages.f Select the check boxes next to the ThinApp packages to which to entitle the user or group.g In the DEPLOYMENT column, select the activation method for the ThinApp package. Regardless of whether you select User Activated or Automatic, the application is added to the Apps tab in the Workspace ONE Intelligent Hub app and portal. Users can run the application from the Apps page or mark it as a favorite to run it from the Favorites tab. However, if you want to set up an approval flow for the application, select User Activated.h Click Save.

Results

The selected users or groups are now entitled to use the ThinApp package.

What to do next

Verify that the Workspace ONE Access Desktop application is installed on users' Windows systems.

Distributing and Managing ThinApp Packages with Workspace ONE Access

Before your Workspace ONE Access users can run their ThinApp packages that are registered to them using Workspace ONE Access, those users must have the Workspace ONE Access Desktop application installed and running on their Windows systems.

ThinApp packages are virtualized Windows applications. The ThinApp packages are distributed to Windows systems, and a user logged into the Windows system can launch and run those ThinApp packages that are registered on that Windows system. Workspace ONE Access can distribute and manage ThinApp packages that are compatible with Workspace ONE Access.

To successfully launch and run one of these virtualized applications in the user's logged-in Windows session, the following elements are required:

- The virtualized application's ThinApp package is registered for that user's use by Workspace ONE Access.
- A particular DLL is available on that Windows system.
- The `hws-desktop-client.exe` process is running.

When a compatible ThinApp package is created, it is configured to load a particular DLL when the logged-in user launches the virtualized application in their logged-in Windows session. At that time, the virtualized application attempts to load the DLL. When the DLL is loaded, it attempts to verify with the locally installed Workspace ONE Access Desktop application whether that ThinApp package is registered on that Windows desktop for that user. The locally installed Workspace ONE Access Desktop application determines whether that application is registered for that user without communicating with Workspace ONE Access. If the application is registered on that Windows desktop for that user, the Workspace ONE Access Desktop application checks to see when it last synced with Workspace ONE Access. If the Workspace ONE Access Desktop application confirms that the time from the last sync is within the offline grace period configured for the installed client, the client allows the application to run.

Because that DLL is available on the Windows system only if the Workspace ONE Access Desktop application is installed, and because the `hws-desktop-client.exe` process is running if the Workspace ONE Access Desktop application is running on that system, the Workspace ONE Access Desktop application must be installed on the Windows system to run ThinApp packages that are distributed and managed by Workspace ONE Access.

Deploying the Workspace ONE Access Desktop Application To Use ThinApp Packages

The Workspace ONE Access Desktop application can be installed by either double-clicking its installer EXE file, running the executable file using the command-line options, or running a script that uses the command-line options. Local administrator privileges are required to install the application. For information about installing the Workspace ONE Access Desktop application by double-clicking its installer EXE file, see the *Workspace ONE Access Desktop User Guide*.

The configuration of the installed application determines how a ThinApp package that is distributed by Workspace ONE Access is deployed to that Windows system. By default, when the Workspace ONE Access Desktop application is installed by double-clicking its installer EXE file, the client is configured to deploy ThinApp packages using the `COPY_TO_LOCAL` deployment mode, with the `AUTO_TRY_HTTP` option enabled. Those default installer options result in what is called a download deployment mode. With the `COPY_TO_LOCAL` and `AUTO_TRY_HTTP` default settings, the client application first tries to download the ThinApp packages by copying them to the Windows system endpoint, and if the first attempt fails, the client application tries to download the ThinApp packages using HTTP.

If the Workspace ONE Access connector is configured for account-based access to your ThinApp repository, the client application can download the ThinApp packages using HTTP. After the ThinApp packages are downloaded to the local Windows system, the user runs the virtualized applications on the local system.

To avoid having the virtualized applications downloaded to the local Windows system and using space on the Windows system, you can have users run the ThinApp packages from the network share by using what is called a streaming deployment mode. To have your users run the ThinApp packages using streaming mode, you must install the Workspace ONE Access Desktop application on the Windows systems using a command-line installation process. The installer has command-line options that you can use to set the runtime deployment mode for the ThinApp packages. To set the runtime deployment mode to stream the ThinApp packages, use the `RUN_FROM_SHARE` installer option.

One method for installing the Workspace ONE Access Desktop application to multiple Windows systems is to use a script to install the application silently to the Windows systems. You can install the client silently to multiple Windows systems at the same time.

Note A silent installation does not display messages or windows during the install process.

You set a value in the script to indicate whether the clients installed by that script deploy ThinApp packages using the ThinApp streaming mode, or `RUN_FROM_SHARE` option, or one of the ThinApp download modes, such as the `COPY_TO_LOCAL` or `HTTP_DOWNLOAD` option.

Determining the Appropriate Deployment Mode for ThinApp Packages on Windows Endpoints

The configuration of the Workspace ONE Access Desktop application on the Windows endpoint determines whether a ThinApp package that is distributed using Workspace ONE Access is deployed using ThinApp streaming mode, `RUN_FROM_SHARE`, or one of the ThinApp download modes, `COPY_TO_LOCAL` or `HTTP_DOWNLOAD`. When you create the script to silently install the Workspace ONE Access Desktop application to Windows endpoints, such as desktop and laptop computers, you set the options that set the ThinApp package deployment mode. Choose the deployment mode that best fits the network environment for the selected endpoints, considering details such as network latency.

With streaming mode, when the Workspace ONE Access Desktop application synchronizes with Workspace ONE Access, the client downloads application shortcuts for the ThinApp packages' virtualized Windows applications to the Windows desktop, and when the user launches the ThinApp packages, the virtualized Windows applications run from the file share on which the ThinApp packages reside.

Therefore, streaming mode is appropriate for systems that will always be connected to the network share, such as Windows desktops that are shared by multiple users, or Horizon desktops.

With download mode, at the first use or update of a ThinApp package, the user must wait for the ThinApp package to download to the Windows system first, and shortcuts to be created. After the initial download, the user launches and runs the virtualized Windows application on the local Windows system.

Important For non-persistent Horizon desktops, also known as floating or stateless Horizon desktops, you are expected to set the client to use ThinApp streaming mode by using the command-line installer option `/v INSTALL_MODE=RUN_FROM_SHARE` when installing the client. The `RUN_FROM_SHARE` option provides the most optimal runtime experience for using ThinApp packages in floating Horizon desktops. See [Command-Line Installer Options for Workspace ONE Access Desktop](#) .

Important `HTTP_DOWNLOAD` mode requires the IDP URL to be reachable from the user's Windows machine. `RUN_FROM_SHARE` and `COPY_TO_LOCAL` modes require the ThinApp share to be reachable from the user's Windows machine.

Table 6-1. ThinApp Deployment Mode for the Virtualized Applications Captured as ThinApp Packages

Mode	Description
ThinApp streaming mode	<p>In ThinApp streaming mode, the virtualized applications are streamed each time they are started. This method avoids using disk space in the desktop that would be used when copying the virtualized applications to the desktop. The desktop must be connected to the ThinApp packages' network share for the applications to run.</p> <p>The following environments might provide the consistency and stability required:</p> <ul style="list-style-type: none"> ■ Horizon desktops, either stateless or persistent, with excellent connectivity to the file share on which the ThinApp packages reside. ■ Users with Windows desktops that are not Horizon desktops, that are shared by multiple users. This situation avoids the accumulation on disk of downloaded user-specific applications and also provides quick access to applications without causing a delay for downloads specific to a user. <p>The account that the user uses to log in to the Windows system is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and execute files on the network share.</p>
ThinApp download mode	<p>In ThinApp download mode, applications are downloaded to the Windows endpoint. The user runs the virtualized application locally on the endpoint. You might prefer ThinApp download mode for the following situations:</p> <ul style="list-style-type: none"> ■ Persistent Horizon desktops (Workspace ONE Access on premises) ■ LAN-connected desktops that are periodically offline ■ A LAN with poor network latency <p>Workspace ONE Access provides two flavors of the ThinApp download mode: COPY_TO_LOCAL and HTTP_DOWNLOAD. If the client is configured for COPY_TO_LOCAL, the Windows endpoint must be joined to the same domain as the file share unless the AUTO_TRY_HTTP option is enabled and the Workspace ONE Access connector is configured for account-based access to the ThinApp packages' network share.</p> <p>When the AUTO_TRY_HTTP option is enabled and the Workspace ONE Access connector is configured for account-based access, if the Windows endpoint is not joined to the same domain and the first attempt to download the ThinApp packages fails, the Workspace ONE Access Desktop application will automatically try to download the ThinApp packages using the HTTP protocol as for the HTTP_DOWNLOAD mode. With HTTP_DOWNLOAD, the Windows endpoint does not have to be joined to the same domain as the file share. However, the copy and sync times when using HTTP_DOWNLOAD are significantly longer than when using COPY_TO_LOCAL.</p>
	<p>Important If Workspace ONE Access is not enabled for account-based access, downloading using the HTTP protocol does not work, even if AUTO_TRY_HTTP is enabled or the client is configured with the HTTP_DOWNLOAD option.</p> <p>When using COPY_TO_LOCAL, the account that the user uses to log in to the Windows system is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and copy files from the network share. When using HTTP_DOWNLOAD, the share user account that you enter in the Workspace ONE Access console when you configure access from the connector to the ThinApp packages' network share is the account that is used to download the ThinApp packages. That share user account needs to have read permission on the ThinApp packages' network share to copy the files from the network share.</p>

The ThinApp packages' network share must meet the appropriate requirements for the deployment mode that you set for the Windows endpoints. See *Workspace ONE Access Installation and Configuration*.

Offline Grace Period for ThinApp Packages Integrated with Workspace ONE Access

The offline grace period is the period of time for which a virtualized application is allowed to launch and run on a Windows system without syncing with Workspace ONE Access.

ThinApp packages are virtualized Windows applications, and Workspace ONE Access can distribute these applications to Windows systems. When Workspace ONE Access distributes a ThinApp package to the Windows system for the first time for the user logged in to that system, the package's virtualized applications are registered on that Windows system for that user's use. The appropriate shortcuts are added to the Windows desktop, and the user can launch the virtualized applications using the shortcuts as for standard Windows applications installed to that system.

When a user launches one of the virtualized applications that was deployed to the Windows system by Workspace ONE Access, the ThinApp package requests permission to run from the ThinApp agent running on the system. The ThinApp agent verifies the following conditions.

- Verifies whether the application is registered on this Windows desktop for the logged-in user.
- Verifies whether the Windows system has synced with Workspace ONE Access within the allowed offline grace period.

If both of those conditions are true, the ThinApp agent allows the virtualized application to run.

The frequency of how often the Workspace ONE Access Desktop application syncs with Workspace ONE Access is set by the POLLINGINTERVAL installer option. By default, the frequency is every 5 minutes. The offline grace period is set to 30 days by default. If a Windows system has had network connectivity to connect to Workspace ONE Access at any time within a 30-day timespan, the application can sync with Workspace ONE Access and virtualized applications can run.

However, if the Windows system has no network connectivity to connect to Workspace ONE Access, the application cannot sync with Workspace ONE Access. Virtualized applications registered on that Windows system can run on the disconnected system up to the time set by the offline grace period.

Updating Managed ThinApp Packages After Deployment in Workspace ONE Access

After adding a ThinApp package to your organization's catalog and entitling your Workspace ONE Access users to that ThinApp package, your organization might want to update that package and have the users use a newer, or rebuilt, version of the ThinApp package, without having to unentitle the users from the current package and then entitling them to the newer package.

An updated ThinApp package might be made available because a newer version of the Windows application for that package is released, or because the packager of the application has changed the values of parameters used by the package.

ThinApp 4.7.2 and newer versions provide an update mechanism for ThinApp packages used in Workspace ONE Access. This ThinApp update mechanism is different from other update mechanisms for ThinApp packages used outside of a Workspace ONE Access environment. The updated ThinApp package must have been updated with this mechanism for you to be able to deploy the updated package in Workspace ONE Access and have users automatically see the newer version.

For ThinApp packages that are managed in Workspace ONE Access, two Package.ini parameters are used by Workspace ONE Access to determine that a package is an updated version of another package.

AppID

The unique identifier for the ThinApp package in Workspace ONE Access. All entry points (executables) for the package's application are assigned the same AppID. After a ThinApp package is synced to your organization's Workspace ONE Access catalog, the package's AppID is displayed in the GUID column in the ThinApp package's resource page. This value consists of alphanumeric characters in a pattern of character sets, each set separated by dashes, such as in the following example:

```
xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Workspace ONE Access considers any ThinApp package with the same AppID to be versions of the same application.

VersionID

The version number of the ThinApp package. Workspace ONE Access uses the VersionID to keep track of different versions of the managed ThinApp package. You increment the VersionID value by one (1) to mark that ThinApp package as an update of another package, retaining the same AppID.

You place the updated package in a new folder in the network share folder configured for the managed ThinApp packages. See *Installing and Configuring Workspace ONE Access*. When Workspace ONE Access performs the scheduled sync with the network share folder and it encounters an application that has the same AppID as another application, it compares the

`VersionID` values. The ThinApp package with the highest `VersionID` is used as the most recent update. Workspace ONE Access automatically incorporates the previous user entitlements to the ThinApp package with the highest `VersionID`, and shortcuts on the users' systems are synced to point to the updated package.

Important The standard ThinApp `InventoryName` parameter is important to successful updates of managed ThinApp packages. Both the previous and updated ThinApp packages must have the same value for the `InventoryName` parameter. If the person creating the ThinApp package changes the `InventoryName` in a package, and then creates an updated package, you must make sure the `InventoryName` values match for the updates to work properly in Workspace ONE Access.

See the *ThinApp Package.ini Parameters Reference Guide* for details about the various parameters that are used in a ThinApp package's `Package.ini` file.

Update a ThinApp Package Managed by Workspace ONE Access

Updating a ThinApp package that is already managed by Workspace ONE Access and in your organization's catalog involves multiple steps. The updated ThinApp package might be provided to you by another group in your organization. To ensure that Workspace ONE Access can automatically use the updated package in place of the existing one for the entitled users, you must ensure the updated package was created using the same `AppID` as the current package, has a `VersionID` value that is higher than the existing package's `VersionID` value, and is enabled for management by Workspace ONE Access.

Prerequisites

Verify that you have access to the location where your managed ThinApp packages reside and can create subfolders at that location.

Procedure

- 1 Obtain the `AppID` and `VersionID` values of a Managed ThinApp Package.
- 2 Create the Updated ThinApp Package.
- 3 Copy an Updated ThinApp Package to the Network Share.

Obtain the `AppID` and `VersionID` values of a Managed ThinApp Package

To ensure that Workspace ONE Access automatically uses the updated ThinApp package in place of the current one, the updated ThinApp package must be created using the `AppID` of the currently managed ThinApp package and a higher `VersionID` value than the current version.

When the Setup Capture process is used to create an updated ThinApp package, the `AppID` value is automatically retrieved by the Setup Capture program from the existing ThinApp package's executables, and the `VersionID` value is automatically incremented. However, the person who is creating the updated ThinApp package might use a different method for creating the updated package. When the Setup Capture process is not used to create the updated ThinApp package,

the person creating the package must obtain the `AppID` and `VersionID` values for the ThinApp package that is currently managed by Workspace ONE Access. The `AppID` and `VersionID` values are displayed on pages in the ThinApp package's resource page in the Workspace ONE Access console.

Procedure

- 1 In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
- 2 (Optional) Click the icon in the **Type** column heading and search for the package by name or select **ThinApp Package** to view all ThinApp packages.
- 3 Click the ThinApp package.
- 4 Make note of the following values.
 - The **Version** value in the **Definition** section of the page.
 - The `AppID` value listed in the **GUID** column in the **ThinApp Package** section.

The value listed in the GUID column is the value that Workspace ONE Access uses to identify this ThinApp package.

What to do next

To create the updated ThinApp package, complete the steps in [Create the Updated ThinApp Package](#).

Create the Updated ThinApp Package

After you obtain the `AppID` and `VersionID` values of a ThinApp package managed by Workspace ONE Access, create the updated ThinApp package following this procedure to ensure that Workspace ONE Access automatically uses the updated ThinApp package.

The `AppID` and `VersionID` values of the currently managed ThinApp package are used for creating the updated package. The updated package uses the same `AppID` value and a higher `VersionID` value.

Sometimes the updated ThinApp package is provided to you by another team in your organization. The person who creates the updated ThinApp package can use one of the described methods.

Prerequisites

Verify that you have the `AppID` and `VersionID` values of the current ThinApp package by completing the steps in [Obtain the AppID and VersionID values of a Managed ThinApp Package](#).

Verify that you have a version of the ThinApp program that is compatible with your version of Workspace ONE Access. For information about specific ThinApp versions, see the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Procedure

- ◆ Using a version of the ThinApp program that is supported by Workspace ONE Access, create the updated ThinApp package using one of the available methods.

Option	Description
<p>Recapture using Setup Capture.</p>	<p>Use this method when the project folder for the existing ThinApp package managed by Workspace ONE Access is unavailable. To create an updated package with Setup Capture, you need only the following items:</p> <ul style="list-style-type: none"> ■ The application executables from the existing ThinApp package ■ The application installer ■ Setup Capture and the ThinApp program at a version supported by Workspace ONE Access. <p>During the capture process, select to manage the package with Workspace ONE Access and that the package is an update of an existing base ThinApp package. Browse to the folder that contains the executables for the currently managed ThinApp package. Point to the folder, and not to specific executables.</p> <p>With this method, you do not need to obtain the <code>AppID</code> or <code>VersionID</code> values in advance of creating the updated package. After you designate the package as an update and point to the prior version in Setup Capture, the capture process reads the <code>AppID</code> of the prior package and reuses it for the updated package. The process also provides an incremented <code>VersionID</code> for the updated package, and assigns the same <code>InventoryName</code>.</p>
<p>Update the <code>Package.ini</code> file manually and then rebuild the package.</p>	<p>Use this method when you do not have the application installer for the recapture process, or when you need to update the package to a newer ThinApp version and want to update more than what the <code>relink</code> command would handle. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new <code>Package.ini</code> parameter that you want to set.</p> <p>To mark the new package as an update, edit the following Workspace ONE Access parameters in the <code>[Build Options]</code> section of the <code>Package.ini</code> file:</p> <ul style="list-style-type: none"> ■ Set the <code>AppID</code> parameter to match the <code>AppID</code> value of the currently managed ThinApp application. You cannot reuse a value of <code>genid</code> for <code>AppID</code>, because then a new <code>AppID</code> value will be generated for the updated package and Workspace ONE Access will not recognize the new package as an update to the existing one. ■ Increment the value of the <code>VersionID</code> parameter to a higher integer than the currently managed ThinApp package. If there is no <code>VersionID</code> parameter set for the currently managed package, its value is 1 by default, and you would add a line for the <code>VersionID</code> parameter to <code>Package.ini</code> and set it to a value of 2 (<code>VersionID = 2</code>). ■ Make sure the <code>InventoryName</code> parameter value matches the <code>InventoryName</code> value of the currently managed package. The <code>InventoryName</code> values for the current package and the updated package must be identical.
<p>Use the <code>relink -h</code> command with the <code>AppID</code> and <code>VersionID</code> options.</p>	<p>Use this method in one of the following situations:</p> <ul style="list-style-type: none"> ■ You do not have the project folder for the application.

Option	Description
	<ul style="list-style-type: none"> <li data-bbox="635 226 1428 346">■ You have already captured, built, and tested the package outside of a Workspace ONE Access environment, and the only remaining steps are to enable the updated package for Workspace ONE Access and place it in the network share used by the Workspace ONE Access connector. <li data-bbox="635 357 1428 420">■ You are updating the package only to update the ThinApp runtime for the package to incorporate bug fixes available in that new ThinApp version. <p data-bbox="635 430 1428 619">For example, if you have changed the project directory, including the Package.ini file, for a virtual application, rebuilt the package, and tested the package, the test environment might not have been Workspace ONE Access. The final stage of updating the application is to enable it for Workspace ONE Access. At that point, the easiest route is to use the <code>relink -h</code> command, instead of recapturing or rebuilding.</p> <hr/> <p data-bbox="635 640 1428 703">Note The ThinApp runtime is always updated when you run the <code>relink -h</code> command on a ThinApp package.</p> <hr/> <p data-bbox="635 724 1428 787">You can run the <code>relink</code> command from the ThinApp Program Files directory to get help on the command's syntax.</p> <p data-bbox="635 798 1428 882">When the existing ThinApp package is already enabled for use by Workspace ONE Access, you can run the following command to reuse the package's existing <code>AppID</code> and increment the <code>VersionID</code>:</p> <pre data-bbox="646 892 1428 945" style="background-color: #f0f0f0; padding: 5px;">relink -h -VersionID + executable-folder/*.*</pre> <p data-bbox="635 966 1428 1029">Where <code>executable-folder</code> is a folder containing the executables of the ThinApp package you want to update.</p> <hr/> <p data-bbox="635 1050 1428 1270">Important When you use the <code>relink</code> command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Workspace ONE Access environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point <code>relink</code> to a copy of the folder of executables.</p> <hr/> <p data-bbox="635 1291 1428 1375">Other use cases for the <code>relink</code> command, including enabling a ThinApp package for use in a Workspace ONE Access environment, are covered in the VMware knowledge base article at http://kb.vmware.com/kb/2021928.</p>

Results

You have a set of files (EXE files, and optionally DAT files) for the updated ThinApp package.

What to do next

Copy the files to a new subfolder on the network share, by completing the steps in [Copy an Updated ThinApp Package to the Network Share](#).

Copy an Updated ThinApp Package to the Network Share

After you create the updated ThinApp package, you copy the appropriate files to a new subfolder at the same level as the existing subfolder on the network share to ensure that Workspace ONE Access automatically uses the updated ThinApp package.

Prerequisites

Verify that you have the files for the updated ThinApp package, as a result of completing the steps in [Create the Updated ThinApp Package](#) and incrementing the `VersionID` value.

Verify that you have access to the network share and can make subfolders and copy files to it.

Procedure

- 1 In the network share folder, create a new subfolder for the updated ThinApp package.

Retain the existing subfolder for the ThinApp package that you are updating, and do not alter its contents.

After the next scheduled sync, Workspace ONE Access ignores the older package, when it recognizes the new package has the same `AppID` value and a higher `VersionID` value.

Typically, you name the subfolder to match the name of the ThinApp application, or indicate what application is in the folder. For example, if the network share is named `appshare` on a host named `server`, and the application is called `abceditor`, the subfolder for the ThinApp package is `\\server\appshare\abceditor`.

Note Do not use non-ASCII characters when you create your network share subfolder names for ThinApp packages to distribute by using Workspace ONE Access. Non-ASCII characters are not supported.

- 2 Copy the EXE and DAT files for the updated ThinApp package into that new subfolder.
- 3 (Optional) If you do not want to wait for the next scheduled sync time, you can manually sync Workspace ONE Access with the network share from the Packaged Apps - ThinApp page of the Workspace ONE Access console.

When the Workspace ONE Access connector performs the scheduled sync with the network share folder and it encounters an application that has the same `AppID` as another application, it compares the `VersionID` values. The ThinApp package with the highest `VersionID` is used as the most recent update. Workspace ONE Access automatically incorporates the previous user entitlements to the ThinApp package with the highest `VersionID`, and shortcuts on the users' systems are synced to point to the updated package.

What to do next

Your Workspace ONE Access catalog displays the new version of the updated ThinApp package after the next ThinApp package sync. If you want to see the new version reflected in the ThinApp package's resources page, you can manually sync using the Packaged Apps - ThinApp page of the Workspace ONE Access console.

Make Existing ThinApp Packages Compatible with Workspace ONE Access

You can convert a ThinApp package from one that is not compatible with Workspace ONE Access to one that Workspace ONE Access can distribute and manage. You can use one of the following methods: use the ThinApp 4.7.2 `relink` command, rebuild the package from its ThinApp project files after editing the project's `Package.ini` file to add the necessary Workspace ONE Access parameters, or recapture the Windows application with the appropriate Workspace ONE Access settings selected in the ThinApp Setup Capture program.

Note A ThinApp package that is compatible with Workspace ONE Access can only be used for a Workspace ONE Access deployment. Only Workspace ONE Access users who have the Workspace ONE Access Desktop application installed can launch and run these enabled packages. At runtime, the ThinApp package loads a specifically named DLL, and uses that DLL to verify the user's entitlement with Workspace ONE Access. Because the DLL is installed with the Workspace ONE Access Desktop application, such ThinApp packages can only be run on Windows systems on which the Workspace ONE Access Desktop application is installed.

Prerequisites

Verify that you have access to the necessary items for your chosen method.

- If you are using the `relink` command, verify that you have the executable files for the ThinApp package that you are converting and the ThinApp 4.7.2 `relink.exe` application.
- If you are updating the ThinApp project's `Package.ini` file and rebuilding the package, verify that you have the project files needed by the ThinApp 4.7.2 program to rebuild the package.
- If you are recapturing the Windows application, verify that you have the ThinApp 4.7.2 Setup Capture program and the application installer and other items that the program needs to recapture the application. See the *ThinApp User's Guide* for details.

Verify that you have access to the ThinApp network share used by Workspace ONE Access and that you can make subfolders and copy files to it.

Procedure

- ◆ Using a version of the ThinApp program that is supported by Workspace ONE Access, create a compatible ThinApp package using one of the available methods.

Option	Description
<p>Use the <code>relink -h</code> command.</p>	<p>Using the <code>relink -h</code> command is the easiest method. You must use the <code>relink.exe</code> program from ThinApp 4.7.2 or later. Use this method in one of the following situations:</p> <ul style="list-style-type: none"> ■ You cannot use the rebuild method because you do not have the project folder. ■ Using Setup Capture to recapture the application would take too long. ■ You do not have the application installer that is required for recapturing with Setup Capture. <p>Note The ThinApp runtime is always updated when you run the <code>relink -h</code> command on a ThinApp package.</p> <p>You can run the <code>relink</code> command from the ThinApp Program Files directory to get help on the command's syntax.</p> <p>To create a compatible package, use the basic syntax of the command:</p> <pre>relink -h executable-folder/*.*</pre> <p>Where <i>executable-folder</i> is a folder containing the executables of the ThinApp package you want to update.</p> <p>Important When you use the <code>relink</code> command, you cannot point it directly to the folder of package executables on the network share used for the ThinApp packages in the Workspace ONE Access environment. The command converts the old executables to BAK files when it updates the ThinApp runtime, and it writes those BAK files, as well as the new files, to the folder. Because the network share typically does not allow writing to it, you must point <code>relink</code> to a copy of the folder of executables.</p> <p>Other use cases for the <code>relink</code> command are covered in the VMware knowledge base article at http://kb.vmware.com/kb/2021928.</p>
<p>Update the Package.ini file manually with the necessary parameters, and then rebuild the package.</p>	<p>Use this method when you do not have the application installer for the recapture process, when you want to avoid doing the up-front setup that recapturing the application requires, or when you want to incorporate functionality from a newer ThinApp version more than what the <code>relink</code> command would provide. Because rebuilding a package incorporates changes to the file system and registry which come in a new version of ThinApp, a rebuild would pick up those changes, such as when a new ThinApp version provides a new Package.ini parameter that you want to set.</p> <p>In the [Build Options] section of the Package.ini file, add the following parameters:</p> <pre>;--- VMware Identity Manager Parameters --- AppID=genid NotificationDLLs=hztapluginlogin.dll</pre> <p><code>hztaplugin.dll</code> is the DLL that the ThinApp runtime calls to verify the Workspace ONE Access user's entitlement to use the virtualized application.</p>

Option	Description
	You can optionally include the <code>HorizonOrgURL</code> parameter and set it to your Workspace ONE Access fully qualified domain name.
Recapture using Setup Capture, and select the necessary Workspace ONE Access settings.	Use this method when you would prefer to recapture the application rather than use one of the other methods. To create a compatible package using ThinApp Setup Capture, select the appropriate settings in the wizard to manage the package with Workspace ONE Access during the capture process. See the <i>ThinApp User's Guide</i> for details on the capture process.

Results

You have a set of files (EXE files, and optionally DAT files) for a ThinApp package that Workspace ONE Access can distribute and manage.

What to do next

For steps to add ThinApp packages to the network share, see [Create a Network Share for ThinApp Packages That Workspace ONE Access Manages](#).

Change the ThinApp Packages Share Folder in Workspace ONE Access

After you configure Workspace ONE Access access to your ThinApp packages, your IT environment might change such that your ThinApp packages are in a new location. When this situation occurs, in the Workspace ONE Access console, update the path to the new location.

Prerequisites

Verify that the new network share location adheres to the network share requirements as described in [Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository](#).

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Select the ThinApp collection and click **Edit**.
- 4 In the Edit ThinApp wizard, click **Configuration** to go to the Configuration page.
- 5 Change the value in the **Path** text box to the new shared folder where the ThinApp packages are located in the UNC path format.
- 6 (Optional) If the new share is a DFS share, select the **Enable account based access** check box and enter the name and password of a user who has read access to that network share.
- 7 Click **Next**, then click **Save**.

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access

The default access policy set applies to all applications and desktops in your Workspace ONE Access catalog. You can also set access policies for individual applications or desktops, which override the default access policy.

You can configure application policies for desktops and applications from the application configuration page or from the Policies page in the Workspace ONE Access console.

For detailed information on access policies and how they are applied, see the *Workspace ONE Access Administration Guide*.

Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
 - a In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
 - b Click the application.
 - c Click **Edit**.

Certain fields on the application page are now editable.
 - d In the **Access Policies** section, select the access policy for the application.
 - e Click **Save** at the top of the page.
- 2 To apply an access policy to one or more applications and desktops from the Policies page, follow these steps.
 - a In the Workspace ONE Access console, navigate to the **Identity & Access Management > Policies** page.
 - b Click a policy to edit or click **Add Policy** to create a new policy.
 - c In the Definition page of the wizard, in the **Applies to** section, select the applications and desktops to which you want to apply the policy.
 - d In the **Applies to** section, select the applications to which you want to apply the policy.
 - e Save your changes.

Configuring Workspace ONE Access Desktop

7

Before your Workspace ONE Access users can run the ThinApp packages that are registered to them using Workspace ONE Access, they must have the Workspace ONE Access Desktop application installed and running on their Windows systems.

The Workspace ONE Access Desktop application can be installed by double-clicking its installer executable file and using the Setup wizard, by running the executable file using the command-line options, or by running a script that uses the command-line options. Local administrator privileges are required to install the application.

The configuration of the Workspace ONE Access Desktop application on the Windows endpoint determines whether a ThinApp package that is distributed using Workspace ONE Access is deployed using ThinApp streaming mode, `RUN_FROM_SHARE`, or one of the ThinApp download modes, `COPY_TO_LOCAL` or `HTTP_DOWNLOAD`. When you create the script to silently install Workspace ONE Access Desktop to Windows endpoints, such as desktop and laptop computers, you set the options that set the ThinApp package deployment mode. Choose the deployment mode that best fits the network environment for the selected endpoints, considering details such as network latency.

Important `HTTP_DOWNLOAD` mode requires the IDP URL to be reachable from the user's Windows machine. `RUN_FROM_SHARE` and `COPY_TO_LOCAL` modes require the ThinApp share to be reachable from the user's Windows machine.

Note If any browser windows are open during installation of the Workspace ONE Access Desktop application, problems might occur with launching ThinApp packages from the user portal. Either close all browser windows before installing the application, or immediately after installing the application, restart your browsers. See [#unique_74](#).

This chapter includes the following topics:

- [Command-Line Installer Options for Workspace ONE Access Desktop](#)
- [Install the Workspace ONE Access Desktop Application with Identical Settings to Multiple Windows Systems](#)
- [Add Workspace ONE Access Desktop Installer Files to Workspace ONE Access Virtual Appliances](#)
- [Using the Workspace ONE Access Command-Line `hws-desktop-ctrl.exe` Application](#)

Command-Line Installer Options for Workspace ONE Access Desktop

You can set various options for the Workspace ONE Access Desktop application when you run its installer using the command line or a deployment script.

Available Command-Line Options for the Workspace ONE Access Desktop Installer

After you download the .exe file for the client application's installer to a Windows system, you can see a list of the installation options by running the following command:

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn /?
```

where *n.n.n-nnnnnnn* represents the file's version and build number. A dialog box appears that lists the available installation options for installing the client application using the command line or a deployment script.

Table 7-1. Installer Command-Line Options

Installer Option	Value	Description
/?		Displays the installer command-line options.
/a		Performs an administrative installation. For more information, see the Windows Installer documentation .
/a	<i>full path to existing administrative installation</i>	Patches an existing administrative installation.
/s		Hides the initialization dialog box during installation. To install in silent mode, use <code>/s /v/qn</code> . In silent mode, no messages, dialog boxes, or prompts are displayed during installation. You typically use this option when creating a deployment script to run the installer.
/v	<i>key-value pairs</i>	A set of parameters to pass to the installer, specified as key-value pairs. Use the format <code>key=value</code> . These arguments configure runtime options for the ThinApp packages and for the Workspace ONE Access Desktop in general.
/c		Cleans out installation registration information.
/l	<i>[full path to log file]</i>	Performs detailed logging and saves to the specified log file. If you don't specify a log file, a default log in <code>%TEMP%</code> is used.
/x		Unpacks the installer into the <code>%TEMP%</code> folder.

Key-Value Pairs for the /v Option

You can use the following key-value pairs for the /v installer option.

Table 7-2. Keys for the /v Installer Command-Line Option

Key	Value	Description
WORKSPACE_SE RVER	<i>Host name or URL of the Workspace ONE Access service</i>	<p>Provides the Workspace ONE Access service host name or URL, to allow the Workspace ONE Access Desktop application to communicate with the service. HTTPS is the required protocol. Enclose the value in quotation marks.</p> <p>Use the following format:</p> <pre>WORKSPACE_SERVER="https://VMwareIdentityManagerFQDN"</pre> <p>or</p> <pre>WORKSPACE_SERVER="VMwareIdentityManagerHostName"</pre> <p>For example:</p> <pre>WORKSPACE_SERVER="https://myserver.mycompany.com"</pre> <pre>WORKSPACE_SERVER="myserver"</pre>
INSTALL_MODE	One of the following: COPY_TO_LOCAL HTTP_DOWNLOAD RUN_FROM_SHARE	<p>Sets the deployment mode for how the Workspace ONE Access Desktop application obtains ThinApp packages at runtime. ThinApp packages are virtualized Windows applications. The ThinApp packages reside on a network share that is integrated with Workspace ONE Access.</p> <ul style="list-style-type: none"> COPY_TO_LOCAL: The user's entitled packages are downloaded to the client Windows system using a file copy. When the user launches a ThinApp package, the virtualized application runs locally on that system. Before the user's first download and use of an entitled ThinApp package and to continue synchronizing the packages to the client Windows system, the client Windows system must join the same Active Directory domain to which the ThinApp packages' network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and copy files from the network share. <p>Important COPY_TO_LOCAL mode requires the ThinApp share to be reachable from the user's Windows system.</p> <ul style="list-style-type: none"> HTTP_DOWNLOAD: The user's entitled packages are downloaded to the client Windows system using the HTTP protocol. When the user launches a ThinApp package, the virtualized application runs locally on that system. The Workspace ONE Access Desktop application uses the user's Workspace ONE Access system account to authenticate to Workspace ONE Access to obtain the list of the user's entitled packages to download. The share user account provided in the Workspace ONE Access console for enabling account-based access to the ThinApp packages' network share is the account used by Workspace ONE Access to access the ThinApp packages from the repository. That share user account for Workspace ONE Access needs read permission on the network share. The account that the user used to log in to the client Windows system and the user's Workspace ONE Access system account do not need to have any permissions on the network share. The client Windows system does not have to join the same domain to which the

Table 7-2. Keys for the /v Installer Command-Line Option (continued)

Key	Value	Description
		ThinApp packages' network share is joined. This download method is typically slower than using the other modes. The benefit to this mode is that the client Windows system does not have to join the Active Directory domain to obtain and run the virtualized application.
		Important For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in Workspace ONE Access must be configured for account-based access.
		Important For Workspace ONE Access 2.6 and later on Windows 2008 R2 or Windows 7, the HTTP_DOWNLOAD option does not work unless you either enable TLS 1.0 in Workspace ONE Access or enable TLS 1.1 or 1.2 in the Windows 2008 R2 or Windows 7 system. To enable TLS 1.0 in Workspace ONE Access, see Knowledge Base article 2144805 . To enable TLS 1.1 or 1.2 on the Windows system, see the Microsoft documentation at https://support.microsoft.com/en-us/kb/3140245 .
		Important HTTP_DOWNLOAD mode requires the IDP URL to be reachable from the user's Windows system.
		<ul style="list-style-type: none"> ■ RUN_FROM_SHARE: The virtualized application is streamed to the client Windows system from the network share when the user launches the ThinApp package. The RUN_FROM_SHARE option is best suited for Windows systems that will always have connectivity to the network share where the ThinApp packages reside, because the ThinApp packages are not present on the Windows system and the virtualized applications only run if the Windows system can connect to the network share. The client Windows system must join the same Active Directory domain to which the ThinApp packages' network share is joined. The user account used to log in to the Windows system is the account that is used to obtain the ThinApp packages from the network share. That account must have the appropriate permissions on the network share to read and execute files on the network share.
		Important RUN_FROM_SHARE mode requires the ThinApp share to be reachable from the user's Windows machine.
		The default value is COPY_TO_LOCAL.
		For all of the modes, the network share must have the appropriate file and sharing permissions configured. See <i>Workspace ONE Access Installation and Configuration</i> .
		Important When installing Workspace ONE Access Desktop in floating Horizon desktops, use the RUN_FROM_SHARE option to avoid copying the ThinApp packages into those stateless Horizon desktop systems.
		When the Workspace ONE Access Desktop application is installed with one of these configurations, the user account that logs into the Windows system must have the appropriate file and sharing permissions on the network share to be able to obtain the ThinApp packages:
		<ul style="list-style-type: none"> ■ The RUN_FROM_SHARE option ■ The COPY_TO_LOCAL option, without also having the AUTO_TRY_HTTP option enabled and account-based access configured in Workspace ONE Access

Table 7-2. Keys for the /v Installer Command-Line Option (continued)

Key	Value	Description
POLLING_INTERVAL	<i>Frequency in seconds</i>	<p>Sets the frequency, in seconds, of synchronization between the installed Workspace ONE Access Desktop application and Workspace ONE Access to check for new ThinApp packages or entitlements. If unspecified, the default value of 300 seconds (5 minutes) applies.</p> <p>For example:</p> <pre>POLLING_INTERVAL=600</pre>
ENABLE_AUTOUPDATE	0 or 1	<p>Turns on or turns off the automatic update check and download activity. If enabled, the installed Workspace ONE Access Desktop application automatically checks if a newer application is available for download. If a newer version is available, the Workspace ONE Access Desktop application automatically downloads and updates itself to the newer version. This option is enabled by default.</p> <p>To turn off automatic update, set the value of this variable to 0. If unspecified, the default value of 1 applies.</p> <p>Installation of automatic updates requires administrator privileges.</p>
SHARED_CACHE	0 or 1	<p>Determines whether the ThinApp package cache is located in a common folder in the Windows system to which the client application is being installed. Set the value of this variable to 1 to specify that all user accounts on the Windows system share a common cache location. By default, the common folder is %ProgramData%\VMware\Identity Manager Desktop\thinapp.</p> <p>If unspecified, the default value of 0 applies, and each Windows user account gets its own cache, and its default location is %LOCALAPPDATA%\VMware\Identity Manager Desktop\thinapp.</p> <p>Note If you specify a shared cache, the Workspace ONE Access Desktop application does not automatically delete ThinApp packages from this shared cache. Because SHARED_CACHE=1 indicates that all user accounts on the Windows system share the same location, the packages must remain in the shared location so that entitled users can use them, even when you unentitle one user. When you unentitle a user from a ThinApp package, the Workspace ONE Access Desktop application unregisters that package for that user. Other entitled users on that Windows system can continue to use the ThinApp package. You can delete the common cache manually to reclaim the space if no user accounts on that Windows system are entitled to use the ThinApp packages. Each ThinApp package has its own folder under the cache location.</p>
CACHE_DIR	<i>Path to folder</i>	<p>Sets the location where ThinApp packages will be cached locally if the HTTP_DOWNLOAD or COPY_TO_LOCAL install modes are used. This value is set per system, not per user, so you must use environment variables, such as %LOCALAPPDATA%, to select user-specific locations. Be sure to escape the % character on the command-line to prevent immediate expansion. For example:</p> <pre>CACHE_DIR=^%LOCALAPPDATA%^%cache</pre>

Table 7-2. Keys for the /v Installer Command-Line Option (continued)

Key	Value	Description
AUTO_TRY_HTTP	0 or 1	When the Workspace ONE Access Desktop application is installed with the COPY_TO_LOCAL option and account-based access is configured for Workspace ONE Access, the AUTO_TRY_HTTP option determines whether the client should automatically try downloading the user's entitled ThinApp packages using the HTTP protocol, similar to the HTTP_DOWNLOAD option, if the first download attempt fails. This option is enabled by default. Set the value of this option to 0 if you do not want the client to try the HTTP protocol for the download automatically.
		Important For the AUTO_TRY_HTTP option to work, the ThinApp packages integration in Workspace ONE Access must be configured for account-based access. See Workspace ONE Access Requirements for ThinApp Packages and the Network Share Repository .
INSTALL_MODULES	thinapp	A comma-separated list specifying which modules to install. Currently, only the thinapp module is available.
MIGRATE_ACTION	One of the following: MOVE COPY NONE	If the old Workspace for Windows application is installed, the installer will migrate data and settings from the old application to the new one. The default value is MOVE. The following settings are moved, copied, or ignored, depending on the value you specify. Cached ThinApp Packages Downloaded ThinApp packages will be copied from the Workspace for Windows cache, %LOCALAPPDATA%\VMware\Horizon ThinApp\PackageCache, to the new cache location, %LOCALAPPDATA%\VMware\Identity Manager Desktop\thinapp. Folder names within the cache folder will be altered.
		Important Properties set for Workspace ONE Access during installation take precedence over any migrated values for those properties. For example, if the INSTALL_MODE in Workspace for Windows was set to COPY_TO_LOCAL, and, while installing Identity Manager Desktop you specify /v INSTALL_MODE=HTTP_DOWNLOAD, then INSTALL_MODE is set to HTTP_DOWNLOAD.

Example: Using the Workspace ONE Access Desktop Command-Line Installer Options

If your Workspace ONE Access instance has a URL of `https://identitymanagerFQDN`, and Workspace ONE Access is configured for account-based access to your ThinApp packages' network share, and you want to silently install the Workspace ONE Access Desktop application to multiple desktops of that Workspace ONE Access instance with these options:

- The ThinApp install option set to HTTP_DOWNLOAD, because you expect these Windows systems will not be likely to join the domain. Workspace ONE Access is appropriately configured for account-based access to the ThinApp packages' network share.

- The clients check for new packages and entitlements with Workspace ONE Access every 60 seconds.

You would create a script that invokes the following command:

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnn.exe /s  
  /v/qn WORKSPACE_SERVER="https://identitymanagerFQDN" INSTALL_MODE=HTTP_DOWNLOAD  
  POLLING_INTERVAL=60
```

where you replace the *n.n.n-nnnnnnn* portion of the file name to match the name of your downloaded Workspace ONE Access Desktop installer.

Install the Workspace ONE Access Desktop Application with Identical Settings to Multiple Windows Systems

To deploy the Workspace ONE Access Desktop application to multiple Windows systems and have the same configuration settings applied to all of those systems, you can implement a script that installs the Workspace ONE Access Desktop application using the command-line installation options.

Important Error messages do not appear on screen when you deploy Workspace ONE Access Desktop silently. To check for errors during a silent installation, monitor the %TEMP% folder, checking for new `vminst.XXXXXX.log` files. The error messages for a failed silent installation appear in these files.

Typically, this deployment scenario is used for Windows systems that are Horizon desktops.

Prerequisites

- Verify that the Windows systems are running Windows operating systems that are supported for the version of the Workspace ONE Access Desktop application you are installing. See the release notes.
- Verify that the Windows systems have supported browsers installed.
- If you want the ability to run a command to familiarize yourself with the available options before you create the deployment script, verify that you have a Windows system on which you can run that command. The command to list the options is only available on a Windows system. See [Command-Line Installer Options for Workspace ONE Access Desktop](#).

Procedure

- 1 Obtain the Workspace ONE Access Desktop installer's executable file and locate that executable file on the system from which you want to silently run the installer.

One method for obtaining the executable file is to download it using the your Workspace ONE Access system's download page. If you have set up your Workspace ONE Access system to provide the Windows application installer from the download page, you can download the executable file by opening the download page's URL in a browser.

- 2 Using the installer's command-line options, create a deployment script that fits the needs of your organization.

Examples of scripts you can use are Active Directory group policy scripts, login scripts, VB scripts, batch files, SCCM, and so on.

For example, if your Workspace ONE Access instance has a URL of `https://identitymanagerFQDN`, you want to silently install the Windows client to Windows systems that you expect will be used off the domain, with the ThinApp deployment mode set to download mode, and have the Workspace ONE Access Desktop application sync with the server every 60 seconds, you would create a script that invokes the following command:

```
VMware-Identity-Manager-Desktop-n.n.n-nnnnnnnn.exe /s  
/v /qn WORKSPACE_SERVER="https://identitymanagerFQDN" INSTALL_MODE=HTTP_DOWNLOAD  
POLLING_INTERVAL=60
```

where you replace the `n.n.n-nnnnnnnn` portion of the file name to match that of your downloaded file.

- 3 Run the deployment script against the Windows systems.

Results

If the silent installation is successful, the Workspace ONE Access Desktop application is deployed to the Windows systems. Users logged in to those Windows systems can access their entitled assets from those systems.

Note A user's entitled ThinApp package is streamed or downloaded and cached to the user's Windows system after the polling interval elapses. As a result, users might see the ThinApp package displayed when they log in to the Workspace ONE Access user portal. The ThinApp package does not start until the client syncs the application on the next polling interval.

What to do next

Verify that Workspace ONE Access Desktop is properly installed on the Windows systems by trying some of the typical user tasks.

Add Workspace ONE Access Desktop Installer Files to Workspace ONE Access Virtual Appliances

When new versions of Workspace ONE Access Desktop are released, you copy and install the zip file from the VMware Downloads page to each Workspace ONE Access virtual appliance in your deployment. You run the `check-client-updates.pl` command to deploy the installer files and restart the Tomcat service on each virtual appliance.

Prerequisites

- Users must have administrator privileges on their computers to install and automatically update the Workspace ONE Access Desktop application. If users do not have administrator privileges, you can use software distribution tools to distribute and update the application to your users.
- Schedule adding these installer files to the Workspace ONE Access virtual appliances during a maintenance window since the virtual appliance is restarted and this might interrupt user access.

Procedure

1 Download the Workspace ONE Access Desktop zip file from the My VMware Downloads page to a computer that can access the Workspace ONE Access virtual appliance.

2 Copy the zip file to a temporary location in the virtual appliance. For example:

```
scp file.n.n-nnnnnn.zip root@identitymanager-va.com:/tmp/
```

3 Log in to the virtual appliance as the root user.

4 Unzip and install the new zip file to the Downloads directory.

```
/usr/local/horizon/scripts/check-client-updates.pl --install --clientfile /tmp/  
file.n.n.n-nnnnn.zip
```

This script automatically unzips the file and copies the Workspace ONE Access Desktop installer file for the Windows computers to the `/opt/vmware/horizon/workspace/webapps/ROOT/client` directory. It automatically updates to the `/opt/vmware/horizon/workspace/webapps/ROOT/client/cds` directory, and updates the URL parameter value for the downloads link.

5 Restart the Tomcat service on the virtual appliance.

6 Repeat these steps for each Workspace ONE Access virtual appliance in your environment.

Users can download the Workspace ONE Access Desktop application from their Workspace ONE Access accounts or via the download link, `https://WorkspaceONEAccessFQDN/download`. Users' Workspace ONE Access Desktop applications are automatically updated when they download the new version.

Using the Workspace ONE Access Command-Line `hws-desktop-ctrl.exe` Application

The Workspace ONE Access Desktop application includes a command-line application, `hws-desktop-ctrl.exe`, that you can use to perform operations related to using ThinApp packages on the user's Windows system.

The installation process for the Workspace ONE Access Desktop application installs `hws-desktop-ctrl.exe` in the `HorizonThinApp` folder in the Windows directory location where the Workspace ONE Access Desktop application is installed.

To use the `hws-desktop-ctrl.exe` application to perform one of its supported commands, use the following format.

```
hws-desktop-ctrl.exe command options
```

Command	Description
<code>hws-desktop-ctrl.exe recheck</code>	This command immediately does an entitlement check of the ThinApp packages that are associated with the user account that is logged into the Workspace ONE Access Desktop application. Any newly entitled or updated ThinApp packages are synced.
<code>hws-desktop-ctrl.exe set InstallMode=<i>install_mode</i></code>	This command changes the ThinApp deployment mode used for ThinApp packages on this Windows system. Because this command changes the registry keys associated with the ThinApp deployment mode, only administrators with the appropriate registry permissions are able to change the install mode using this command. Available values for <i>install_mode</i> are: <ul style="list-style-type: none"> ■ CopyToLocal ■ RunFromShare ■ HttpDownload
<code>hws-desktop-ctrl.exe authorize guid=<i>ThinApp_GUID</i> path=<i>package_path</i></code>	This command verifies whether a ThinApp package can be launched. This command does not actually launch the ThinApp package. Provide the ThinApp package's GUID and the path to the package's executable file. If ThinApp download mode is used for the packages on the Windows client system, the path is relative to the local cache root folder, which is the same as the path relative to the repository root. An example is <pre>hws-desktop-ctrl.exe authorize guid= 436E1D7D-552C-4F70-8197-DB1B05D30394 path="FileZilla Client 3.3.2/FileZilla.exe"</pre> <p>You can see the ThinApp package's GUID, application path, and executable file name on its resources page in the Workspace ONE Access console.</p>
<code>hws-desktop-ctrl.exe quit</code>	This command tells the Workspace ONE Access Desktop application to exit cleanly.
<code>hws-desktop-ctrl.exe launch app=<i>package_path</i> url=<i>launch_url</i></code>	This command is used to manually launch a ThinApp package, where <i>package_path</i> is the path to the package's executable file, and <i>launch_url</i> is the Workspace ONE Access protocol URL for that package, in the form <code>horizon://package_path</code> . An example is <pre>hws-desktop-ctrl.exe launch app="FileZilla Client 3.3.2/FileZilla.exe" url="horizon://FileZilla Client 3.3.2/FileZilla.exe"</pre> <p>This command is not typically used by end users, who can launch their entitled ThinApp packages from their Workspace ONE portal. This command is typically used for debugging.</p>

Providing Access to Citrix-Published Resources in VMware Workspace ONE Access



You can integrate your Citrix deployment with Workspace ONE Access (formerly called VMware Identity Manager) to provide users the ability to access their assigned Citrix-published resources from the Workspace ONE Intelligent Hub app or portal. Citrix-published resources include applications and desktops in Citrix XenApp and XenDesktop server farms. Desktops are also referred to as Citrix-published delivery groups.

You manage Citrix-published applications and desktops in the Citrix management console. You also set user and group entitlements in the Citrix console, not in the Workspace ONE Access console. You must sync these users and groups to the Workspace ONE Access service from Active Directory before integrating Workspace ONE Access with the Citrix server farms.

To integrate Citrix server farms with Workspace ONE Access, you create one or more virtual apps collections in the Workspace ONE Access console. The collections contain the configuration information for the server farms as well as sync settings.

You can set up a sync schedule for each collection to regularly sync resources and entitlements from the Citrix server farms to the Workspace ONE Access service.

After you integrate the Citrix server farms, you can view the synced resources and entitlements in the Workspace ONE Access console.

End users can launch Citrix-published applications and desktops from the Intelligent Hub app or portal. They install Citrix Workspace app (formerly called Citrix Receiver) on their systems and devices to access the resources to which they are entitled.

Note Workspace ONE Access supports Citrix deployments that include Citrix NetScaler.

Supported Citrix Versions

- Workspace ONE Access supports the following Citrix versions:
 - Citrix Virtual Apps and Desktops 7 1912 LTSR
 - XenApp and XenDesktop 7.15 LTSR
 - XenApp and XenDesktop 7.6 LTSR

- Workspace ONE Access connects to the Citrix server farm using the Citrix StoreFront API. In your Citrix deployment, make sure that the StoreFront version corresponds to the Citrix server farm version.

Note Workspace ONE Access does not support Citrix Web Interface.

Note Using the latest available version of Workspace ONE Access and its components is recommended.

Supported Citrix Authentication Methods

Workspace ONE Access only supports password-based authentication on the XenApp server or NetScaler server. It does not support other authentication methods such as Smart Card, HTML 5, 2 factor authentication, or SAML authentication (Citrix FAS).

Supported Citrix Features

Workspace ONE Access supports the following XenApp and XenDesktop features.

- Application and desktop launch with Citrix StoreFront API
- External launch with NetScaler
- Application group functionality

Workspace ONE Access supports the application group feature available in Citrix deployment versions 7.15 LTSR and 1912 LTSR. Application groups are a logical grouping of applications and desktops, and entitlements can be provided at the application group level.

- Disabling applications on the XenApp and XenDesktop server

If the administrator disables an application on the XenApp or XenDesktop server, the application is hidden in Workspace ONE Access.

- Limiting visibility for an application

This feature sets the visibility for an application. Workspace ONE Access honors the entitlements set at the application level.

- Showing an application to the entire delivery group

In XenApp and XenDesktop, visibility for an application can be set to **Show this application to entire delivery group**. The application inherits the entitlements from the delivery group.

- Entitlements at the desktop level

Workspace ONE Access honors entitlements for desktops that are set at the desktop level.

- Static desktop sync and launch

Static desktops configured in XenApp and XenDesktop can be synced and launched from Workspace ONE Access.

Citrix StoreFront Requirements

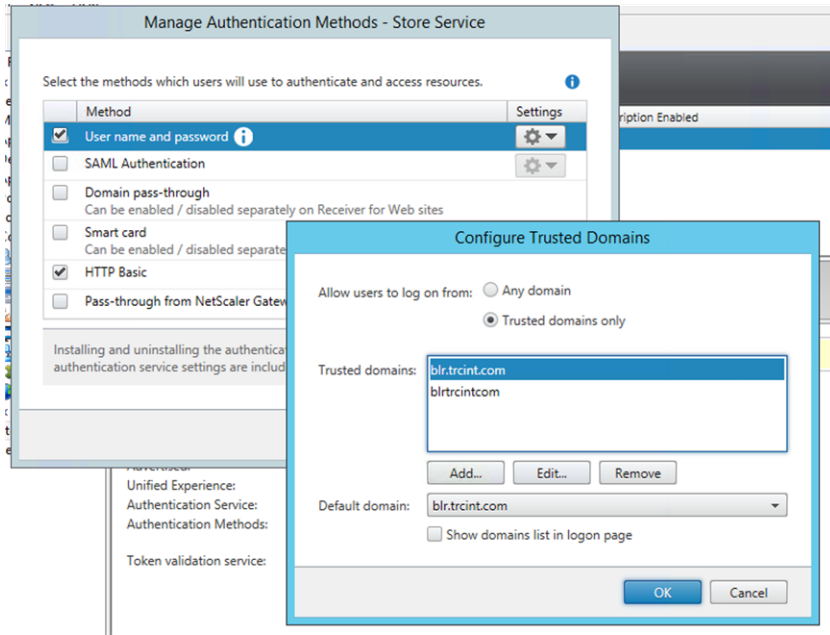
The Virtual App service uses the Citrix StoreFront REST API to authenticate with and generate ICA files from the Citrix deployment to launch desktops and applications.

Make sure that you meet the following requirements for StoreFront.

- Ensure that StoreFront is supported by the Citrix server farm version that you are using and that the StoreFront version corresponds to the Citrix server farm version.
- Ensure that all instances of the Workspace ONE Access Virtual App service can communicate with the StoreFront server.
- Ensure that you specify the same farm name in StoreFront and in the Citrix Delivery Controller or XML Broker.
- If the StoreFront URL is behind a load balancer, ensure that the load balancer does not have any additional authentication requirements such as MFA. The Virtual App service must be able to access the StoreFront URL without additional authentication requirements from the load balancer.

The Virtual App service only supports the NetScaler load balancer. It does not support any other load balancers.

- Workspace ONE Access only supports user name and password authentication on the XenApp server or NetScaler server. It does not support other authentication methods such as Smart Card, HTML 5, 2 Factor Authentication, or SAML Authentication (Citrix FAS).
- In the StoreFront server, when you configure authentication for a store, trusted domains can be configured for the "User name and password" authentication method. If you configure trusted domains, ensure that you add domain names in the fully qualified domain name format to the "Trusted domains" list. If you use NetBIOS names for StoreFront, add the fully qualified domain name in addition to the NetBIOS name. Workspace ONE Access requires the fully qualified domain name. If only the NetBIOS name is added, Citrix application and desktop launch from Workspace ONE will fail.



Note To use the StoreFront REST API, you do not need to download or copy any additional files to your Workspace ONE Access installation.

This chapter includes the following topics:

- Components Required for Citrix Integration with Workspace ONE Access
- Synchronization of Citrix-published Resources and Assignments to Workspace ONE Access
- Launch of Citrix-published Applications and Desktops Integrated with Workspace ONE Access
- Configuring Citrix Server Farms in Workspace ONE Access
- Configuring Citrix Resource Launch in Workspace ONE Access
- Configuring Workspace ONE Access Settings for Citrix Integration
- Launching Citrix-Published Resources Integrated with Workspace ONE Access

Components Required for Citrix Integration with Workspace ONE Access

To integrate a Citrix deployment with the Workspace ONE Access service, you need the following components.

- A Workspace ONE Access cloud service tenant or on-premises instance.
- One or more instances of the Virtual App service deployed on premises. The Virtual App service is a component of Workspace ONE Access Connector 21.08 and later. You can download the connector from the Workspace ONE Access product page on <https://my.vmware.com>.

When you install the Virtual App service, make sure that you follow the requirements and prerequisites for Citrix integration described in the *Installing VMware Workspace ONE Access Connector* guide. These include:

- The Virtual App service server must be joined to the directory domain.
 - You must specify a domain user account to use to run the Virtual App service. That domain user must also be a Citrix server Read Only administrator who is able to load the Citrix PSSnapin.
 - You must install Citrix Studio on the Virtual App service server. Citrix Studio includes the Citrix PowerShell SDK, which is required for the integration between Citrix and Workspace ONE Access. The Citrix Studio version must be compatible with your Citrix deployment version.
- A Citrix deployment on premises.

While deploying the on-premise components, make sure that you meet the following requirements:

- All instances of the Virtual App service must be able to communicate with the Citrix server farm.
- All instances of the Virtual App service must be able to communicate with Citrix StoreFront.

All communication between the Workspace ONE Access service and the on-premise components is through the connector. The connector and the service communicate over a communication channel that is automatically set up during installation.

Note Using the latest available version of Workspace ONE Access and its components is recommended.

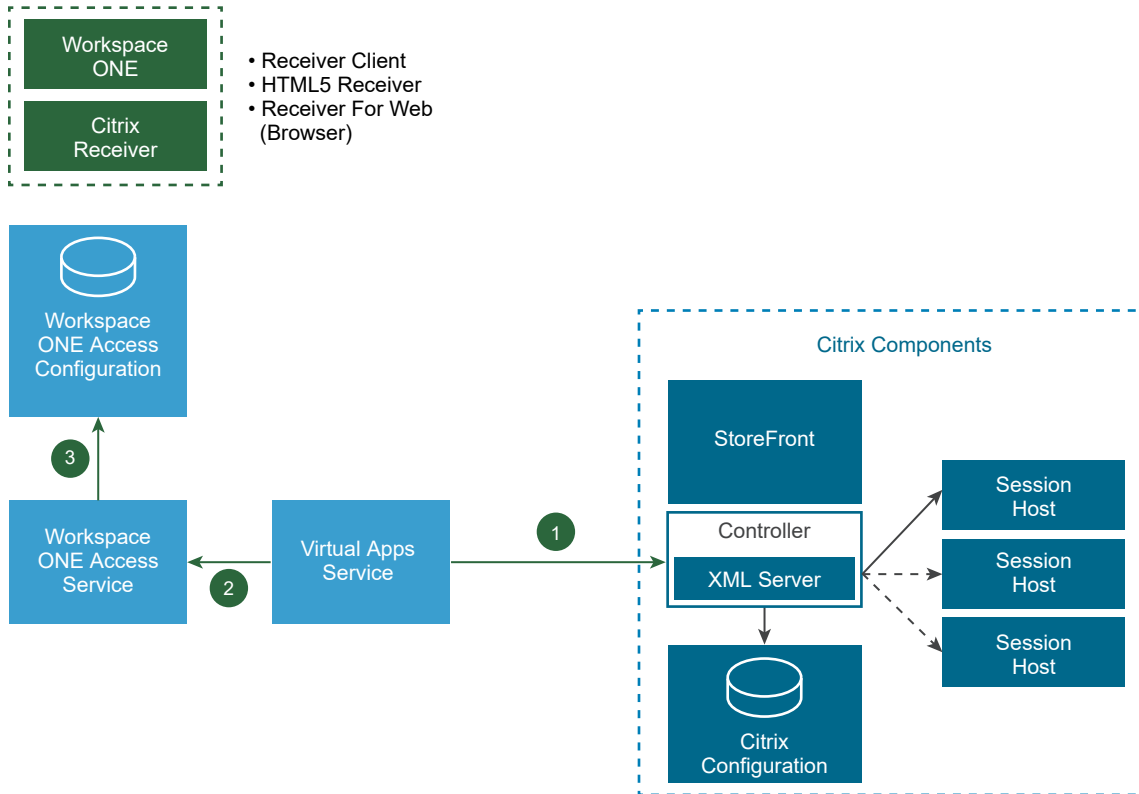
Synchronization of Citrix-published Resources and Assignments to Workspace ONE Access

Workspace ONE Access synchronizes Citrix-published applications and desktops, and user assignments, from the Citrix server farm to the Workspace ONE Access service using the Virtual App service. You can set a sync schedule to sync applications, desktops, and assignments at regular intervals.

The Citrix farm is the single source of truth for all supported operations in Workspace ONE Access. You manage the resources and entitle users to them in the Citrix administrative interface.

When resources or entitlements are added, changed, or deleted in the Citrix farm, the information is updated in Workspace ONE Access after a sync.

Synchronization Architecture Diagram



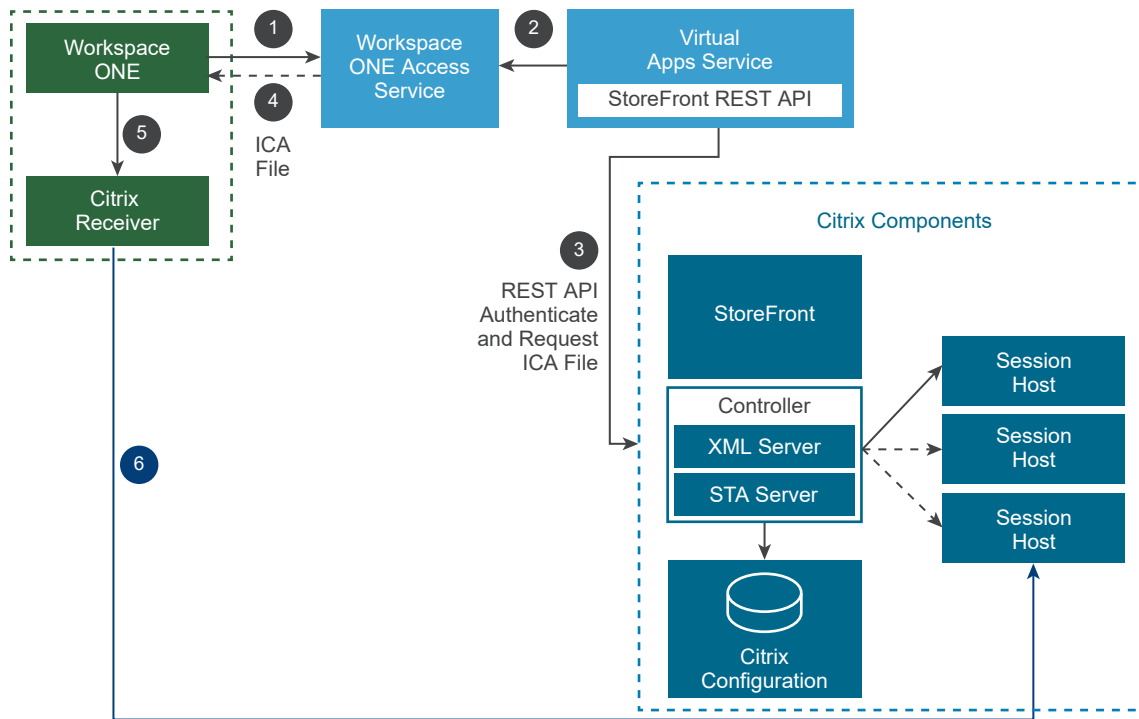
- 1 The Workspace ONE Access Virtual App service fetches application, desktop, and entitlements information from the Citrix XML server.
- 2 The Virtual App service compares the new information with the existing application, desktop, and entitlements information and sends the differences to the Workspace ONE Access service.
- 3 The Workspace ONE Access service stores the results in the Workspace ONE Access database.

Launch of Citrix-published Applications and Desktops Integrated with Workspace ONE Access

Workspace ONE Access uses the Virtual App service and the Citrix StoreFront REST API to launch Citrix-published applications and desktops from the Workspace ONE Intelligent Hub portal or app. You can configure internal and external access to the Citrix-published resources. End users must install Citrix Workspace app or Citrix Receiver on their systems or devices to launch the applications and desktops to which they are entitled.

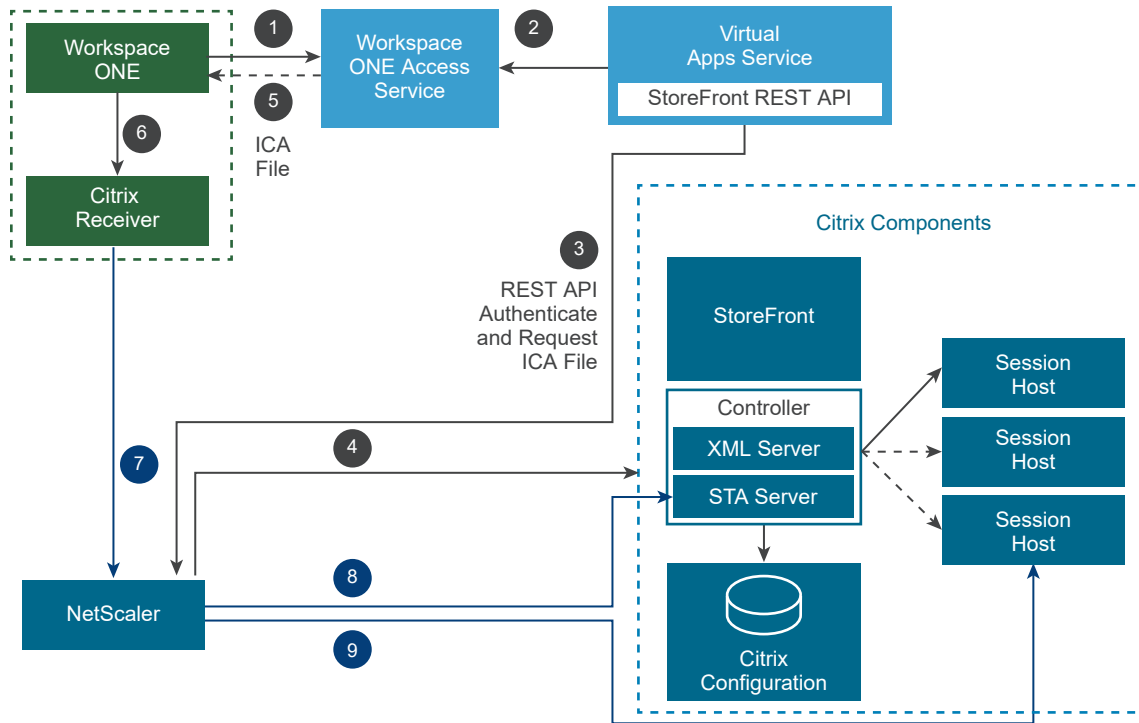
Note Workspace ONE Access does not support Citrix Web Interface.

Launch Architecture Diagram (Internal Access)



- 1 A user launches a Citrix-published application or desktop from the Workspace ONE Intelligent Hub portal or app.
- 2 The request goes to the Workspace ONE Access service, which sends it to the Virtual App service.
- 3 The Virtual App service communicates with the Citrix server farm through the StoreFront REST API to authenticate and request the ICA file.
- 4 The ICA file is retrieved and passed to the Intelligent Hub portal or app.
- 5 The ICA file is passed to the Citrix Workspace app or Citrix Receiver.
- 6 The Citrix Workspace app or Citrix Receiver launches the application or desktop.

Launch Architecture Diagram (External Access)



- 1 A user launches a Citrix-published application or desktop from the Workspace ONE Intelligent Hub portal or app.
- 2 The request goes to the Workspace ONE Access service, which sends it to the Virtual App service.
- 3 To communicate with the Citrix server farm to authenticate and request the ICA file, the Virtual App service sends a request to NetScaler through the StoreFront REST API.
- 4 NetScaler forwards the request to the StoreFront server.
- 5 The ICA file is retrieved and passed to the Intelligent Hub portal or app.
- 6 The ICA file is passed to the Citrix Workspace app or Citrix Receiver.
- 7 Citrix Workspace app or Citrix Receiver communicates with Netscaler.
- 8 NetScaler communicates with the Citrix STA server with the STA ticket and gets the Citrix session server information.
- 9 NetScaler communicates with the Citrix Session Host server and creates a session for application launch.

Note In version 7.x, the Citrix Session Host server is referred to as the Citrix VDA server.

Configuring Citrix Server Farms in Workspace ONE Access

To configure Citrix server farms in Workspace ONE Access, you create one or more virtual apps collections from the Virtual Apps Collections page. The collections contain configuration information such as the Citrix servers from which to sync applications, desktops, and assignments, the Virtual App service instance to use for sync, and sync settings.

You can add all your Citrix server farms in one collection or create multiple collections, based on your requirements. For example, you may choose to create a separate collection for each farm for easier management and to distribute the sync load across multiple Virtual App service instances. Or you may choose to include all server farms in one collection for a test environment and have another identical collection for your production environment.

Before you configure Citrix published resources in Workspace ONE Access, ensure that you meet all the prerequisites.

Also follow these guidelines for Citrix server farm settings.

- If you use the Limited Visibility Group option to restrict users, ensure that the Limited Visibility Group contains users or groups. If it does not contain any users or groups, no entitlements are synced to Workspace ONE Access.
- Ensure that all Citrix-published applications and desktops in a Site contain valid users. If you delete a user or group, make sure that you remove the user or group from the Citrix-published applications and desktops too.
- Make sure that users and groups have been assigned to the correct Delivery Group.
If you select settings to restrict users, make sure that they include users and groups.
- XenDesktop and XenApp 7.x and later versions allow you to set entitlements for all authenticated users at the delivery group level with the "Allow any authenticated user to use this delivery group" setting. Workspace ONE Access does not support this setting. To ensure that users have the correct entitlements in Workspace ONE Access, set explicit entitlements for the users and groups.
- Workspace ONE Access does not support the Citrix anonymous user group feature.

Prerequisites

- Configure your Workspace ONE Access environment. See *Installing and Configuring Workspace ONE Access* and *Workspace ONE Access Administration* for information.
- Install the Virtual App service component of the Workspace ONE Access connector. See *Installing VMware Workspace ONE Access Connector 21.08* for information.
- Sync users and groups with Citrix entitlements from your enterprise directory to Workspace ONE Access using directory sync.

While creating the directory in Workspace ONE Access, map the userPrincipalName attribute to the Active Directory attribute userPrincipalName and the distinguishedName attribute to the Active Directory attribute distinguishedName. Also make sure that users have a value set for the userPrincipalName and distinguishedName attributes, otherwise they might not be able to run their desktops and applications.

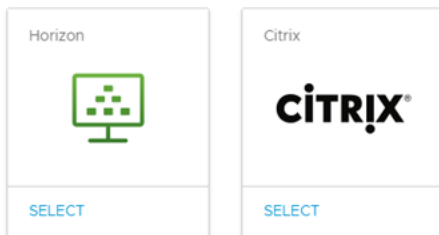
- Ensure that you meet the StoreFront requirements listed in [Chapter 8 Providing Access to Citrix-Published Resources in VMware Workspace ONE Access](#).
- Review the Citrix documentation for your version of Citrix software.
- To perform this task in the Workspace ONE Access console, use an administrator role that can perform the Manage Desktop Apps action in the Catalog service.
- At the end of this procedure, you are redirected to the Network Ranges page to configure Client Access FQDNs. To edit and save network ranges, you require a Super Admin role, or a custom role that can perform the Manage Settings action in the Identity and Access Management service. You can choose to perform that step separately.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 If an information page appears, review the information and click **Get Started**, otherwise click **New**.
- 4 Select **Citrix** as the source type.

Select the Source Type

Select the source type to use to create the virtual apps collection.



- 5 In the New Citrix Collection wizard, enter the following information in the Connector page.

Option	Description
Name	Enter a unique name for the Citrix virtual apps collection.
Connector	Select the connectors to use to sync this collection. You can add multiple connectors and arrange them in failover order. Only connectors that have the Virtual App service installed appear in the list.



For example:

Name *

Citrix Apps

Connector

Select the connectors to use to sync this collection. If multiple connectors are available, you can add them and arrange them in fallback order. Only connectors associated with the same directory should be used.

1.  connector1.example.com 

6 In the Server Farm page, click **Add Server Farm** and enter your Citrix server farm information.

Option	Description
Server	<p>Click Add Server and add the fully-qualified domain name of your Citrix XML server (XML broker). For example, xenappserver.example.com. You must add at least one Citrix XML server.</p> <p>To add multiple servers, click Add Server and add the servers.</p> <p>Arrange the servers in failover order. Workspace ONE Access follows this order for SSO and for failover. To rearrange the list, click and drag the rows to the desired position. To delete a server from the list, click the x icon at the right of the row.</p>
StoreFront Server URL	<p>Enter the StoreFront server URL in the following format:</p> <p><i>transportType://storefrontServerFQDN/Citrix/storenameWeb</i></p> <p>For example: <i>http://xen76.example.com/Citrix/mystoreWeb</i></p> <hr/> <p>Note This is the StoreFront server Website URL.</p> <hr/> <p>Important Later, after creating the virtual apps collection, when you configure internal network ranges for the collection, ensure that you enter the same StoreFront server URL in the Client Access URL Host text box.</p>

For example:

Add Server Farm

Version 7.x of XenApp or XenDesktop server is supported.

Server

Add Citrix XML Servers and arrange them in failover order. At least one server is required.

Server Name

citrixserver.example.com



+ ADD SERVER

StoreFront Server URL ^{*} ⓘ

http://storefrontserver.example.com/Citrix/StoreWeb

- 7 In the Configuration page, enter the following information.

Option	Description
Sync Frequency	Select how often you want to sync applications, desktops, and assignments from the Citrix server farm to Workspace ONE Access. You can set up an automatic sync schedule or choose to sync manually. To set a schedule, select the interval such as daily or weekly and select the time of day to run the sync. If you select Manual , you must click Sync > Sync with safeguards or Sync > Sync without safeguards on the virtual apps collection page after you create the collection and whenever there is a change in the Citrix resources or assignments. For more information about sync, see Syncing Virtual Apps Collections in Workspace ONE Access .
Sync Duplicate Apps	Set to No if you want to prevent duplicate applications from being synced from multiple servers. When Workspace ONE Access is deployed in multiple data centers, the same resources are set up in the multiple data centers. Setting this option to No prevents duplication of the applications and desktops in the Intelligent Hub catalog.
Sync Categories from Server Farms	Select this option if you want to sync categories from the Citrix servers to Workspace ONE Access.

Option	Description
Safeguard Thresholds Limits	<p>Configure sync safeguard thresholds if you want to limit the number of changes that can be made to applications, desktops, and entitlements when a virtual apps collection syncs. If any of the thresholds is met, sync is cancelled.</p> <p>By default, Workspace ONE Access sets the threshold for all categories to 10%.</p> <p>Sync safeguards are ignored the first time a collection syncs and are applied to all subsequent syncs.</p> <p>For more information about sync safeguards, see Syncing Virtual Apps Collections in Workspace ONE Access.</p>
Activation Policy	<p>Select how you want to make resources in this collection available to users in the Intelligent Hub portal and app. If you intend to set up an approval flow, select User-Activated, otherwise select Automatic.</p> <p>With both the User-Activated and Automatic options, the resources are added to the Apps tab. Users can run the resources from the Apps tab or mark them as favorites and run them from the Favorites tab. However, to set up an approval flow for any of the apps, you must select User Activated for that app.</p> <p>The activation policy applies to all user entitlements for all the resources in the collection. You can modify the activation policy for individual users or groups per resource, from the user or group page in the Users & Groups tab.</p>

- 8 In the Summary page, review your selections, then click **Save & Configure** to configure network ranges.

The collection is created but the resources in the collection are not yet synced. The **Network Ranges** tab appears.

What to do next

- Configure network ranges for resource launch. See [Configuring Citrix Resource Launch in Workspace ONE Access](#).
- To sync the resources and entitlements in the collection from the Citrix servers to Workspace ONE Access, you can either wait for the scheduled sync time or select the collection in the Virtual Apps Collections page and click **Sync > Sync with safeguards** or **Sync > Sync without safeguards**.

Note Workspace ONE Access does not support the Citrix anonymous user group feature.

Configuring Citrix Resource Launch in Workspace ONE Access

After configuring the virtual apps collection for Citrix-published resources, configure network IP ranges for resource launch. You can specify whether users' application or desktop launch traffic (ICA traffic) from specific network ranges is routed through NetScaler or through a direct connection to the XenApp server. This enables you to serve the needs of users for both external and internal access to the Citrix resources in your deployment.

When a user launches an application or desktop from the Workspace ONE catalog, if the user's IP address falls in a network range configured for NetScaler, the ICA traffic is routed through NetScaler to the XenApp server. If the IP address falls in the direct connection range, the ICA traffic is routed directly to the XenApp server.

Configuring Citrix Resource Launch for Internal Networks in Workspace ONE Access

Configure the network ranges from which you want users' application or desktop launch traffic (ICA traffic) to be routed directly to the XenApp server. This configuration is typically used to provide internal access to the Citrix-published resources integrated with Workspace ONE Access.

When a user launches an application or desktop from the Workspace ONE Intelligent Hub app or portal, if the user's IP address falls in the internal network range, the ICA traffic is routed directly to the XenApp server.

Note To configure resource launch for external networks, see [Configuring Citrix Resource Launch for External Networks with NetScaler Gateway](#).

Prerequisites

A Super Admin role, or a custom role that can perform the Manage Settings action in the Identity and Access Management service, is required to create and edit network ranges.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Click the Citrix collection for which you want to set network ranges.
- 3 Select the **Network Ranges** tab.
- 4 In the **Network Ranges** tab, click the network range to configure for internal Citrix resource launch so that end users accessing Citrix resources from an internal network can connect to the correct server.
 - a Click the network range to edit or create a new network range, if necessary.
 - b If you are creating a new network range, enter a name, optional description, and the IP address range.
 - c Scroll to the **Server Farm** section.

This section lists all the XenApp servers that you configured in the Citrix virtual apps collection.

- d For each XenApp server, enter the appropriate values for this network range.

Option	Description
Client Access FQDN	Enter the complete StoreFront URL. This entry must match the URL that you entered in the StoreFront Server URL text box in the virtual apps collection. Use the following format: <i>transportType://storefrontServerFQDN/Citrix/storenameWeb</i> For example: <code>http://xen76.example.com/Citrix/mystoreWeb</code> If a load balancer is configured, use the following format: <i>loadbalancerURL/citrix/storeweb</i>
Port	The StoreFront server port. For example, 443. If you entered a load balancer URL in the Client Access FQDN text box, use port 443.
NetScaler	Set this option to No .

XenApp Farm UUID	XenApp Farm Server	Client Access FQDN	Port	NetScaler
acfa4389-feba-4651-945f-7d6a3bbec008	xenapptest.example.com	xenapptest.example.com	443	No <input type="checkbox"/>

- e Click **Save**.
- f Repeat these steps to edit the other network ranges, if necessary.

Important Verify that each network range in your environment has a Client Access FQDN set. If a network range is missing the Client Access FQDN, users accessing resources through that network range cannot launch their Citrix desktops and applications.

Configuring Citrix Resource Launch for External Networks with NetScaler Gateway

VMware Workspace ONE Access supports Citrix deployments that include NetScaler Gateway. NetScaler Gateway is typically used to provide external access to XenApp or XenDesktop applications or desktops.

If your Citrix deployment includes a NetScaler Gateway appliance, you can configure VMware Workspace ONE Access with the appropriate settings so that when users launch Citrix resources, the traffic is routed through the NetScaler Gateway appliance to the XenApp server.

You set policies on client network IP ranges that specify whether launch traffic is routed through NetScaler Gateway to the XenApp server or whether it is routed directly to the XenApp server. This allows you to meet both external and internal access needs.

Note VMware Workspace ONE Access also supports Citrix Secure Gateway. The configuration steps in this section are applicable to both NetScaler Gateway and Citrix Secure Gateway.

Configure Network Range for NetScaler Gateway in Workspace ONE Access

You can configure the network ranges for which you want users' application or desktop launch traffic (ICA traffic) to be routed through NetScaler Gateway to the XenApp server. This configuration is typically used to provide external access to Citrix-published resources integrated with Workspace ONE Access.

When a user launches an application or desktop from the Workspace ONE Intelligent Hub portal or app, if the user's IP address falls in the IP range configured for NetScaler Gateway, the ICA traffic is routed through NetScaler Gateway to the XenApp server.

Note To configure resource launch for internal networks, see [Configuring Citrix Resource Launch for Internal Networks in Workspace ONE Access](#).

Prerequisites

- A Super Admin role, or a custom role that can perform the Manage Settings action in the Identity and Access Management service, is required to create and edit network ranges.

Procedure

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Click the Citrix collection for which you want to configure network ranges.
- 3 Select the **Network Ranges** tab.
- 4 In the Network Ranges page, click the network range to configure for Netscaler Gateway.
 - a Click the network range to edit or create a new network range, if necessary.
 - b If you are creating a new network range, enter a name, optional description, and the IP address range.
 - c Scroll to the **Server Farm** section.

This section lists all the XenApp servers configured in the Citrix virtual apps collection.

- d For each XenApp server, enter the appropriate values for this network range.

Option	Description
Client Access FQDN	The NetScaler Gateway appliance host name. For example: <code>netscalerhost.example.com</code>
Port	The NetScaler Gateway appliance port. For example: <code>443</code>
NetScaler	Set this option to Yes .

XenApp Farm UUID	XenApp Farm Server	Client Access FQDN	Port	NetScaler
acfa4389-feba-4651-945f-7d6a3bbee008	xenapptest.example.com	<input type="text" value="netscalerhost.example.com"/>	<input type="text" value="443"/>	Yes <input checked="" type="checkbox"/>

Note If you are using Citrix Secure Gateway instead of NetScaler Gateway, enter the Citrix Secure Gateway host name and port, and set the NetScaler option to **Yes**.

- e Click **Save**.
- f Repeat these steps to edit the other network ranges, if required.

Important Verify that each network range in your environment has a Client Access FQDN set. If a network range is missing the Client Access FQDN, users accessing resources through that network range cannot launch their Citrix desktops and applications.

Configuring Workspace ONE Access Settings for Citrix Integration

After you configure the Citrix integration with Workspace ONE Access, you can view the synced Citrix applications and desktops as well as user entitlements in the Workspace ONE Access console. You can also configure several settings for the integration from Workspace ONE Access. You can create categories, configure delivery settings, and set access policies for Citrix-published applications and desktops.

Managing Categories for Citrix-Published Resources Integrated with Workspace ONE Access

You can manage categories for Citrix-published resources from the Workspace ONE Access console and from your Citrix deployment.

Workspace ONE Access does not support the following settings for categories:

- Nested categories
- Tags
- Citrix Filtering when it is set in StoreFront

In your Citrix deployment, you give a Citrix-published application or desktop a category name by editing the **Client application folder** text box in the resource's properties. When you integrate your Citrix deployment with Workspace ONE Access, existing category names for Citrix-published applications and desktops are carried over to Workspace ONE Access.

After the integration, you can continue to create categories in your Citrix deployment. If you enabled the **Sync categories from server farms** option for the virtual apps collection, the new categories appear in Workspace ONE Access at the next sync. When you update a category name in your Citrix deployment, the updated category name appears in Workspace ONE Access at the next sync.

You can also create categories directly in Workspace ONE Access. You create, assign, and view categories from the **Catalog > Virtual Apps** page in the Workspace ONE Access console.

When you create a category in Workspace ONE Access, the category does not appear in your Citrix deployment.

Setting Access Policies for Specific Applications and Desktops in Workspace ONE Access

The default access policy set applies to all applications and desktops in your Workspace ONE Access catalog. You can also set access policies for individual applications or desktops, which override the default access policy.

You can configure application policies for desktops and applications from the application configuration page or from the Policies page in the Workspace ONE Access console.

For detailed information on access policies and how they are applied, see the *Workspace ONE Access Administration Guide*.

Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
 - a In the Workspace ONE Access console, click the **Catalog > Virtual Apps** tab.
 - b Click the application.
 - c Click **Edit**.

Certain fields on the application page are now editable.
 - d In the **Access Policies** section, select the access policy for the application.
 - e Click **Save** at the top of the page.
- 2 To apply an access policy to one or more applications and desktops from the Policies page, follow these steps.
 - a In the Workspace ONE Access console, navigate to the **Identity & Access Management > Policies** page.
 - b Click a policy to edit or click **Add Policy** to create a new policy.

- c In the Definition page of the wizard, in the **Applies to** section, select the applications and desktops to which you want to apply the policy.
- d In the **Applies to** section, select the applications to which you want to apply the policy.
- e Save your changes.

Viewing User and Group Assignments for Citrix-Published Resources in Workspace ONE Access

In the Workspace ONE Access console, you can view user and group assignments for Citrix-published applications and desktops. These assignments are set in your Citrix deployment and synced to Workspace ONE Access. You cannot edit the assignments from Workspace ONE Access.

Prerequisites

To see the latest updates, manually sync resources and entitlements from the Citrix server farms to Workspace ONE Access from the **Catalog > Virtual Apps Collections** page.

Procedure

- 1 Log in to the VMware Workspace ONE Access console.
- 2 View user and group assignments for Citrix-published resources.

Citrix-published resources include Citrix-published applications and Citrix-published desktops, which are also referred to as delivery groups.

Option	Action
List users and groups assigned to a specific Citrix-published application or desktop	<ul style="list-style-type: none">a Click the Catalog > Virtual Apps tab.b (Optional) Click the icon in the Type column heading and select Citrix Published Application and Citrix Published Delivery Group to view all Citrix-published resources. You can also search for an application or desktop by name.c Click the desktop or application.d Click View Assignments. All users and groups to whom the application is assigned are listed.
List Citrix-published application and desktop assignments for a specific user or group	<ul style="list-style-type: none">a Click the Users & Groups tab.b Click the Users tab or the Groups tab.c Click the name of an individual user or group.d Click the Apps tab. Citrix-published application and desktop assignments for the user or group are listed.

Launching Citrix-Published Resources Integrated with Workspace ONE Access

When users launch a Citrix-published desktop or application from the Workspace ONE Intelligent Hub portal or app, an ICA file is downloaded and passed to the Citrix Workspace app or Citrix Receiver. Citrix Workspace app and Citrix Receiver are native OS applications which launch Citrix-published desktops and applications. The launch experience varies across different platforms and browsers.

Launch Process

Depending on the platform and browser, the application or desktop is launched differently. In some cases the application or desktop is launched directly. In other cases, the user needs to associate the .ica file type with the Citrix Workspace app or Citrix Receiver first so that the application or desktop can be launched directly. In a few cases, the user needs to click the downloaded ICA file to launch the application or desktop. See the table for detailed information.

Platform	Browser	How the application or desktop is launched	Action Required
Windows	Firefox	Launches the application or desktop directly	None
	Chrome	Launches the application or desktop directly.	None
	Internet Explorer	Downloads the ICA file with a .ica extension. After the file type is associated with the Citrix Workspace app or Citrix Receiver, launches the application or desktop automatically.	In the browser, associate the .ica file type with the Citrix Workspace app or Citrix Receiver.
	Edge	Launches the application or desktop directly.	None
Mac	Safari, Firefox	Launches the application or desktop directly	None
	Chrome	Launches the application or desktop directly	None
Windows Surface	Chrome	Downloads the ICA file with a .ica extension. After the file type is associated with the Citrix Workspace app or Citrix Receiver, launches the application or desktop automatically.	In the browser, associate the .ica file type with the Citrix Workspace app or Citrix Receiver.
Android	Chrome	Downloads the ICA file	Click the ICA file to launch the desktop or application.

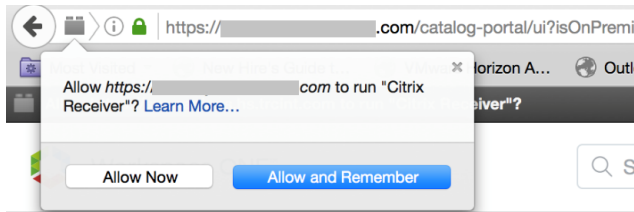
Platform	Browser	How the application or desktop is launched	Action Required
iOS	Safari	Downloads the ICA file	Click the ICA file to launch the desktop or application.
	Chrome	Unable to download the ICA file	This scenario is not supported.

Note There is a known issue with application launch on Chrome browsers related to NPAPI plugins. If users are unable to launch their applications or desktops on Chrome, you can turn off the Workspace ONE Access feature flag `orgUseNonNPAPIForCitrixLaunch`. With the feature flag turned off, the browser downloads the ICA file and users can click it to launch their application or desktop. For more information, see "Disabling Feature Flag for Citrix Application Launch on Chrome" in *Troubleshooting Citrix-Published Resources Configuration in Workspace ONE Access*.

Allowing Citrix Workspace app or Citrix Receiver Plugin on Firefox

On Firefox, when users launch a Citrix-published application, they are prompted to allow the Citrix Workspace app or Citrix Receiver plugin.

Allow `https://IdentityManagerHostname` to run Citrix Receiver?



Users must click **Allow Now** or **Allow and Remember** to launch the application.

Providing Access to Third-Party Managed Applications in Workspace ONE Access

9

You can add third-party identity providers as an application source in Workspace ONE Access to simplify the deployment of large numbers of applications from these third-party identity providers to the Workspace ONE Intelligent Hub catalog. Adding an identity provider as an application source streamlines the process of adding individual applications from that provider to the end-user catalog.

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

When you add applications, you can entitle users and groups to the application and apply an access policy to control user access to the application. Users can access these applications in the Intelligent Hub portal or app.

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

Sometimes third-party identity providers send an authentication request without including which application a user is trying to access. If Workspace ONE Access receives an authentication request that does not include the application information, the backup access policy rules configured in the application source are applied instead of the rule set for the individual application.

The following identity providers can be configured as application sources in Workspace ONE Access.

- Okta
- Ping Federated server from Ping Identity
- Active Directory Federation Services (ADFS)

This chapter includes the following topics:

- [Add an Application Source to Workspace ONE Access Catalog](#)
- [Entitle Users to the Application Source in Workspace ONE Access](#)
- [Add Applications Managed by the Application Source to Workspace ONE Access](#)

Add an Application Source to Workspace ONE Access Catalog

Configure the application source in the Workspace ONE Access Catalog > Settings page to integrate third-party applications with the Workspace ONE Access catalog. After the application source is configured, you can add applications from the source to the Workspace ONE Access catalog.

The common configuration settings are set at the application source level. Applications from the application source that you add to the Workspace ONE Access catalog use these configuration settings. Configuring the application source once makes it easy to add multiple applications to the catalog.

Procedure

- 1 Log in to the VMware Workspace ONE Access console.
- 2 Click the **Catalog > Web Apps** tab and click **Settings**.
- 3 Select **Application Sources**.
- 4 Select the type of application source to configure.
- 5 Enter a descriptive name for the application source and click **Next**.
- 6 Modify the application source configuration.

Option	Description
Configuration	Select URL/XML to use auto-discovery URL or meta-data XML or select Manual . <ul style="list-style-type: none"> ■ Auto-discovery (meta-data) URL: If the XML metadata is accessible on the Internet, provide the URL. ■ Meta-data XML: If the XML metadata is not accessible on the Internet, but is available to you, paste the Meta-data XML in the text box. ■ Manual configuration: If the XML metadata is not available to you, manually configure the XML in the text boxes that are displayed.
Relay State URL	Enter a custom landing page that users are sent to by Workspace ONE after authenticating to the single sign-on URL.
Advanced Configuration Options	
Sign Response	Enabled. The entire response is signed.
Sign Assertion	Enable to sign the assertion.
Encrypt Assertion	If enabled, the SAML assertion is encrypted. For encryption to work, the ability to read encrypted SAML assertions must be supported.
Include Assertion Signature	Enable to include the Workspace ONE signing certificate inside the SAML response. Your application service provider might require this the signing certificate included with the SAML response.
Signature Algorithm	Select SHA256 with RSA as the secure encrypted hash algorithm to use for the signature.

Option	Description
Digest Algorithm	Select SHA256.
Application Login URL	Enter the application service provider's login page URL to trigger a service provider initiated log in to Workspace ONE. Some application service providers do not support single sign-on assertions sent directly from Workspace ONE and instead require that the login process start at their own login page.
Enable Authentication Failure Notification	If enabled, a SAML failure response is sent to the service provider when a login attempt fails.
Proxy Count	Set the proxy count to limit the number of proxy layers between the service provider and the authenticating identity provider.
API Access	Allow API access to this application.

- 7 Click **Next**.
- 8 Select the access policy. Either verify that the default access policy meets the requirements for this application or select another access policy from the drop-down menu.

Results

The application source is configured.

What to do next

Add the associated applications to the catalog.

Entitle Users to the Application Source in Workspace ONE Access

After you configure an application source in Workspace ONE Access, set the entitlements for the application source to All Users. You can manage the entitlements from the specific application configuration pages.

Procedure

- 1 In the Workspace ONE Access console, in the **Catalog > Web Apps** page, select the application source from the list.
- 2 Click **Assign**.
- 3 Type **ALL USERS** in the search box to find and select the ALL USERS group.
- 4 Click **Save**.

Results

All users can access the application source managed applications. You can manage the entitlements from the specific application entitlements page.

What to do next

The access policy is automatically set to the default access policy. Verify that this is the correct access policy to use.

Add the individual applications from the application source.

Add Applications Managed by the Application Source to Workspace ONE Access

After the identity provider is configured as an application source, you can add web applications that use the SAML 2.0 authentication profile to the Workspace ONE Access catalog.

Prerequisites

Third-party identity provider configured as an application source in the Catalog > Settings page.

Procedure

- 1 Log in to the Workspace ONE Access console.
- 2 Click the **Catalog > Web Apps** tab.
- 3 Click **New**
- 4 Complete the information on the Definition page, and click **Next**.

Form Item	Description
Name	Enter the name of the application.
Description	(Optional) Add a description of the application.
Icon	(Optional) To add an icon that displays in the users Workspace ONE application page, click Choose File to upload an icon. PNG, JPG, and ICON file formats, up to 4 MB, are supported. Uploaded icons are resized to 80px X 80px. To prevent distortion, upload icons where the height and width are equal to each other and as close as possible to the 80px X 80px resize dimensions.

- 5 In the Configuration page, **Authentication Type** drop-down menu select the application source for this application. Enter the target URL for the application.

This URL is either the identity provider URL for the application as represented in the application source or the service provider URL.

The configuration is populated with the application source configuration values.

- 6 On the **Access Policies** page, either verify that the default access policy meets the requirements for this application or select another access policy from the drop-down menu.

See "Managing Access Policies" in the *Workspace ONE Access Administration* guide for more information.

Results

The application is added to the Workspace ONE Access catalog and users can access the application from the Workspace ONE Intelligent Hub app or portal.

What to do next

If users are assigned to the application source, they are automatically assigned to the application. You can change the users and groups that are assigned to the application.

Troubleshooting Workspace ONE Access Resource Configuration

10

Use this information to troubleshoot issues that you or your end users experience after you integrate Web apps, Horizon desktops and apps, Horizon Cloud desktops and apps, Citrix-published resources, or ThinApp packages with Workspace ONE Access.

This chapter includes the following topics:

- [Troubleshooting Launch Errors in Workspace ONE Access](#)
- [Troubleshooting ThinApp Integration with Workspace ONE Access](#)
- [Troubleshooting VMware Horizon Integration with Workspace ONE Access](#)
- [Troubleshooting Citrix-Published Resources Integration with Workspace ONE Access](#)

Troubleshooting Launch Errors in Workspace ONE Access

You can troubleshoot Horizon, Horizon Cloud, and Citrix resource launch failures by viewing error messages about the root cause and suggested solutions in the Workspace ONE Access console.

Procedure

- 1 In the Workspace ONE Access console, select the **Dashboard > Reports** tab.
- 2 Select **Audit Events** from the list of reports.
- 3 Set the Type as **LAUNCH** or **LAUNCH_ERROR**.
- 4 Select a time frame and click **Show**.

Troubleshooting ThinApp Integration with Workspace ONE Access

Use this information to troubleshoot the ThinApp configuration in Workspace ONE Access.

ThinApp Packages Fail to Launch from the User Portal

When a user tries to launch a ThinApp package from the user portal, a browser message might appear that prompts the user to download and install the Workspace ONE Access Desktop application even when the application is already installed and running.

Problem

After installing the Workspace ONE Access Desktop application, when the user opens the user portal in a browser on that Windows system, logs in, and tries to launch a ThinApp package, a message might appear stating that the Workspace ONE Access Desktop application must be installed on the system, and prevents the ThinApp package from starting. This message might appear even when the Workspace ONE Access Desktop application process is running on the Windows system. The Workspace ONE Access Desktop application might report that all files are up to date.

Cause

This problem can occur for multiple reasons.

Cause	Description
<p>The Workspace ONE Access Desktop browser plugin is not properly installed or it is not activated in the browser window for the browser in which the user is trying to launch the ThinApp package.</p>	<p>Because installation of the Workspace ONE Access Desktop application is required to run ThinApp packages on the Windows system, the user portal uses a browser plugin to verify whether the application is installed before launching the ThinApp package from the user portal. When the user clicks the icon for a ThinApp package in the user portal, the Workspace ONE Access Desktop browser plugin checks to see if the application is installed before launching the package. If the browser plugin is not installed and active in the browser, the verification cannot happen, the message appears, and the package does not launch.</p> <p>If there are browser windows open during the Workspace ONE Access Desktop installation process, the browser plugin might not be properly installed for that browser. The browser plugin might become deactivated in the browser if the user deselected the plugin in the browser's add-ons or plug-ins page.</p>
<p>The custom protocol handler used to launch the ThinApp package from the browser has been deactivated for the browser in which the user is trying to launch the ThinApp package.</p>	<p>In the user portal, ThinApp packages are represented using a link with a <code>horizon://</code> protocol. When the Workspace ONE Access Desktop application is installed, the installer registers a protocol handler for that <code>horizon://</code> protocol. The protocol handler is an executable named <code>HorizonThinAppLauncher.exe</code>, and is registered as a handler by the registry entry <code>HKEY_CLASSES_ROOT\horizon\shell\open\command</code>. When the user tries to launch a ThinApp package from its icon in the user portal, this <code>HorizonThinAppLauncher.exe</code> application is launched.</p> <p>If the user has deactivated the use of all protocol handlers in the browser, or deactivated the use of the handler for the <code>horizon://</code> protocol, ThinApp packages will not launch using their icons in the user portal. Some browsers present a warning when protocol handlers are launched and give the user the option to select to execute the protocol handler. One way in which the user might have deactivated the use of the <code>horizon://</code> protocol handler is when the user clicked one of the ThinApp package icons for the first time, when the browser warning dialog appeared to ask for permission to run the protocol handler, the user selected No or a similar choice to prevent the launch, and also selected Remember my selection or a similar choice that prevents the launch for all such links. Because permission to run the protocol handler was not given and is remembered, none of the ThinApp packages launch from the user portal.</p>

Solution

- 1 Verify the user has logged in to the Workspace ONE Access Desktop application with their user account.

The user signs into the client using the Workspace ONE Access icon in the Windows system tray.

- 2 If this problem appears shortly after the application is installed on the system, close all open browser windows, reopen the browser, log in to the user portal, and try launching the ThinApp package.
- 3 If the problem appears even after closing the open browser windows and reopening the browser, verify the browser plugin appears in the browser's list of plugins and is active.

Browser	Description
Internet Explorer	<p>For Internet Explorer, a COM server is registered instead of a browser plugin or add-on. To test whether the COM server is installed, create a test HTML file with the following contents and open that file in Internet Explorer. The result tells whether the COM server is installed or not.</p> <pre><html> <script type="text/vbscript"> On Error Resume Next dim objName objName = "HorizonAgentFinder.HorizonFinder" dim obj Set obj = CreateObject(objName) document.write(objName & " is ") if IsEmpty(obj) then document.write("not installed") else document.write("installed") end if </script> </html></pre>
Firefox	<p>Open Firefox's Add-ons Manager by clicking Tools > Add-ons. On the Plugins page, verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate.</p>
Chrome	<p>In the browser settings, verify that the VMware Horizon Agent Finder browser plugin is listed and set it to always activate.</p>
Safari for Windows	<p>In the browser settings, verify that the VMware Horizon Agent Finder browser plugin is listed and is activated for Safari.</p>

- 4 Verify the registry entry `HKEY_CLASSES_ROOT\horizon\shell\open\command` exists and has a value that is a path that points to the location of the required protocol handler, named `HorizonThinAppLauncher.exe`, where the Workspace ONE Access Desktop application was installed on the Windows system.

If the registry entry does not exist, or does not have a value that points to the location where the Workspace ONE Access Desktop application was installed, uninstall the application and reinstall it.

- 5 If the registry entry exists and has a value that points to the location of the `HorizonThinAppLauncher.exe` executable, verify the executable exists at that location and has not been moved or deleted.

If the registry entry does not exist, or does not have a value that points to the location where the Workspace ONE Access Desktop application was installed, uninstall the application and reinstall it.

- 6 If the registry entry exists and has a value that points to the location of the HorizonThinAppLauncher.exe executable, verify that the (Default) value for the registry entry HKEY_CLASSES_ROOT\horizon has a Data value of URL:horizon Protocol and that the URL Protocol value for the HKEY_CLASSES_ROOT\horizon entry exists.

If the Data value for the (Default) value of the HKEY_CLASSES_ROOT\horizon registry entry is not set to URL:horizon Protocol, update the Data value to set it to URL:horizon Protocol. If the URL Protocol value does not exist for the HKEY_CLASSES_ROOT\horizon entry, you can create it using a value name URL Protocol and no value data.

- 7 Determine if the user deactivated the horizon:// protocol for the browser, or if all protocol handlers are deactivated in the browser, and if so, enable the protocol handler for the browser as appropriate for your organization's needs.

In most situations, the browsers rely on the settings in the registry for information about the protocol handlers available for that Windows system. For some browsers, when the user clicks a link that is associated with a protocol handler, a dialog prompt appears that asks the user a question such as *Do you want to allow this website to open a program on your computer? Or This link needs to be opened with an application or a similar statement* about needing to launch an external application to handle the link. Typically, the dialog provides the user with the option of not launching the external application and to remember that choice for all links of that type. The steps to re-enable the ability to launch the application associated with the protocol handler are usually different depending on the browser type. Consult the documentation for the user's type of browser on how to enable protocol handlers for that browser type.

Troubleshooting VMware Horizon Integration with Workspace ONE Access

Use this information to troubleshoot the VMware Horizon configuration in Workspace ONE Access.

Users Unable to Launch Horizon Applications or Desktops

Users are unable to launch Horizon applications or desktops from the Workspace ONE Access Intelligent Hub app or portal and the following error appears in the user interface:.

```
Error launching resource. Please contact your IT Administrator.
```

This error might occur if the SAML metadata on the Horizon Connection Server instances expired after the last sync. This error might also occur if you added or updated network ranges or policies.

Solution

- 1 In the Workspace ONE Access console, select the **Catalog > Virtual Apps Collections** tab.

- 2 Select the Horizon virtual apps collection and click **Sync > Sync with safeguards** or **Sync > Sync without safeguards** to sync Horizon resources to VMware Workspace ONE Access again.
- 3 Click **Edit** to edit the virtual apps collection, click **Next** in the wizard until the last page appears, then click **Save**.

Important This step is important if you added or updated network ranges or policies. You must save the virtual apps collection again for the changes to take effect.

Horizon Virtual Apps Collection Certificate Error

With Workspace ONE Access connector 21.08, when you try to add a Horizon pod or sync the Horizon virtual apps collection in the Workspace ONE Access console, you might get the following error: `Enterprise service <connectorFQDN>(EIS) response: Unable to get certificate from the URL: <https://FQDN/SAML/metadata/sp.xml>`.

Solution: Ensure that the Horizon Connection Servers have valid certificates signed by a trusted Certificate Authority (CA). If the Horizon Connection servers have self-signed certificates, you must upload the certificate chain to the Workspace ONE Access connector instances on which the Virtual App service is installed to establish trust between the connectors and the Horizon Connection servers. This is a new requirement in Workspace ONE Access connector 21.08. You upload the certificates using the connector installer. See [Installing VMware Workspace ONE Access Connector](#) for more information.

Troubleshooting Citrix-Published Resources Integration with Workspace ONE Access

Use this information to troubleshoot the Citrix-published resources configuration in Workspace ONE Access.

See also *Troubleshooting Citrix-Published Resources Configuration in VMware Identity Manager*.

Resource Not Available Error while Launching XenApp 7.x Desktops

Users are unable to launch a XenApp 7.x desktop. A `Resource not available` error appears.

Problem

While launching a desktop from a XenApp 7.x delivery group, users get a `Resource not available` error.

Cause

Machine catalogs created using the Citrix Machine Creation server have power management switched on by default. This results in the machine being shut down after logging off.

Solution

- 1 Turn off the power management option for the delivery group in the Citrix XenApp 7.x server.
- 2 Sync the Citrix-published resources to the VMware Workspace ONE Access service again.

Unable to Launch Desktop from Citrix XenDesktop Farm on Windows 7

On Windows 7, users are unable to launch desktops from a Citrix XenDesktop farm when SSL is enabled.

Problem

If SSL is enabled, when users launch a desktop on Windows 7, sometimes the desktop does not start and displays the following error: "The connection to *desktop* failed with status 1030." This problem has been observed intermittently on Firefox but may also occur on other browsers.

Solution

See the Citrix Knowledge Center article, [Troubleshooting 1030 Error on Windows 7 Image](#), for more information about this problem.

Sync Issues if Published Applications or Desktops in a Site Do Not Contain Valid Users

If a Citrix-published application or desktop does not contain valid users, sync to Workspace ONE Access does not work.

Problem

All Citrix-published applications and desktops in a Site must contain valid users. If a user or group is deleted and that user or group is not removed from a Citrix-published resource, the Citrix application or desktop shows an orphaned SID. This prevents the sync to Workspace ONE Access from working.

Cause

Some published applications or desktops in the Site do not contain valid users.

Solution

Ensure that all Citrix-published applications and desktops within a Site contain valid users.

Citrix Entitlements do not Appear in Workspace ONE Access

Citrix entitlements do not appear in Workspace ONE Access.

Problem

Entitlements to an application or delivery group are set on the Citrix server but they do not appear in Workspace ONE Access.

Cause

Users and groups that are entitled to the application or delivery group may not be synced to Workspace ONE Access.

Solution

Ensure that the users and groups are synced to Workspace ONE Access.

- 1 Log in to the Citrix Management Console and locate the application that does not have any entitlements.
- 2 Make a note of the Active Directory users and groups that have permissions to launch the application in the Citrix Management Console.
- 3 Log in to the Workspace ONE Access console, click the **Users & Groups** tab, and verify that the users and groups appear in the list.

You can also use the search box in the top right of the page.

- 4 If the users and groups appear, sync Citrix resources again from the **Catalog > Virtual Apps Collections** page.

Note The users and groups must exist in Workspace ONE Access before you sync Citrix resources. If they do not exist, the sync runs but entitlements are not updated.

- 5 If the users and groups do not exist in Workspace ONE Access, perform these actions.
 - a Check where the users and groups exist in Active Directory (using Active Directory Users and Computers Snap-in).
 - b In the Workspace ONE Access console, update the AD Sync DNs for the users and groups in the directory's **Sync Settings** pages.
 - c When the users and groups appear in the Workspace ONE Access console, sync Citrix resources again.

When sync completes, the entitlements appear in Workspace ONE Access.

Citrix Delivery Groups Not Synced to Workspace ONE Access

If Citrix delivery groups are not syncing to Workspace ONE Access, check the settings in the Citrix server farm. A delivery group's Delivery Type setting in Citrix determines how Workspace ONE Access syncs the delivery group.

Workspace ONE Access syncs a delivery group only if its Delivery Type is set to Desktops And Apps or Desktops Only. If the delivery group's Delivery Type is set to Apps Only, its applications are synced but the delivery group itself is not synced and does not appear in the Workspace ONE Access catalog.

Configure your delivery groups accordingly.