

# Setting Up Resources in VMware Identity Manager 19.03 (On Premises)

Modified JUN 2021

APR 2019

VMware Workspace ONE Access 19.03

VMware Identity Manager 1903

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](http://www.vmware.com)

Copyright © 2013-2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

Setting Up Resources in VMware Identity Manager (On Premises)	7
<b>1 Introduction to Setting Up Resources in VMware Identity Manager</b>	<b>8</b>
<b>2 Providing Access to Web Applications</b>	<b>10</b>
Adding a Web Application to Your Catalog	12
Assigning Users and Groups to a Web Application	15
Editing a Web Application	17
Copying a Web Application	17
Exporting a Web Application	18
Importing a Web Application	18
Deleting a Web Application from the Catalog	19
Creating and Selecting Categories for Applications	19
Adding Multiple Tenants of Web Apps	20
Adding OpenID Connect Applications to the Catalog	21
Add an OpenID Connect Application	22
Using Provisioning Adapters	24
Managing Web Apps Settings	25
Additional Information	25
<b>3 Using Virtual Apps Collections for Desktop Integrations</b>	<b>26</b>
About Virtual Apps Collections	26
Migrating Existing Configurations to Virtual Apps Collections	28
Using the Migration Wizard to Migrate to Virtual Apps Collections	29
Creating Virtual Apps Collections	31
Editing Virtual Apps Collections	33
Syncing Virtual Apps Collections	34
Monitoring Virtual Apps Collections	35
Deleting Virtual Apps Collections	38
<b>4 Providing Access to Horizon 7 or Horizon 6 Desktop and Application Pools</b>	<b>40</b>
About Integrating Independent Horizon Pods	41
Requirements for Integrating Horizon Pods	42
About Integrating Horizon Cloud Pod Architecture (CPA) Deployments	42
Requirements for Integrating Horizon Pod Federations	46
Configuring Horizon Pods and Pod Federations in VMware Identity Manager	47
Set up Your VMware Identity Manager Environment	48
Configure Horizon Pods and Pod Federations in VMware Identity Manager	48

- Configure SAML Authentication in Horizon 54
- Setting Client Access FQDNs for Network Ranges 55
- Launching Horizon Resources Through Validating Gateways 57
- Viewing Horizon Desktop and Application Pool Information in VMware Identity Manager 58
- Viewing User and Group Assignments for Horizon Desktop and Application Pools 59
- Setting Access Policies for Specific Applications and Desktops 60
- Allowing Users to Reset Their Horizon Desktops from the Workspace ONE Catalog 61
- Viewing Launch Options for Horizon Desktops and Applications 62
- Launching a Horizon Desktop or Application 63

## 5 Providing Access to VMware Horizon Cloud Service Desktops and Applications 65

- Integrating Horizon Cloud Desktops and Applications 66
  - Integrating Multiple Horizon Cloud Instances 66
  - Prerequisites for Integration 67
  - Configure Horizon Cloud Tenant in VMware Identity Manager 68
  - Configure SAML Authentication in the Horizon Cloud Tenant 72
- Viewing Horizon Cloud Desktop and Application Pool Information in VMware Identity Manager 74
- Viewing User and Group Assignments for Horizon Cloud Desktops and Applications 74
- Setting Access Policies for Specific Applications and Desktops 75
- Allowing Users to Reset Horizon Cloud Desktops 76
- Running a Horizon Cloud Desktop or Application 76

## 6 Providing Access to VMware ThinApp Packages 78

- Integrating VMware ThinApp Packages 79
  - VMware Identity Manager Requirements for ThinApp Packages and the Network Share Repository 79
  - Create a Network Share for ThinApp Packages 85
  - Configuring VMware Identity Manager Access to ThinApp Packages 86
- Entitle Users and Groups to ThinApp Packages 89
- Distributing and Managing ThinApp Packages 91
  - Offline Grace Period and ThinApp Packages 95
- Updating Managed ThinApp Packages After Deployment in VMware Identity Manager 95
  - Update a Managed ThinApp Package 97
    - Obtain the AppID and VersionID values of a Managed ThinApp Package 97
    - Create the Updated ThinApp Package 98
    - Copy an Updated ThinApp Package to the Network Share 100
- Make Existing ThinApp Packages Compatible with VMware Identity Manager 101
- Change the ThinApp Packages Share Folder 104
- Setting Access Policies for Specific Applications and Desktops 105

## 7 Configuring VMware Identity Manager Desktop 106

- Command-Line Installer Options for VMware Identity Manager Desktop 107
- Install the Windows Application with Identical Settings to Multiple Systems 113
- Add VMware Identity Manager Desktop Installer Files to VMware Identity Manager Virtual Appliances 114
- Using the Command-Line hws-desktop-ctrl.exe Application 115

## 8 Providing Access to Citrix-Published Resources 117

- Overview of Citrix-Published Resources Integration 117
- Components Required for Citrix Integration 120
- High-level Integration Design 120
  - Synchronization of Citrix-published Resources and Entitlements 120
  - Launch of Citrix-published Applications and Desktops 121
- Prerequisites for Citrix Integration 126
  - About Deploying the Integration Broker 127
    - Integration Broker Deployment Models 129
  - Prepare Windows Server for the Integration Broker Installation 131
    - Add Windows Server Roles and Features (Windows Server 2012 R2, 2012, or 2008 R2) 132
    - Add Windows Server Roles and Features (Windows Server 2016) 135
    - Install Microsoft Visual J# 2.0 64-bit Redistributable Package 141
  - Deploy Integration Broker 141
    - Install Integration Broker 141
    - Configure IIS Manager Settings for the Integration Broker Component of VMware Identity Manager 142
    - Set HTTPS Site Binding for the Integration Broker 145
  - Enable Citrix PowerShell Remoting 149
    - Install Citrix PowerShell SDK on the Integration Broker Server 149
    - Enable Citrix PowerShell Remoting on the Citrix Server Farm 150
  - Enabling Integration Broker to Use TLS 1.2 152
  - Verify the Connection to the Citrix Server Farm 152
  - Download Citrix Web Interface SDK 5.4 153
- Configuring Citrix Server Farms in VMware Identity Manager 153
- Configuring Citrix Resource Launch in VMware Identity Manager 161
  - Configuring Resource Launch for Internal Networks 161
  - Configuring Resource Launch for External Networks with NetScaler Gateway 162
    - Obtain the STA Server URL for the NetScaler Gateway 163
    - Configure NetScaler Gateway in VMware Identity Manager 164
    - Configure Network Range for NetScaler Gateway 165
- Configuring VMware Identity Manager Settings for Citrix Integration 166
  - Managing Categories for Citrix-Published Resources 166
  - Configuring Delivery Settings (ICA Properties) for Citrix-Published Resources 167

- Editing ICA Properties for all Citrix-Published Resources 167
- Setting Access Policies for Specific Applications and Desktops 168
- Viewing User and Group Assignments for Citrix-Published Resources 169
- Launching Citrix-Published Resources in Different Browsers 170
- Upgrade Impact on Citrix-Published Resources Integration 171
  
- 9 Providing Access to Third-Party Managed Applications in Workspace ONE 172**
  - Add an Application Source to Workspace ONE Catalog 173
  - Entitle Users to the Application Source 174
  - Add Applications Managed by the Application Source 175
  
- 10 Troubleshooting VMware Identity Manager Resource Configuration 176**
  - Troubleshooting Launch Errors 176
  - Troubleshooting ThinApp Integration 176
    - ThinApp Packages Fail to Launch from the User Portal 176
  - Troubleshooting Horizon Integration 179
    - Users Unable to Launch Horizon Applications or Desktops 179
  - Troubleshooting Citrix-Published Resources Integration 180
    - Citrix-Published Resources Are Not Available in VMware Identity Manager 180
    - Unable to Launch Citrix Published Applications or Desktops 183
    - Users Accessing Citrix-Published Resources Receive an Encryption Error 184
    - When Users Launch a Citrix-Published Resource, the Browser Displays 500 Internal Server Error 185
    - Memory Issue Prevents Proper Configuration of Integration Broker 186
    - Resource Not Available Error while Launching XenApp 7.x Desktops 186
    - Unable to Launch Desktop from Citrix XenDesktop Farm on Windows 7 186
    - Launch of Citrix-published Resources Fails if XML Port is Set Incorrectly 187
    - Citrix Resource Sync Fails if Limited Visibility Group Does Not Contain Any Users or Groups 187
    - Sync Issues if Published Applications or Desktops in a Site Do Not Contain Valid Users 188
    - Citrix Entitlements do not Appear in VMware Identity Manager 188
    - Exception During Sync if Application Pool Identity is not Configured 189
    - ICA File is not Created During Citrix Resource Launch 190
    - Restarting Integration Broker 191

# Setting Up Resources in VMware Identity Manager (On Premises)

*Setting Up Resources in VMware Identity Manager* provides information about adding resources to the VMware Identity Manager catalog and making them available from users' systems, such as from their desktops and mobile devices. Supported resources include Web applications, VMware Horizon<sup>®</sup> desktops and applications, VMware Horizon<sup>®</sup> Cloud Service<sup>™</sup> desktops and applications, Citrix published resources, and VMware ThinApp<sup>®</sup> packages.

## Intended Audience

This information is intended for anyone who configures and administers resources for VMware Identity Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology.

# Introduction to Setting Up Resources in VMware Identity Manager

# 1

To provide users access to supported resources you must configure the resources in the VMware Identity Manager console. Except for Web applications, each resource type requires you to integrate VMware Identity Manager with another product or component.

You can integrate the following types of resources with VMware Identity Manager:

- Web apps
- Virtual apps
  - VMware Horizon<sup>®</sup> Cloud Service<sup>™</sup> applications and desktops
  - VMware Horizon<sup>®</sup> 7 and Horizon 6 desktop and application pools
  - Citrix-published resources
  - VMware ThinApp<sup>®</sup> packaged applications

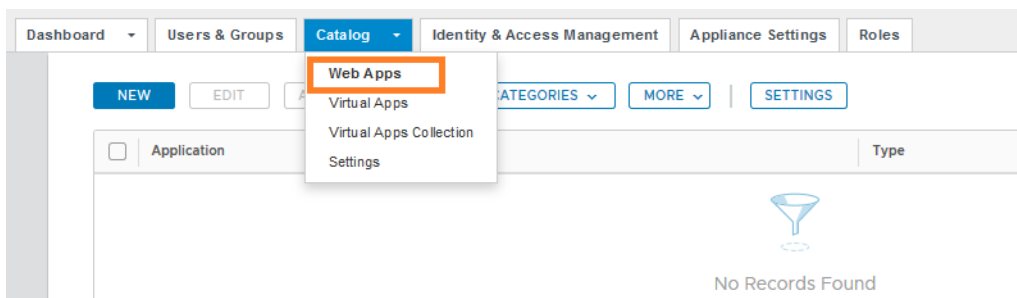
---

**Note** Integration with ThinApp packaged applications is only supported with the Linux VMware Identity Manager connector. It is not supported with the Windows connector.

---

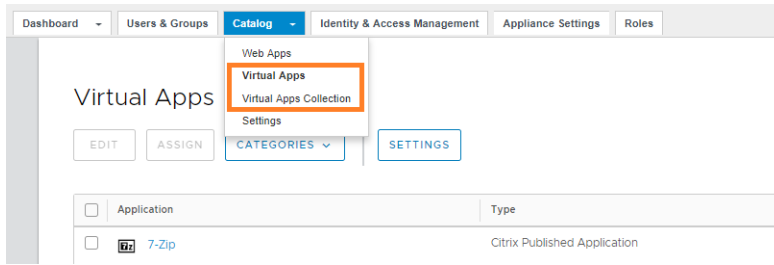
You integrate these resources from the **Catalog** tab in the VMware Identity Manager console.

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



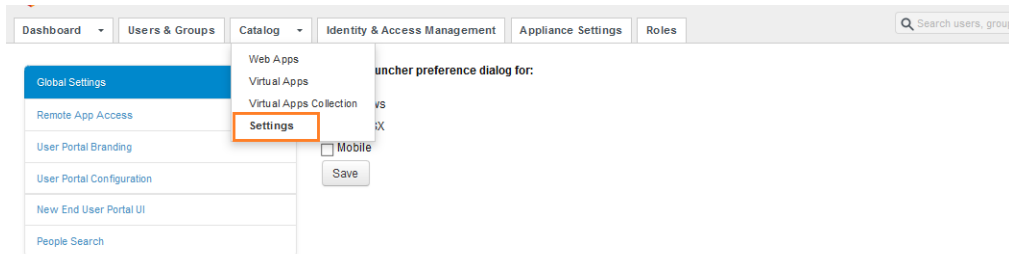
- To integrate and manage Horizon desktop and application pools, Horizon Cloud desktops and applications, Citrix-published resources, or ThinApp packaged applications, you use the **Catalog > Virtual Apps Collections** and **Catalog > Virtual Apps** tabs. You configure the integrations in the **Catalog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



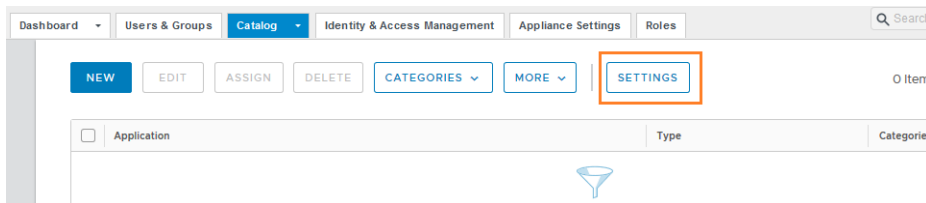


You can manage settings for integrated resources from the following pages.

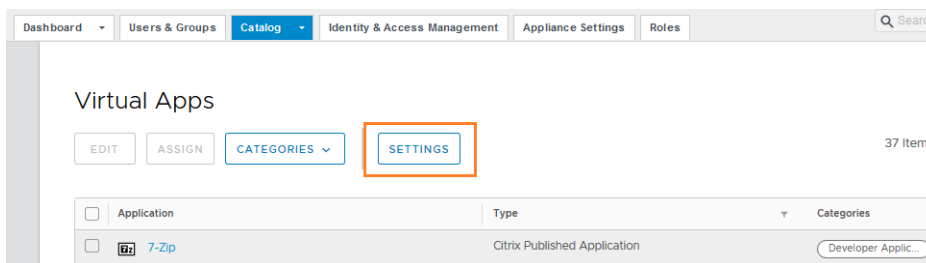
- Global settings are available on the **Catalog > Settings** tab.



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



- Settings for Horizon, Horizon Cloud, 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

## 2

You can add Web applications to the VMware Identity Manager catalog and assign them to users and groups to provide users access to these applications from the Workspace ONE portal or app. You enable 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 VMware Identity Manager. See

[Chapter 9 Providing Access to Third-Party Managed Applications in Workspace ONE](#) 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 VMware Identity Manager 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 Identity Manager Administration*.

This chapter includes the following topics:

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

## Adding a Web Application to Your Catalog

You can add Web applications to your catalog by either selecting them from the cloud application catalog or creating new ones.

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 VMware Identity Manager 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 *VMware Identity Manager 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 user groups, if required. You can create groups from the **Users & Groups > Groups** tab.

### Procedure

- 1 In the VMware Identity Manager 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
<b>Name</b>	Enter a unique name for the application.
<b>Description</b>	(Optional) Enter a description of the application.
<b>Icon</b>	(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.
<b>Category</b>	(Optional) To add the application to a category, select it from the drop-down menu. Categories must already be created.  A predefined <b>Recommended</b> category is available. Select it if you want the application to appear in the Recommended page in Workspace ONE. If you want the app to appear in the users' Bookmarks page, select the <b>Recommended</b> category and in the <b>Catalog &gt; Settings &gt; User Portal Configuration</b> page, select <b>Show recommended apps in Bookmarks</b> 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
<p><b>Single Sign-On</b></p>	<p><b>Authentication Type</b></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"> <li>■ SAML 2.0                     <p>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 to the application.</p> </li> <li>■ SAML 1.1                     <p>If the Web application supports SAML 1.1, select this option to enable single sign-on from Workspace ONE to the application.</p> </li> <li>■ WSFed 1.2 (Supported for Office 365 only)                     <p>Do not select the WSFed 1.2 option while creating a new Web application.</p> <p>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.</p> </li> <li>■ OpenID Connect                     <p>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 to the application.</p> </li> <li>■ Any third-party identity providers configured as application sources in VMware Identity Manager, for example, Okta.                     <p>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.</p> </li> <li>■ Web Application Link                     <p>Select this option if the application does not use a federation protocol. You only need to enter the target URL of the application.</p> </li> </ul> <p><b>Configuration</b></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.</p>
<p><b>Application Parameters</b></p>	<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> <p><b>Note</b> This section does not appear when OpenID Connect, an application source, or Web Application Link is selected as the authentication type.</p>
<b>Advanced Properties</b>	<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> <p><b>Note</b> This section does not appear when OpenID Connect, an application source, or Web Application Link is selected as the authentication type.</p>
<b>Open in VMware Browser</b>	<p>Select this option if you want the Workspace ONE 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 Catalog page in Workspace ONE. Users can run the application from the Catalog page or bookmark it and run it from the Bookmarks page. 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

After you add Web applications to your catalog, you can assign them to users and groups.

When you entitle a user to a Web application, the user can view and launch the application from the Workspace ONE portal or app. If you remove the user's entitlement, 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.

### Prerequisites

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

### Procedure

- 1 Log in to the VMware Identity Manager console.
- 2 Entitle users to a Web application.

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

### Results

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



## Editing a Web Application

You can edit any Web applications that you added to your VMware Identity Manager catalog. You can change the application definition, configuration, access policy, and user assignments.

### Procedure

- 1 In the VMware Identity Manager 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 Catalog](#).

## Copying a Web Application

You can make a copy of a Web application in your 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 VMware Identity Manager 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 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 appears in the Catalog page in Workspace ONE. Users can run the application from the Catalog page or bookmark it and run it from the Bookmarks page. If you plan to set up an approval flow for the application, select **User Activated**.
  - c Click **Save**.

## Exporting a Web Application

You can export and import a Web application from one VMware Identity Manager instance to another. For example, you might want to import an application from your staging environment into your production environment.

This process involves exporting the application bundle from one instance and importing it into the other. The application might not require further configuration, especially if you thoroughly tested it in the original environment.

### Procedure

- 1 Log in to the console of the VMware Identity Manager 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.

### What to do next

Import the application bundle into the VMware Identity Manager instance in which you want to use it.

## Importing a Web Application

You can export and import a Web application from one VMware Identity Manager instance to another. For example, you might want to import an application from your staging environment into your production environment.

### Prerequisites

You have exported the application from another VMware Identity Manager instance.

### Procedure

- 1 Log in to the console of the VMware Identity Manager instance in which to import a Web application.
- 2 Select the **Catalog > Web Apps** tab.
- 3 Click **More > Import**.
- 4 Select the application zip file and click **Open**.

The application is uploaded.

## Deleting a Web Application from the Catalog

You can delete Web applications from the VMware Identity Manager 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 Workspace ONE.

### Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Web Apps** tab.
- 2 Click the application you want to delete.
- 3 Click **Delete**.

## Creating and Selecting Categories for Applications

You can group Web applications into categories to make it easier to find applications. 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 page in Workspace ONE. 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 VMware Identity Manager 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

VMware Identity Manager supports adding multiple tenants of a service provider to a VMware Identity Manager instance. If you have multiple tenants of an app such as Office 365 that may be used by different lines of business in your organization, you can add all the tenants to a single instance of VMware Identity Manager. 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 VMware Identity Manager 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 Workspace ONE 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 VMware Identity Manager for authentication and VMware Identity Manager authenticates the user and launches the correct app based on user entitlements.

### Procedure

- 1 In the VMware Identity Manager 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 VMware Identity Manager 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 Catalog page in Workspace ONE. Users can run the application from the Catalog page or move it to the Bookmarks 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 the Catalog

You can add applications that use the OpenID Connect authentication protocol to VMware Identity Manager 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 VMware Identity Manager 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 from the **Clients** tab on the **Catalog > Settings > Remote App Access** page. Click the client name to view the configuration information. Do not edit any fields in the client.

---

**Important** 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 VMware Identity Manager redirects the user to the target URL.
- 3 The application redirects the user to VMware Identity Manager with an authorization request.
- 4 VMware Identity Manager authenticates the user based on the authentication policy that you specified for the application.
- 5 VMware Identity Manager checks whether the user is entitled to the application.
- 6 VMware Identity Manager sends the authorization code to the redirect URL.
- 7 Using the authorization code, the application requests the access token.
- 8 VMware Identity Manager 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 VMware Identity Manager for authentication.
- 3 VMware Identity Manager authenticates the user based on the authentication policy that you specified for the application.
- 4 VMware Identity Manager checks whether the user is entitled to the application.
- 5 VMware Identity Manager sends an ID token to the service provider.

## Add an OpenID Connect Application

You add OpenID Connect applications to the VMware Identity Manager catalog from the **Catalog > Web Apps** tab.

## 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 VMware Identity Manager 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
<b>Name</b>	Enter a unique name for the application.
<b>Description</b>	(Optional) Enter a description of the application.
<b>Icon</b>	(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.
<b>Category</b>	(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 it if you want the application to appear in the Recommended page in Workspace ONE. 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
<b>Authentication Type</b>	Select OpenID Connect.
<b>Target URL</b>	The application URL to which users will be sent when they click the app in Workspace ONE.
<b>Redirect URL</b>	The URL to which VMware Identity Manager will send the authorization code.
<b>Client ID</b>	The Client Identifier that the app will include in the authentication requests made to VMware Identity Manager. The Client ID must be unique per tenant.

Option	Description
<b>Client Secret</b>	The secret that the app will use to identify itself in the authentication requests made to VMware Identity Manager.
<b>Open in VMware Browser</b>	Select this option if you want the Workspace ONE 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 *VMware Identity Manager 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 Catalog page in Workspace ONE. Users can run the application from the Catalog page or bookmark it and run it from the Bookmarks page. If you plan to set up an approval flow for the application, select **User Activated**.

10 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

Provisioning provides automatic application user management from a single location.

Provisioning adapters allow Web applications to retrieve specific information from the VMware Identity Manager 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 VMware Identity Manager service.

If provisioning is enabled for a Web application, when you entitle a user to the application in the VMware Identity Manager 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 VMware Identity Manager service currently includes provisioning adapters for the following applications:

- Google Apps
- Office 365
- Socialcast

## Managing Web Apps Settings

Settings for Web applications are available from the **Settings** button on the **Catalog > Web Apps** page in the VMware Identity Manager console.

From the **Settings** page, you can enable an approval flow for applications, configure third-party identity providers as application sources, and manage SAML metadata.

Setting	Description
<b>Approvals</b>	<p>When approvals are enabled, users need to request access to applications before they can use the applications from the Workspace ONE catalog.</p> <p>For information about setting up approvals, see <i>VMware Identity Manager Administration</i>.</p>
<b>SAML Metadata</b>	<p>You can download the self-signed VMware Identity Manager SAML signing certificate and SAML metadata from the <b>Download SAML Metadata</b> 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 <b>Generate CSR</b> 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>VMware Identity Manager Administration</i>.</p>
<b>Application Sources</b>	<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 <a href="#">Chapter 9 Providing Access to Third-Party Managed Applications in Workspace ONE</a>.</p>

## Additional Information

Additional information is available on configuring SAML-based single sign-on to specific Web applications, such as Office 365 and Google Apps. Information on provisioning adapters is included, if applicable.

See the [VMware Identity Manager Integrations Documentation](#) site.

# Using Virtual Apps Collections for Desktop Integrations

## 3

In addition to Web applications, you can integrate Horizon desktops and applications, Horizon Cloud desktops and applications, Citrix published applications and desktops, and ThinApp packaged applications with VMware Identity Manager. These resources are called Virtual Apps in the VMware Identity Manager interface and are managed through the Virtual Apps Collections feature.

This chapter includes the following topics:

- [About Virtual Apps Collections](#)
- [Migrating Existing Configurations to Virtual Apps Collections](#)
- [Creating Virtual Apps Collections](#)
- [Editing Virtual Apps Collections](#)
- [Syncing Virtual Apps Collections](#)
- [Monitoring Virtual Apps Collections](#)
- [Deleting Virtual Apps Collections](#)

## About Virtual Apps Collections

You can integrate Horizon desktops and applications, Horizon Cloud desktops and applications, Citrix published resources, and ThinApp packaged applications with the VMware Identity Manager service. These resources are managed through virtual apps collections.

A virtual apps collection contains the configuration information for an integration, including the type of resource, the servers from which to sync resources, the connector 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 50 Citrix XenApp farms, you can set up 10 virtual apps collections in VMware Identity Manager, with five farms in each collection. This allows for easier management of the configuration and faster sync as each collection is synced separately.

You can also use different connectors for each collection to distribute the sync load.

The Virtual Apps Collections page, accessed by navigating to **Catalog > Virtual Apps Collections** in the VMware Identity Manager 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.

## Collections



	Name	Source Type	Sync Frequency	Sync Status		Last Attempt Sync
<input type="radio"/>	<a href="#">Horizon Cloud</a>	Horizon Cloud	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:23:16 AM
<input type="radio"/>	<a href="#">Horizon View On-Premises</a>	Horizon	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:24:38 AM
<input type="radio"/>	<a href="#">Citrix</a>	Citrix	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 8:23:42 AM
1 - 3 of 3 item(s)						

**Note** Integration with ThinApp packaged applications is only supported with the Linux VMware Identity Manager connector. It is not supported with the Windows connector.

## 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:

- All instances of the VMware Identity Manager service must be version 3.1 or later.
- All connectors used to sync resources must be version 2017.12.1.0 or later.

- Role requirements
  - The Super Admin role is required to access the Virtual Apps Collections page initially.
    - 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.
    - For installations that are upgraded from an earlier release, the Super Admin role is required to migrate existing resource configurations to virtual apps collections.
    - For installations that are upgraded from an earlier release but do not have any resources configured, the Super Admin role is required to access the Virtual Apps Collections page initially. This scenario is similar to the new installation scenario.
  - 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, Horizon Cloud, and Citrix-published virtual apps collections)
    - Manage ThinApps (to create, edit, or delete ThinApps collections)
  - The Super Admin role is required to save the Network Ranges page for Horizon and Citrix collections. The Network Ranges page is used to specify Client Access FQDNs to direct user requests to the appropriate servers.

## Migrating from Earlier Releases

The Virtual Apps Collection feature was introduced in VMware Identity Manager 3.1.

With virtual apps collections, resource configurations are stored in the VMware Identity Manager service instead of the connector. They are managed from the **Catalog > Virtual Apps Collections** page instead of the **Catalog > Application Catalog > Manage Desktop Applications > ResourceType** pages.

In new installations, the Virtual Apps Collections page is automatically enabled. To integrate Horizon, Horizon Cloud, Citrix, or ThinApp resources, create new collections.

For upgrade from earlier releases, a migration path is available for maintaining your existing resource integrations. See [Migrating Existing Configurations to Virtual Apps Collections](#) for information.

## Migrating Existing Configurations to Virtual Apps Collections

The Virtual Apps Collections feature was introduced in VMware Identity Manager 3.1. With virtual apps collections, resource configurations are stored in the VMware Identity Manager service instead of the connector. They are managed from the **Catalog > Virtual Apps Collections** page instead of the **Catalog > Catalog Applications > Manage Desktop Applications > ResourceType** pages.

The old Manage Desktop Applications user interface is no longer supported. You must migrate any existing resource integrations to virtual apps collections, if you have not already done so.

In VMware Identity Manager 19.03, you can get started with virtual apps collections directly or follow a migration path, depending on your installation scenario.

- In new installations, you can create new virtual apps collections for Horizon, Horizon Cloud, Citrix, or ThinApp resources directly. Select the **Catalog > Virtual Apps Collections** tab. Review the information on the page and click **Get Started**. Select the type of resource you want to integrate and follow the wizard to create a new virtual apps collection.
- If you upgrade to VMware Identity Manager 19.03 and all your connectors are version 2017.12.1.0 or later, you must migrate any existing configurations that were still being managed through the Manage Desktop Applications user interface to virtual apps collections. Select the **Catalog > Virtual Apps Collections** tab. Review the information on the page and click **Get Started** to use the Migration wizard. See [Using the Migration Wizard to Migrate to Virtual Apps Collections](#).

After you migrate the existing configurations, the new Virtual Apps Collections page is enabled, allowing you to view and edit the migrated configurations and create new ones. To access the page at any time, select the **Catalog > Virtual Apps Collections** tab.

- If you are upgrading from an earlier release and you have at least one connector that is older than version 2017.12.1.0, you cannot create new virtual apps collections. Upgrade all connectors to 2017.12.1.0 or later, then use the Migration wizard to migrate your existing configurations to virtual apps collections.

---

### Important

- To create new virtual apps collections or to migrate existing configurations to virtual apps collections, all instances of the VMware Identity Manager service must be version 3.1 or later and all connectors must be version 2017.12.1.0 or later.
- The Super Admin role is required to access the Virtual Apps Collections page initially and to migrate existing resources. See [About Virtual Apps Collections](#) for more information.

---

## Using the Migration Wizard to Migrate to Virtual Apps Collections

Use the Migration wizard to migrate existing resource configurations from the Manage Desktop Applications user interface available in previous releases to virtual apps collections.

---

**Important** You must migrate all existing resource configurations at the same time. For example, if you have Horizon Cloud and Citrix resources configured, select both in the Migration wizard. The Migration wizard is intended to be used only once to migrate all the resources at the same time. After it is run once, it will no longer be available.

---

**Note** In a hosted environment, the migration process might take some time.

---

## Prerequisites

- Upgrade all VMware Identity Manager service instances to version 3.1 or later and all connector instances to version 2017.12.1.0 or later.
- The Super Admin role is required for initial access to the Virtual Apps Collections page and for performing the migration. See [About Virtual Apps Collections](#) for more information.

## Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Review the information and click **Get Started**.

The Migration wizard appears and displays all existing resource configurations. Note that the Migration wizard appears only if your old installation had resources configured.

- 3 In the Migration wizard, for each resource type, select the connector worker that was used for the configuration in the old installation.

The screenshot shows a web interface for migrating configurations. The title is "Migrating Existing Configurations to Virtual Apps Collection". Below the title is the instruction "Select the connectors from which to migrate configurations." There are three rows, each with a resource type label and a dropdown menu: "Horizon", "Citrix Published Application", and "Horizon Cloud". At the bottom left of the form is a blue button labeled "MIGRATE".

The drop-down menu for each resource type lists only the connectors that had that resource configured.

If the resource was configured on multiple connectors for high availability, all the connectors appear in the list. The **Syncing Automatically** or **Syncing Manually** label indicates whether a sync schedule was set for the resource on that connector or whether it was set to manual sync. Select the connector that has the **Syncing Automatically** label. This is also the default selection in each list.

---

**Caution** Ensure that you make a selection for all the existing configurations. The Migration wizard can be used only once to migrate all the resources at the same time. After it is run once, it will no longer be available.

---

- 4 Click **Migrate**.

In a hosted environment, the migration process might take some time.

## Results

The existing resource configurations are migrated. A virtual apps collection is created for each type of configuration. These collections are displayed in the Virtual Apps Collections page that appears after migration is complete. To view or edit a collection, click its name.

To access the Virtual Apps Collections page at any time, select the **Catalog > Virtual Apps Collections** tab.

For troubleshooting information on virtual apps collections, view both the connector log file, `connector.log`, and the service log file, `horizon.log`. On Linux virtual appliances, the log files are in the `/opt/vmware/horizon/workspace/logs` directory. On Windows servers, the log files are in the `install_dir\IDMConnector_or_VMwareIdentityManager\opt\vmware\horizon\workspace\logs` directory.

## What to do next

- Only one connector, the one you selected in the Migration wizard, is added to each new virtual apps collection. If you had set up a connector cluster for high availability, edit the collections and add the other connectors.
- A single virtual apps collection is created for each migrated configuration. For large integrations, with many servers and apps, consider splitting the collection into multiple collections for easier management and faster sync. The virtual apps collection feature allows you to create multiple collections for each type of integration except ThinApp integrations.

# Creating Virtual Apps Collections

You can create one or more virtual apps collections for each type of integration such as Horizon Cloud or Citrix published resources.

## Prerequisites

- All instances of the VMware Identity Manager service must be version 3.1 or later.
- All connectors used for resources sync must be version 2017.12.1.0 or later.
- The following administrator roles are required:
  - To get started with virtual apps collections, use the Super Admin role. See [About Virtual Apps Collections](#) for more information.
  - To create, edit, or delete Horizon, Horizon Cloud, and Citrix-published virtual apps collections, use any role that can perform the Manage Desktop Apps action in the Catalog service.
  - To create, edit, or delete ThinApps collections, use any role that can perform the Manage ThinApps action in the Catalog service.
  - To edit and save the Network Ranges page for Horizon and Citrix-published virtual apps collections, use the Super Admin role.

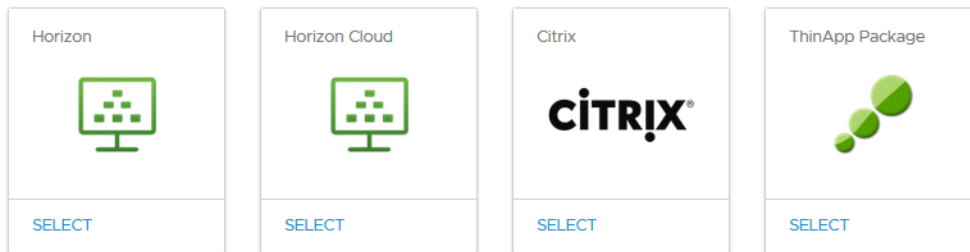
- Integration with ThinApp packaged applications is only supported with the Linux VMware Identity Manager connector. It is not supported with the Windows connector.

## Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
  - If this is the first time you are accessing the page, an information page appears. Click **Get Started** to proceed. The Select the Source Type page appears.

Select the Source Type

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



---

**Note** If a Migration page appears instead, you have existing configurations that must be migrated to virtual apps collections. See [Migrating Existing Configurations to Virtual Apps Collections](#).

---

- If you have accessed the page previously, the Virtual Apps Collections page appears. Click **New** on the page to proceed.
- 2 Select the type of resource to integrate.

You can select Horizon, Horizon Cloud, Citrix published applications, or ThinApp packages as source types.

---

**Note** Integration with ThinApp packaged applications is only supported with the Linux VMware Identity Manager connector. It is not supported with the Windows connector.

---

- 3 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 VMware Identity Manager](#) for more information.
- For a Horizon Cloud Service integration, see [Configure Horizon Cloud Tenant in VMware Identity Manager](#) for more information.
- For a Citrix published applications integration, see [Configuring Citrix Server Farms in VMware Identity Manager](#) for more information.
- For a ThinApp integration, see [Configuring VMware Identity Manager Access to ThinApp Packages](#) for more information.



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

Option	Description
<b>Connector</b>	<p>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 <b>Host</b> list and you can arrange them in failover order for this collection. To rearrange the list, click and drag the rows to the desired position.</p> <hr/> <p><b>Important</b> After you create the collection, you cannot select a different directory.</p>
<b>Sync Frequency</b>	<p>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 <b>Manual</b>.</p>
<b>Activation Policy</b>	<p>Select how you want to make resources in this collection available to users in the Workspace ONE portal and app. If you intend to set up an approval flow, select <b>User-Activated</b>, otherwise select <b>Automatic</b>.</p> <p>With both the <b>User-Activated</b> and <b>Automatic</b> options, the resources are added to the Catalog page. Users can use the resources from the Catalog page or move them to the Bookmarks 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 <b>Users &amp; Groups</b> tab.</p>

### What to do next

After you create the collection, you can view and edit the collection from the Virtual Apps Collections page.

The resources in the new collection are not synced yet. If you set a sync schedule for the collection, the resources are synced at the next scheduled time. To sync the resources manually, select the collection in the Virtual Apps Collections page and click **Sync**.

## Editing Virtual Apps Collections

You can edit all virtual apps collections, for all types of integrations, from the Virtual Apps Collections page in the VMware Identity Manager console.

### Prerequisites

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

## Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the collection to edit and click **Edit**.
- 3 In the Edit Virtual Apps Collection wizard, edit the collection and save your changes.

You can change the following settings:

- The name of the collection
- The source server or path and related settings
- Sync settings such as the sync frequency or the time of the scheduled sync
- Other settings, as applicable to the type of integration

You cannot change the directory after a collection is created.

**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 collection after editing it. Go to the **Catalog > Virtual Apps Collections** page, select the collection, and click **Sync**.

## Syncing Virtual Apps Collections

You can sync a virtual apps collection at any time from the Virtual Apps Collections page, regardless of whether you selected an automatic or manual sync schedule for the collection. Syncing a collection propagates resources and entitlements from the source server to VMware Identity Manager.

## Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the virtual apps collection to sync, and click **Sync**.

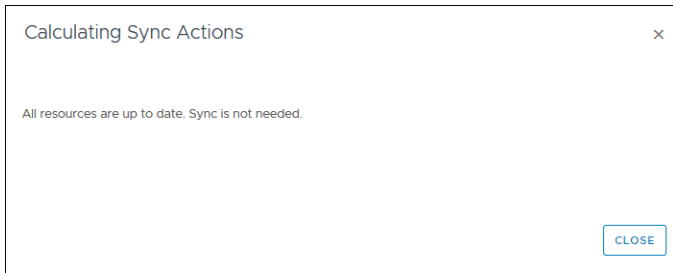
### Collections



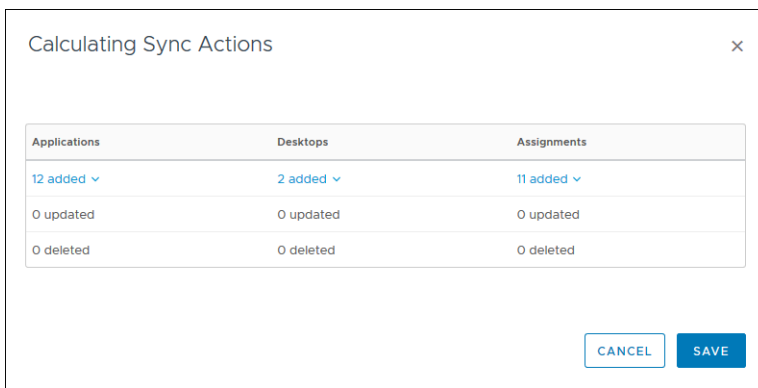
	Name	Source Type	Sync Frequency	Sync Status	⌂	Last Attempt Sync
<input checked="" type="radio"/>	Horizon Cloud	Horizon Cloud	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:23:16 AM
<input type="radio"/>	Horizon View On-Premises	Horizon	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:24:38 AM

VMware Identity Manager compares resources and assignments between the source and the VMware Identity Manager catalog and displays the Calculating Sync Actions dialog box.

If the resources and assignments match, the following message appears:



If there are changes in the source that need to be propagated to VMware Identity Manager, the Calculating Sync Actions dialog box displays the number of applications, desktops, and user assignments that require syncing. You can click the links to see the names of the applications, desktops, and assignments. For example:



- 3 Click **Save** in the Calculating Sync Actions dialog box.

The sync process starts and might take some time to complete, depending on the number of resources and assignments that require syncing. When the sync is completed, the Sync Status in the Virtual Apps Collections page changes from Started to Sync Completed.

## Monitoring Virtual Apps Collections


You can monitor the sync status of all your resource integrations from the Virtual Apps Collections page. 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 VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.  
All collections, for all types of resource integrations, appear on the page.

## Collections

NEW
EDIT
SYNC
DELETE

	Name	Source Type	Sync Frequency	Sync Status		Last Attempt Sync
<input type="radio"/>	<a href="#">Horizon Cloud</a>	Horizon Cloud	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:23:16 AM
<input type="radio"/>	<a href="#">Horizon View On-Premises</a>	Horizon	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 7:24:38 AM
<input type="radio"/>	<a href="#">Citrix</a>	Citrix	Manual	Completed <a href="#">More</a>		Dec 13, 2018, 8:23:42 AM
1 - 3 of 3 item(s)						

### 2 View the information for each collection.

To view	See
The sync schedule that is set for the collection	The <b>Sync Frequency</b> column. If you did not set an automatic sync schedule, the column displays <b>Manual</b> . With a Manual setting, you must sync the virtual apps collection manually each time you want to propagate any changes in resources or entitlements from the source servers to VMware Identity Manager.
The time of the last sync attempt	The <b>Last Sync Attempt</b> column.

To view	See
<p>The status of the last sync</p>	<p>The <b>Sync Status</b> column displays one of the following states:</p> <ul style="list-style-type: none"> <li>■ <b>Not yet synced</b> <p>The virtual apps collection has never been synced.</p> </li> <li>■ <b>Dry Run Completed</b> <p>When you click <b>Sync</b> to sync a virtual apps collection manually, before it performs a sync VMware Identity Manager calculates the number of applications, desktops, and assignments that require syncing and displays the results in the Calculating Sync Actions dialog box. At this point, the status is Dry Run Completed. The sync task is started after you click <b>Save</b>.</p> </li> <li>■ <b>Started</b> <p>The sync process has started.</p> </li> <li>■ <b>Failed to start sync</b> <p>The sync process cannot start because a previous sync is in progress.</p> </li> <li>■ <b>Sync Completed</b> <p>The sync process is complete.</p> </li> <li>■ <b>Failed to complete sync</b> <p>The sync process was not completed. For example, if a network issue prevented the connector from reaching the server from which to sync resources, sync was not completed.</p> </li> <li>■ <b>Not all resources and entitlements were synced</b> <p>Some resources and entitlements were not synced because the sync process was not completed.</p> </li> </ul>


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

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

- 1 Click **More** in the **Sync Status** column.

**Note** The **More** link appears only if all connectors are version 19.03.

- 2 Click the information icon.

Name	Source Type	Sync Frequency	Sync Status	Last Attempt Sync
<input type="radio"/> Horizon Cloud	Horizon Cloud	Manual	Completed 	Dec 13, 2018, 7:23:16 AM

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

Sync Action Summary ✕



Applications	Desktops	Assignments
4 added <span style="font-size: small;">▼</span>	4 added <span style="font-size: small;">▼</span>	0 added
0 updated	0 updated	0 updated
4 deleted <span style="font-size: small;">▼</span>	4 deleted <span style="font-size: small;">▼</span>	18 deleted <span style="font-size: small;">▼</span>

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
<input type="radio"/> Horizon Cloud	Horizon Cloud	Manual	Completed  	Dec 13, 2018, 7:23:16 AM

The Sync Alerts dialog box displays alerts that occurred during sync. For example, if there are assignments for a user that does not exist in VMware Identity Manager, an alert appears.

Sync Alerts ✕

 Could not entitle user with Id cn=adminiator,cn=users,dc=blr,dc=trcint,dc=com to resource Hzc3-Ded-Pool.  
Reason: User not synced in workspace.

 Could not entitle user with Id cn=idmadmin admin,cn=users,dc=blr,dc=trcint,dc=com to resource Hzc3-Ded-Pool.  
Reason: User not synced in workspace.

**Note** Alerts are not separated by collection or by sync run. All alerts appear in the list, including directory sync alerts.

## Deleting Virtual Apps Collections

You can delete virtual apps collections from the Virtual Apps Collections page in the VMware Identity Manager console.

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, Horizon Cloud, 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 VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Select the collection you want to delete and click **Delete**.

# Providing Access to Horizon 7 or Horizon 6 Desktop and Application Pools

# 4

Integrating Horizon 7 or Horizon 6 with the VMware Identity Manager service lets you provide users the ability to access their entitled Horizon desktops and applications from the Workspace ONE portal or app. 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 Administrator interface. You also create entitlements for Active Directory users and groups in Horizon, not in VMware Identity Manager. You must sync these users and groups to the VMware Identity Manager service from Active Directory before integrating with Horizon.

To integrate Horizon pods and pod federations with VMware Identity Manager, you create one or more virtual apps collections in the VMware Identity Manager console. The collections contain the configuration information for the pods and pod federations, as well as sync settings. You then sync the Horizon resources and entitlements to VMware Identity Manager.

In the VMware Identity Manager console, you can view the Horizon desktops and applications. You can also view user and group entitlements.

End users can run their entitled desktops and applications from the Workspace ONE portal or app. These desktops and apps can be accessed over HTML in a browser or over a supported display protocol in the Horizon Client.

## Supported Versions

VMware Identity Manager supports the following versions and features.

- Integrating independent Horizon pods is supported for Horizon 6 and later.
- Integrating pod federations, created using the Cloud Pod Architecture feature, is supported for Horizon 6.2 and later.
- HTML Access is supported for Horizon 6.1.1 and later.
- Certificate SSO is supported for Horizon 7.x.

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



This chapter includes the following topics:

- [About Integrating Independent Horizon Pods](#)
- [About Integrating Horizon Cloud Pod Architecture \(CPA\) Deployments](#)
- [Configuring Horizon Pods and Pod Federations in VMware Identity Manager](#)
- [Setting Client Access FQDNs for Network Ranges](#)
- [Launching Horizon Resources Through Validating Gateways](#)
- [Viewing Horizon Desktop and Application Pool Information in VMware Identity Manager](#)
- [Viewing User and Group Assignments for Horizon Desktop and Application Pools](#)
- [Setting Access Policies for Specific Applications and Desktops](#)
- [Allowing Users to Reset Their Horizon Desktops from the Workspace ONE Catalog](#)
- [Viewing Launch Options for Horizon Desktops and Applications](#)
- [Launching a Horizon Desktop or Application](#)

## About Integrating Independent Horizon Pods

To integrate Horizon pods in VMware Identity Manager, you create one or more virtual apps collections in the VMware Identity Manager console. The collections contain the configuration information for the Horizon Connection Servers as well as sync settings.

Before you perform any integration tasks in the VMware Identity Manager console, set up Horizon. You create and configure desktop and application pools in Horizon Administrator, not in VMware Identity Manager. You also set entitlements for Active Directory users and groups in Horizon Administrator.

Integrating Horizon pods with VMware Identity Manager 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 VMware Identity Manager service using directory sync.
- Create one or more virtual apps collections for the Horizon pods in VMware Identity Manager.
- Configure SAML authenticator on the Horizon Connection Server. You must always use the VMware Identity Manager FQDN on the Authenticator configuration page.

## Requirements for Integrating Horizon Pods

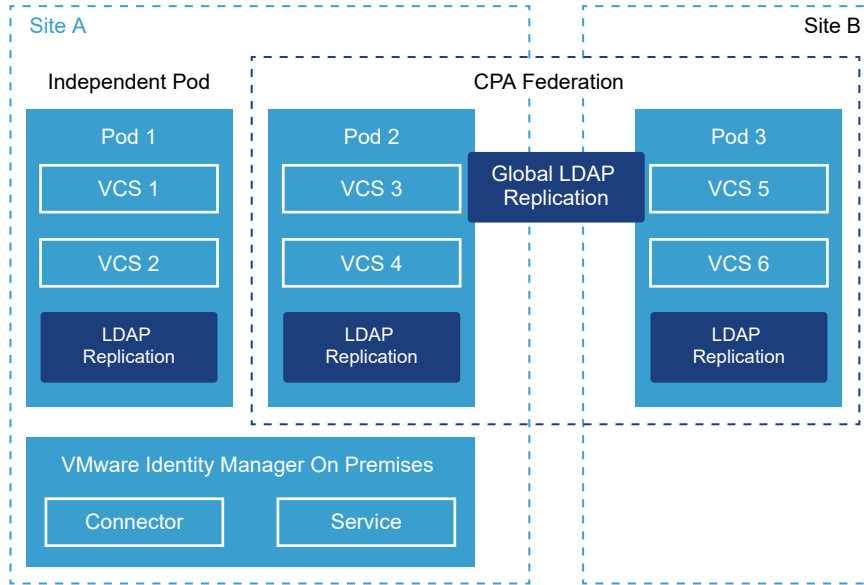
While setting up Horizon pods, ensure that you meet the requirements for the VMware Identity Manager integration.

- 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. VMware Identity Manager requires reverse lookup for the Horizon Connection Servers, Horizon Security Server, and the load balancer. If reverse lookup is not properly configured, the VMware Identity Manager integration with Horizon fails.
- Deploy and configure Horizon pools and desktops 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**.
- Ensure that you create pools in the root folder of the Horizon server. If you create pools in a folder other than the root folder, VMware Identity Manager cannot query those Horizon pools and entitlements.
- 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.

## About Integrating Horizon Cloud Pod Architecture (CPA) Deployments

In addition to integrating independent Horizon pods with VMware Identity Manager, you can integrate Horizon Cloud Pod Architecture (CPA) deployments.

Figure 4-1. Integrating Horizon Pod Federations with VMware Identity Manager



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 VMware Identity Manager 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 VMware Identity Manager.

Pod federations have global entitlements, which enable you to entitle users to desktops and applications which 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 VMware Identity Manager.

Integrating a pod federation with the VMware Identity Manager service involves the following high-level tasks in the VMware Identity Manager console:

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

While VMware Identity Manager 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 VMware Identity Manager service.

---

**Note** Only global entitlements that have the All Sites scope policy in a pod federation are synced. The All Sites scope policy sets the scope of the search for an application or desktop to all the pods across the pod federation.

---

- 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 VMware Identity Manager service, the service does the following:

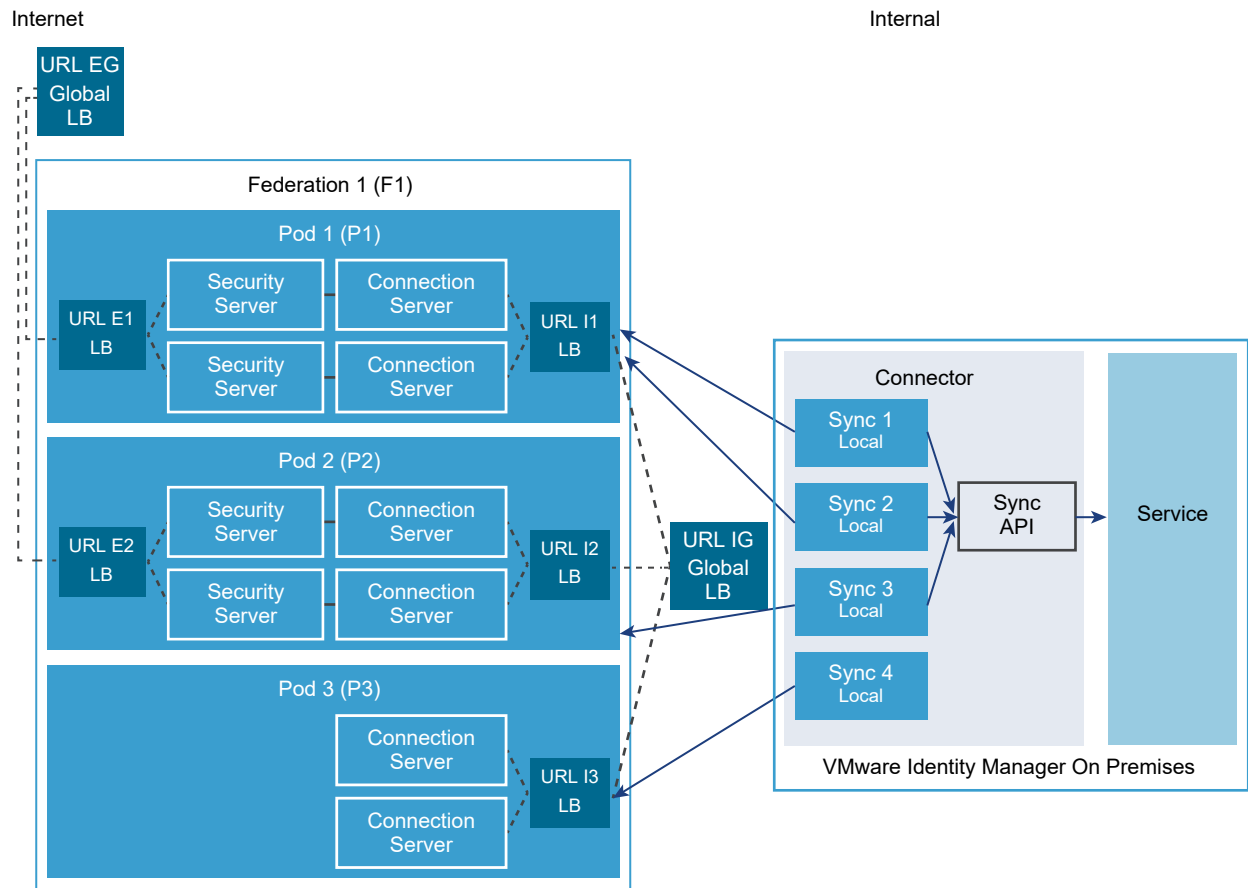
- Syncs all global entitlements that have the All Sites scope policy from the pod federation.
- Syncs local entitlements, if selected, from the pods that are part of the pod federation.
- Syncs metadata from all the Horizon Connection Servers in the pod federation.
- Allows end users to access their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

End users access their Horizon applications and desktops from the Workspace ONE 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. 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 diagram shows a sample cloud pod architecture deployment and how it is integrated with the VMware Identity Manager service.

Figure 4-2. Cloud Pod Architecture Deployment Example



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 VMware Identity Manager service. The VMware Identity Manager 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 VMware Identity Manager Workspace ONE 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

Integrating Horizon pod federations with VMware Identity Manager has the following requirements.

- VMware Identity Manager supports the Cloud Pod Architecture feature in Horizon 6.2 and later, for both applications and desktops.
- You can integrate a maximum of 10 pod federations with the VMware Identity Manager 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. VMware Identity Manager requires reverse lookup for Horizon Connection Server, Security Server, and load balancer instances. If reverse lookup is not properly configured, the VMware Identity Manager integration with Horizon fails.
- The VMware Identity Manager connector must be able to reach all the Horizon Connection Server instances in the pod federation.
- SAML authentication must be configured in Horizon, with the VMware Identity Manager 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 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.

- Horizon Connection Server certificates will be synced to VMware Identity Manager.
- 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 folder in the Horizon server. Ensure that the admin user that you use to sync Horizon entitlements to VMware Identity Manager has root level access so that all pools can be synced.

If you add or remove application or desktop pools after integrating with VMware Identity Manager, for the changes to appear in the VMware Identity Manager 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 VMware Identity Manager 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 with the VMware Identity Manager service, you must edit the pod federation details in the VMware Identity Manager 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.
- The global entitlements that you want to sync to VMware Identity Manager must have the **All sites** scope policy set. Entitlements with any other scope policy are not synced.

The screenshot shows the 'Add Global Entitlement' configuration interface. On the left, there is a navigation pane with 'Type' selected, showing 'Name and Policies', 'Users and Groups', and 'Ready to Complete'. The main content area is titled 'Name and Policies' and is divided into 'General' and 'Policies' sections. In the 'General' section, the 'Name' field is filled with 'GA 2' and the 'Description' field is empty. In the 'Policies' section, the 'Scope' is set to 'All sites' (indicated by a selected radio button). Other options include 'Use home site', 'Entitled user must have home site', 'Automatically clean up redundant sessions', and 'HTML Access', all of which are currently unchecked.

- To enable end users to launch desktops or application in a Web browser, select the HTML Access option for the global entitlement in Horizon.
- (Optional) Create local entitlements on the pods, if required.

For more information about configuring Horizon, see the Horizon 6 or Horizon 7 documentation.

## Configuring Horizon Pods and Pod Federations in VMware Identity Manager

To configure Horizon pods and pod federations in VMware Identity Manager, you set up your VMware Identity Manager 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 VMware Identity Manager Environment

After setting up your Horizon environment, you must set up your VMware Identity Manager environment before you integrate the Horizon pods and pod federations with the VMware Identity Manager service.

### Procedure

- 1 Ensure that `distinguishedName` is set as a required attribute for the VMware Identity Manager directory and that it is mapped to the Active Directory attribute `distinguishedName`.

Attributes must be marked as required before the directory is created. After the directory is created, attributes cannot be changed from optional to required.

- a In the VMware Identity Manager console, navigate to the **Identity & Access Management > Setup > User Attributes** page.
  - b Under **Default Attributes**, select the **Required** check box for **`distinguishedName`**.
  - c Click **Save**.
  - d While creating the directory, map the **`distinguishedName`** attribute to the Active Directory attribute **`distinguishedName`**.
- 2 Sync the users and groups that have global or local entitlements in Horizon from Active Directory to the VMware Identity Manager service using directory sync.
    - 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 Modify the directory settings if needed, and click **Sync Now**.

---

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

---

- 3 If applicable, establish a connection to multi-domains or trusted multi-forest domains in Active Directory. See *Installing and Configuring VMware Identity Manager* for information.

## Configure Horizon Pods and Pod Federations in VMware Identity Manager

Configure Horizon pods and pod federations in the VMware Identity Manager console to sync resources and entitlements to the VMware Identity Manager 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 VMware Identity Manager connector 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 access resources.

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 SAML configuration on the Horizon server, make sure you edit the Virtual Apps Collection page in the VMware Identity Manager console and click Save to update the latest Horizon settings in the VMware Identity Manager service.

---

### Prerequisites

- Set up Horizon according to [Requirements for Integrating Horizon Pods](#) and [Requirements for Integrating Horizon Pod Federations](#).
- Set up VMware Identity Manager according to [Set up Your VMware Identity Manager Environment](#).
- For each Horizon pod that you want to configure in VMware Identity Manager, ensure that you have the credentials of a user with the administrators role.
- To perform this procedure in VMware Identity Manager, 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 select to perform that step separately.

### Procedure

- 1 Log in to the VMware Identity Manager console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click **New**.
- 4 Select **Horizon** as the source type.

- In the New Horizon Virtual Apps Collection wizard, enter the following information in the Connector page.

Option	Description
<b>Name</b>	Enter a unique name for the Horizon collection.
<b>Connector</b>	<p>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 <b>Host</b> list and you can arrange them in failover order for this collection.</p> <p><b>Important</b> After you create the collection, you cannot select a different directory.</p>

- Click **Next**.

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

- To add more pods, click **Add a Pod** and enter the information for each pod.

- 9 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.

Option	Description
<b>Federation Name</b>	The name of the pod federation.
<b>Client Access FQDN</b>	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. For example, <b>federationA.example.com</b> . You can customize the Client Access FQDN for specific network ranges later in the configuration process.
<b>Horizon Pods</b>	Select the pods that belong to the pod federation. The <b>Available Pods</b> column displays all the pods that you added to the collection. When you select a pod, it is added to the <b>Selected Pods</b> column. You can arrange the pods in the <b>Selected Pods</b> column in failover order.

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

10 Click **Next**.

11 In the Configuration page, enter the following information.

Option	Description
<b>Sync Frequency</b>	Select how often you want to sync the resources in the collection. 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 <b>Manual</b> , you must click <b>Sync</b> 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.
<b>Sync Duplicate Apps</b>	Set to <b>No</b> if you want to prevent duplicate applications from being synced from multiple servers. When VMware Identity Manager is deployed in multiple data centers, the same resources are set up in the multiple data centers. Setting this option to <b>No</b> prevents duplication of the desktop or application pools in your VMware Identity Manager catalog.

Option	Description
<b>Activation Policy</b>	<p>Select how you want to make resources in this collection available to users in the Workspace ONE portal and app. If you intend to set up an approval flow, select <b>User-Activated</b>, otherwise select <b>Automatic</b>.</p> <p>With both the <b>User-Activated</b> and <b>Automatic</b> options, the resources are added to the Catalog tab. Users can use the resources from the Catalog tab or move them to the Bookmarks 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 <b>Users &amp; Groups</b> tab.</p>
<b>Default Launch Client</b>	<p>Select the default client for end users accessing Horizon desktops and apps from the Workspace ONE portal or app.</p> <p><b>None:</b> No default preference is set at the administrator level. If this option is set to <b>None</b> and the end user does not set a preference either, the Horizon <b>Default display protocol</b> setting is used to determine how to launch the desktop or application.</p> <p><b>Browser:</b> Horizon desktops and applications are launched in a web browser by default. End user preferences, if set, override this setting.</p> <p><b>Native:</b> 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"> <li>End user preference setting, set in the Workspace ONE portal. This option is not available in the Workspace ONE app.</li> <li>Administrator <b>Default Launch Client</b> setting for the collection, set in the VMware Identity Manager console.</li> <li>Horizon <b>Remote Display Protocol &gt; Default display protocol</b> setting for the desktop or application pool, set in Horizon Administrator. For example, when the display protocol is set to PCoIP, the application or desktop is launched in the Horizon Client.</li> </ol>

12 Click **Next**.

13 In the Summary page, review your selections, then click **Save & Configure Network Range**.

The Network Ranges page appears.

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

- Click the network range to edit or click **Create Network Range** to create a new network range, if necessary.
- If you are creating a new network range, enter a name, optional description, and the IP address range.

- c Scroll to the **Pod** and **View CPA Federation** sections.

The Pod section lists all the Horizon pods that you added to the collection that have the Syc Local Assignments option enabled. The View CPA Federation section lists all the pod federations that you added.

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

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

Option	Description
<b>Client Access FQDN</b>	Specify 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 can be a Horizon Connection Server, security server, load balancer, or reverse proxy FQDN.  For example: <b>internal1b.example.com</b>  The Client Access FQDN for a pod is used to launch locally-entitled resources from the pod.
<b>Port</b>	The server port.
<b>Wrap Artifact in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .
<b>Audience in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .

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

Option	Description
<b>Client Access FQDN</b>	Specify 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 is typically the global load balancer of the pod federation deployment.  For example: <b>global1lb.example.com</b>  The Client Access FQDN for a pod federation is used to launch globally-entitled resources.
<b>Port</b>	The server port.
<b>Wrap Artifact in JWT</b>	When the VMware Identity Manager service is integrated with a validating gateway, such as F5, this option must be enabled to authenticate Horizon resources assigned to users. See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .
<b>Audience in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .

- f Click **Save**.
- g Repeat these steps to edit the other network ranges.
- h Click **Finish** in the Network Ranges page.

#### 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

After you create a Horizon virtual apps collection in VMware Identity Manager, log in to Horizon Administrator and configure SAML authentication on the Horizon Connection Server instances to allow users to launch Horizon desktops and applications using single sign-on.

You must configure SAML authentication on at least one Horizon Connection Server instance in a pod. Configuring SAML authentication on all instances in the pod is recommended.

If SAML authentication is disabled on some of the Horizon Connection Server instances in a pod, VMware Identity Manager uses the other instances for sync. However, ensure that any instance with SAML authentication disabled 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 SAML authentication is disabled on all the Horizon Connection Server instances in the pod, 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 the Horizon Administrator as a user that has the administrator role.
- 2 Configure SAML authentication on the Horizon Connection Server instances.

See the [Horizon 7 documentation](#) for information.

Ensure that you specify the FQDN of the VMware Identity Manager service when you configure the SAML Authenticator.

---

**Important** The Horizon and VMware Identity Manager 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, make sure you edit the Virtual Apps Collection page in the VMware Identity Manager console and click **Save** to update the latest Horizon settings in the VMware Identity Manager service.

---

## Setting Client Access FQDNs for Network Ranges

As part of integrating VMware Identity Manager and Horizon, you specify Client Access FQDNs for network ranges so that users connect to the correct server based on the network range from which they are accessing Horizon resources. When you create a Horizon virtual apps collection, the wizard guides you to the Network Ranges page to configure this information. After creating the collection, you can edit the Client Access FQDNs at any time.

Whenever you create new network ranges in VMware Identity Manager, make sure that you follow this procedure to add Client Access FQDNs for Horizon pods and pod federations to the new network ranges.

#### Prerequisites

A Super Admin role is required for this procedure.

#### Procedure

- 1 Log in to the VMware Identity Manager console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click the Horizon collection, then click **Edit Network Range**.

- 4 In the Network Ranges page, click the network range to edit or click **Create Network Range** to create a network range, if necessary.
- 5 If you are creating a new network range, enter a name, optional description, and the IP range.
- 6 Scroll to the **Pod** and **CPA Federation** sections.

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"/>	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"/>	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
<b>Client Access FQDN</b>	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, security server, load balancer, or reverse proxy FQDN. For example: <b>internal1b.example.com</b> The Client Access FQDN for a pod is used to launch locally entitled resources from the pod.
<b>Port</b>	The server port.
<b>Wrap Artifact in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .
<b>Audience in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .

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

Option	Description
<b>Client Access FQDN</b>	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: <b>global1b.example.com</b> The Client Access FQDN for a pod federation is used to launch globally entitled resources.
<b>Port</b>	The server port.



Option	Description
<b>Wrap Artifact in JWT</b>	When the VMware Identity Manager service is integrated with a validating gateway, such as F5, this option must be enabled to authenticate Horizon resources assigned to users. See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .
<b>Audience in JWT</b>	See <a href="#">Launching Horizon Resources Through Validating Gateways</a> .

9 Click **Save**.

10 Repeat these steps to edit the other network ranges, if necessary.

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 desktops and applications.

11 Click **Finish** in the Network Ranges page.

## Launching Horizon Resources Through Validating Gateways

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

When Wrap Artifact in JWT is enabled to authenticate a Horizon resource launch request, the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager details.
  - SSL Certificate
  - OAuth2 client ID and secret
  - VMware Identity Manager validation endpoint URL
- A Super Admin role is required in VMware Identity Manager to perform this procedure.

### Procedure

1 Log in to the VMware Identity Manager 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 VMware Identity Manager](#) 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 <input type="text"/>	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 VMware Identity Manager

After integrating VMware Identity Manager and Horizon, you can view details about the Horizon desktop and application pools that are synced to VMware Identity Manager from the Horizon servers.

#### Procedure

- 1 In the VMware Identity Manager 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 VMware Identity Manager settings for the application, such as categories, access policies, and licensing.

---

## Viewing User and Group Assignments for Horizon Desktop and Application Pools

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

### Prerequisites

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

### Procedure

- 1** Log in to the VMware Identity Manager console.

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

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

## Setting Access Policies for Specific Applications and Desktops

The default access policy set applies to all applications and desktops in your 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.

For detailed information on access policies and how they are applied, see the *VMware Identity Manager Administration Guide*.

### Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
  - a In the VMware Identity Manager 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 VMware Identity Manager 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

Depending on how you configure Horizon and VMware Identity Manager, users can reset an unresponsive Horizon desktop from the Workspace ONE catalog.

You configure this setting in Horizon Administrator, not in the VMware Identity Manager console. The configuration applies to both Horizon and VMware Identity Manager. In the VMware Identity Manager console, you can view whether a specific desktop is resettable or not.

The option to reset desktops from Workspace ONE is available in VMware Identity Manager 3.2 and Connector 2018.1.1.0, and later versions. Ensure that all connectors are version 2018.1.1.0 or later, otherwise the Reset command does not appear. The option 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 Horizon 7 or Horizon 6.
- Ensure that you are using VMware Identity Manager 3.2 or later and Connector 2018.1.1.0 or later. All connectors must be version 2018.1.1.0 or later.
- 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 VMware Identity Manager to trust those certificates. See *VMware Identity Manager Installation and Configuration* for information about adding a root certificate.

## Procedure

- ◆ (Optional) Verify that VMware Identity Manager lists the desktop as resettable by users.
  - a In the VMware Identity Manager 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

Horizon desktops and applications can be launched from the Workspace ONE catalog in Horizon Client or a Web browser, based on how the desktop or application has been 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 provides Horizon administrators the option of configuring a desktop or application for browsers. This configuration is done in Horizon and no configuration is required in VMware Identity Manager. In Horizon 7, the **Allow HTML Access to desktop and applications on this farm** setting determines whether users in VMware Identity Manager have the option to launch desktops or applications from that farm in a browser.

VMware Identity Manager supports HTML Access for Horizon 6.1.1 and later.

VMware Identity Manager also supports all the display protocols that Horizon supports for Horizon Client. For Horizon 7, VMware Identity Manager supports the Blast protocol in addition to PCoIP and RDP for Horizon Client 4.0. When VMware Identity Manager 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 VMware Identity Manager console, you can check the launch options that a Horizon desktop or application supports.

### Procedure

- 1 Log in to the VMware Identity Manager 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/YmJmZThiMzYtZDIiYS00MjRkLWE5MmVtNTNiY2JiZDQyM... <a href="#">Copy</a>
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 Workspace ONE 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** For Horizon 7 integrations, the **Allow HTML Access to desktop and applications on this farm** option must be enabled in Horizon 7 for the **BROWSER** option to appear in the **Supported client types** list.

## Launching a Horizon Desktop or Application

Users can run the Horizon desktops or applications to which they are entitled from the Workspace ONE portal or app.

Based on how an application or desktop has been 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 in the **Preferences** page in the Workspace ONE portal. This user preference overrides any default launch preference set at the administrator level.

---

**Note** Users cannot set a default launch preference in the Workspace ONE app.

---

### Prerequisites

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

For supported Horizon Client versions, see the VMware Product Interoperability Matrix at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

### Procedure

- 1 Log in to the Workspace ONE portal.
- 2 Click **Open** on the desktop or application you want to use, select the launch method, and click **Open**.

---

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

---

### Results

If you chose the **Browser** option, the application or desktop is started in a browser. If you are using Horizon 6.1.1 or later, the browser window also displays an HTML Access Tray.

---

**Note** If the SAML metadata on the Horizon Connection Server instances has expired, the application or desktop will not launch. To resolve this issue, sync the Horizon resources to VMware Identity Manager again. Navigate to the **Catalog > Virtual Apps Collections** page, select the collection, and click **Sync**.

---



# Providing Access to VMware Horizon Cloud Service Desktops and Applications

# 5

VMware Horizon Cloud Service with Hosted or On-Premises Infrastructure can be integrated with the VMware Identity Manager service.

Integrating Horizon Cloud with the VMware Identity Manager service lets you provide users the ability to access their entitled Horizon Cloud applications and desktops from the Workspace ONE portal or app. This provides users a single place for accessing all their applications across devices.

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

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

You can set up a sync schedule for each collection to regularly sync resources and entitlements from the Horizon Cloud tenants to the VMware Identity Manager service.

After you integrate the Horizon Cloud tenant with VMware Identity Manager, you can see the Horizon Cloud desktops and applications in the VMware Identity Manager console. You can also view user and group entitlements.

End users can launch their entitled desktops and apps from the Workspace ONE portal or app. These desktops and apps can be accessed in a browser or in the VMware Horizon<sup>®</sup> Client<sup>™</sup>. Horizon Client versions 3.4 and later are supported.

This chapter includes the following topics:

- [Integrating Horizon Cloud Desktops and Applications](#)
- [Viewing Horizon Cloud Desktop and Application Pool Information in VMware Identity Manager](#)
- [Viewing User and Group Assignments for Horizon Cloud Desktops and Applications](#)
- [Setting Access Policies for Specific Applications and Desktops](#)

- [Allowing Users to Reset Horizon Cloud Desktops](#)
- [Running a Horizon Cloud Desktop or Application](#)

## Integrating Horizon Cloud Desktops and Applications

To integrate Horizon Cloud desktops and applications with the VMware Identity Manager service, you create one or more virtual apps collections in the VMware Identity Manager console, configure Horizon Cloud tenant details in the collection, and sync resources and entitlements from the Horizon Cloud tenant. You also configure SAML authentication to enable trust between the Horizon Cloud tenant and the VMware Identity Manager service.

## Integrating Multiple Horizon Cloud Instances

You can integrate multiple Horizon Cloud tenants with a single instance of VMware Identity Manager 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.

VMware Identity Manager supports integration with the following types of Horizon Cloud environments:

- Horizon Cloud Hosted Infrastructure (Soft-Layer and Azure)
- Horizon Cloud On Premises Infrastructure

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

- A single VMware Identity Manager connector can sync resources and entitlements from multiple Horizon Cloud tenants to the VMware Identity Manager 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 VMware Identity Manager so all users with entitlements in any of the Horizon Cloud tenants are synced to VMware Identity Manager.
- If the tenant appliances have self-signed certificates, you must upload the self-signed certificate as a trusted root certificate in VMware Identity Manager. 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 VMware Identity Manager.
- VMware Identity Manager cannot access and sync entitlements from a tenant on which two-factor authentication is enabled.
- In VMware Identity Manager, 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 VMware Identity Manager 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 VMware Identity Manager.

## Prerequisites for Integration

Before you integrate Horizon Cloud with VMware Identity Manager, ensure that you meet the prerequisites.

- Verify that you have the following setup:
  - A VMware Identity Manager on-premises deployment  
Integrating multiple Horizon Cloud tenants with a single VMware Identity Manager instance is supported in VMware Identity Manager 3.x and later.
  - A VMware Identity Manager connector installed on premises.  
VMware Identity Manager connector version 2016.1.1 or later is required for Horizon Cloud integration. Version 2017.8.1.0 or later is required for integration with multiple Horizon Cloud tenants.
  - One or more Horizon Cloud tenants that are accessible by the VMware Identity Manager service. Work with your Horizon Cloud representative to set this up.

---

**Important** Your VMware Identity Manager deployment and your Horizon Cloud tenants need VPN connectivity to work.

---

- 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-ta1.example.com` instead of `server-ta1`.
  - The tenant appliances should 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 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 VMware Identity Manager.
  - If the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager.

---

- In the VMware Identity Manager console, ensure that users and groups with Horizon Cloud entitlements are synced from Active Directory to VMware Identity Manager 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 VMware Identity Manager so that users with entitlements in any of the Horizon Cloud tenants are synced to VMware Identity Manager.
- sAMAccountName must be set as the directory search attribute for the directory in VMware Identity Manager.
- distinguishedName must be set as a required attribute for the VMware Identity Manager directory and it must be mapped to the Active Directory attribute distinguishedName.

Attributes must be marked as required before the directory is created. After the directory is created, attributes cannot be changed from optional to required.

- 1 In the VMware Identity Manager console, navigate to the **Identity & Access Management > Setup > User Attributes** page.
- 2 Under **Default Attributes**, select the **Required** check box for **distinguishedName**.
- 3 Click **Save**.
- 4 While creating the directory, map the **distinguishedName** attribute to the Active Directory attribute **distinguishedName**.

## Configure Horizon Cloud Tenant in VMware Identity Manager

To integrate Horizon Cloud tenants with the VMware Identity Manager service, you create a virtual apps collection in the VMware Identity Manager console, which contains Horizon Cloud

tenant information as well as sync settings, and sync resources and entitlements from the Horizon Cloud tenant to the VMware Identity Manager 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 is synced separately.

### Prerequisites

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

### Procedure

- 1 Log in to the VMware Identity Manager 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
<b>Name</b>	Enter a unique name for the Horizon Cloud collection.
<b>Connector</b>	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 <b>Host</b> list and you can arrange them in failover order for this collection.  <b>Important</b> 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
<b>Host</b>	Fully-qualified domain name of your Horizon Cloud tenant host. For example: <b>tenant1.example.com</b>
<b>Port</b>	Port number of your Horizon Cloud tenant host. For example: <b>443</b>
<b>Admin User</b>	User name for your Horizon Cloud tenant administrator account. For example: <b>tenantadmin</b>
<b>Admin Password</b>	Password for your Horizon Cloud tenant administrator account.

Option	Description
<b>Admin Domain</b>	Active Directory NETBIOS domain name in which the Horizon Cloud tenant administrator resides.
<b>Domains to Sync</b>	Active Directory NETBIOS domain names for syncing Horizon Cloud resources and entitlements.  <b>Note</b> This field is case-sensitive. Ensure that you use the proper case when you enter the names.
<b>Assertion Consumer Service URL</b>	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.
<b>True SSO</b>	Enable this option only if True SSO is enabled for the Horizon Cloud tenant. When this option is enabled, users logged into VMware Identity Manager with a non-password authentication method such as SecurID will not be prompted for a password when they launch their Windows desktops.
<b>Custom ID Mapping</b>	<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><b>Name ID Format:</b> Select the name ID format, such as Email address or User Principal Name. The default value is <b>Unspecified (username)</b>.</p> <p><b>Name ID Value:</b> Click <b>Select from suggestions</b> and pick from a predefined list of values or click <b>Custom value</b> and enter the value. This value can be any valid Expression Language (EL) expression such as <b>`\${user.userName}@\${user.domain}</b>. The default value is <b>`\${user.userPrincipalName}</b>.</p> <p><b>Note</b> 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, userName, userPrincipalName, and domain 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"> <li>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.</li> </ul> <p><b>Important</b> Ensure that you use the same name ID format setting in Horizon Cloud and VMware Identity Manager.</p>

8 Click **Add**.

9 Add other tenants, if required, then click **Next**.

**10** In the Configuration page, enter the following information.

Option	Description						
<b>Sync Frequency</b>	<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 <b>Manual</b>, you must click <b>Sync</b> 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>						
<b>Activation Policy</b>	<p>Select how you want to make resources in this collection available to users in the Workspace ONE portal and app. If you intend to set up an approval flow, select <b>User-Activated</b>, otherwise select <b>Automatic</b>.</p> <p>With both the <b>User-Activated</b> and <b>Automatic</b> options, the resources are added to the Catalog page. Users can use the resources from the Catalog page or move them to the Bookmarks 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 <b>Users &amp; Groups</b> tab.</p>						
<b>Default Launch Client</b>	<p>Select the default client for end users accessing Horizon Cloud desktops and apps from the Workspace ONE portal or app.</p> <table border="0" data-bbox="625 966 1434 1323"> <tr> <td data-bbox="625 966 718 1102">None</td> <td data-bbox="718 966 1434 1102">No default preference is set at the administrator level. If this option is set to <b>None</b> 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 data-bbox="625 1102 718 1218">Browser</td> <td data-bbox="718 1102 1434 1218">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 data-bbox="625 1218 718 1323">Native</td> <td data-bbox="718 1218 1434 1323">Horizon Cloud desktops and applications are launched in the Horizon Client by default. End user preferences, if set, override this setting.</td> </tr> </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 data-bbox="625 1428 1434 1617" style="list-style-type: none"> <li>a End user preference setting, set in the Workspace ONE portal. This setting is not available in the Workspace ONE app.</li> <li>b Administrator <b>Default Launch Client</b> setting for the collection, set in the VMware Identity Manager console.</li> <li>c Horizon Cloud Default Protocol settings</li> </ol>	None	No default preference is set at the administrator level. If this option is set to <b>None</b> 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 <b>None</b> 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 VMware Identity Manager.

#### What to do next

Configure SAML authentication in the Horizon Cloud tenant to enable trust between the VMware Identity Manager service and the Horizon Cloud tenant.

## Configure SAML Authentication in the Horizon Cloud Tenant

After you create a virtual apps collection for the Horizon Cloud integration in the VMware Identity Manager 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.

---

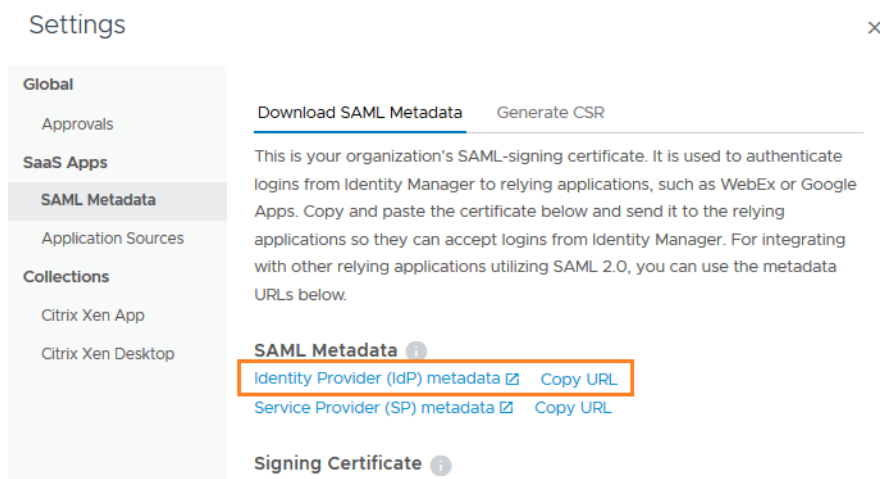
**Note** The Horizon Cloud tenant appliance and VMware Identity Manager must be in time sync. If they are not in time sync, when you try to launch Horizon Cloud desktops and applications, an invalid SAML message appears.

---

#### Procedure

- 1 In the VMware Identity Manager 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
<b>Identity Manager URL</b>	The VMware Identity Manager 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>
<b>Timeout SSO Token</b>	(Optional) The amount of time, in minutes, after which the SSO token times out.
<b>Data Center</b>	The Horizon Cloud data center name. Select the name from the drop-down list.
<b>Tenant Address</b>	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
<b>VMware Identity Manager URL</b>	The VMware Identity Manager 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>
<b>Timeout SSO Token</b>	(Optional) The amount of time, in minutes, after which the SSO token times out.
<b>Location</b>	Select a location to filter the Node drop-down list to the nodes associated with that location.
<b>Node</b>	Select the node you are integrating with VMware Identity Manager.
<b>Data Center</b>	The Horizon Cloud data center name. Select the name from the drop-down list.
<b>Tenant Address</b>	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 VMware Identity Manager, click **Configure** and edit the settings.

Option	Description
<b>Force Remote Users to Identity Manager</b>	Select YES to block remote user access except through IDM. Option only displays if Identity Manager status is green.
<b>Force Internal Users to Identity Manager</b>	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 VMware Identity Manager, you can view Horizon Cloud desktop and application pools in the VMware Identity Manager console and end users can launch the resources to which they are entitled from the Workspace ONE portal or app.

## Viewing Horizon Cloud Desktop and Application Pool Information in VMware Identity Manager

In the VMware Identity Manager console, you can view information about the synced Horizon Cloud desktop and application pools.

### Procedure

- 1 In the VMware Identity Manager 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 VMware Identity Manager settings for the application, such as categories, access policies, and licensing.

---

## Viewing User and Group Assignments for Horizon Cloud Desktops and Applications

In the VMware Identity Manager 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 VMware Identity Manager. You cannot edit the assignments from VMware Identity Manager.

### Prerequisites

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

**Procedure**

- 1 Log in to the VMware Identity Manager console.
- 2 View user and group assignments for Horizon Cloud desktop and application pools.

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

## Setting Access Policies for Specific Applications and Desktops

The default access policy set applies to all applications and desktops in your 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.

For detailed information on access policies and how they are applied, see the *VMware Identity Manager Administration Guide*.

**Procedure**

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
  - a In the VMware Identity Manager 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 VMware Identity Manager 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.

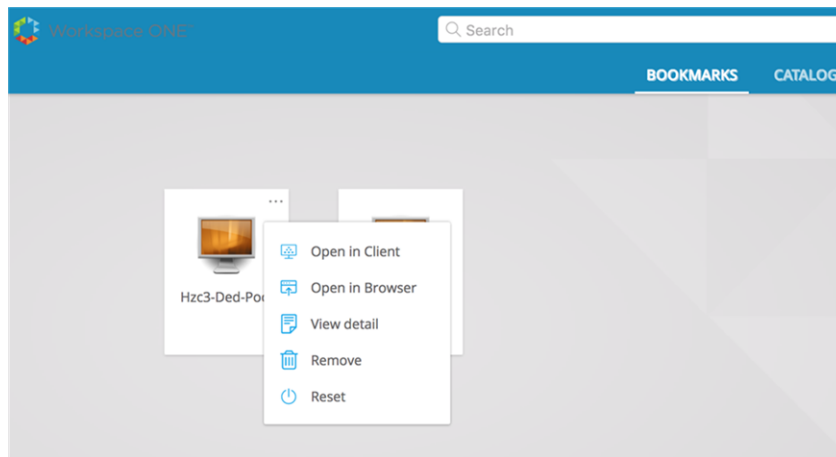
## Allowing Users to Reset Horizon Cloud Desktops

Depending on how the setting is configured in Horizon Cloud, users can reset dedicated Horizon Cloud desktops from Workspace ONE. Users can reset their desktops if they become unresponsive, for example.

The option to allow users to reset their desktops is configured in Horizon Cloud, not in VMware Identity Manager. The setting is supported in VMware Identity Manager 3.2 and Connector 2018.1.1.0, and later versions. Ensure that all connectors are version 2018.1.1.0 or later.

Only dedicated Horizon Cloud desktops can be reset from Workspace ONE.

If Horizon Cloud allows users to reset desktops, the Reset command is available for the desktop in Workspace ONE. The command only appears for those desktops for which reset is allowed.



## Running a Horizon Cloud Desktop or Application

End users can run the Horizon Cloud desktops and applications that are assigned to them from the Workspace ONE 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 in the **Preferences** page in the Workspace ONE portal. This user preference overrides any default launch preference set at the administrator level.

---

**Note** Users cannot set a default launch preference in the Workspace ONE 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](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

### Procedure

- 1 Log in to the Workspace ONE portal.
- 2 Click **Open** on the desktop or application you want to use, select the launch method, and click **Open**.

---

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

---

# Providing Access to VMware ThinApp Packages

## 6

With VMware Identity Manager, 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 VMware Identity Manager Desktop application installed on their Windows systems can launch and use their entitled ThinApp packages on those Windows systems.

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 VMware Identity Manager. When you capture a Windows application, the default settings in the ThinApp capture-and-build process create a package that VMware Identity Manager cannot distribute and manage. You create a ThinApp package that VMware Identity Manager 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 VMware Identity Manager.

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

---

**Important** Integration with ThinApp is supported with the Linux VMware Identity Manager connector only. It is not supported with the Windows connector.

---

This chapter includes the following topics:

- [Integrating VMware ThinApp Packages](#)
- [Entitle Users and Groups to ThinApp Packages](#)
- [Distributing and Managing ThinApp Packages with VMware Identity Manager](#)

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

## Integrating VMware ThinApp Packages

To use VMware Identity Manager to distribute and manage applications packaged with VMware<sup>®</sup> ThinApp<sup>®</sup>, 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 VMware Identity Manager catalog and you can entitle them to your VMware Identity Manager 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 VMware Identity Manager, 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 VMware Identity Manager, see the VMware ThinApp documentation.

Typically, you perform the steps to connect VMware Identity Manager to the repository and sync the packages as part of the overall setup and configuration of your VMware Identity Manager environment. The ThinApp repository must be a network share that is accessible to VMware Identity Manager using a Uniform Naming Convention (UNC) path. VMware Identity Manager synchronizes with this network share regularly to obtain the ThinApp package metadata that VMware Identity Manager requires to distribute and manage the packages. See [VMware Identity Manager 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.

### VMware Identity Manager Requirements for ThinApp Packages and the Network Share Repository

When you capture and store ThinApp applications to distribute from VMware Identity Manager, you must meet certain requirements.

## Requirements on the ThinApp Packages

To create or repackage ThinApp packages that VMware Identity Manager can manage, you must use a version of ThinApp that VMware Identity Manager supports. VMware Identity Manager 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](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

You must have ThinApp packages that VMware Identity Manager can manage. In the ThinApp capture-and-build process, you can create packages that VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager.

For existing ThinApp packages, you can use the `reLink - h` command to enable the packages for VMware Identity Manager. For information about how to convert existing ThinApp packages to packages that VMware Identity Manager can manage, see the *VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager.

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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager	Requirements for the User's Windows System
<p>Domain-based access</p>	<p>You can use a CIFS share for your ThinApp package repository when you use domain-based access. 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 VMware Identity Manager to the Active Directory domain so it can join the Windows network share and access the packages.</p> <p>For more information about how to configure VMware Identity Manager to join the domain, see information about configuring Kerberos in <i>VMware Identity Manager Installation and Configuration</i>.</p> <hr/> <p><b>Note</b> Windows authentication is not required.</p> <hr/> <p>The network share must support authentication and file permissions that are based on computer accounts. VMware Identity Manager accesses the network share with the computer account of VMware Identity Manager in the domain. 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 VMware Identity Manager 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"> <li>■ The user's Windows system</li> <li>■ VMware Identity Manager</li> <li>■ The host of the network share drive with the ThinApp packages</li> </ul> <p>When you use domain-based access, the following installation modes for the ThinApp packages are allowed.</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ 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.</li> </ul> <hr/> <p><b>Note</b> 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 VMware Identity Manager	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 VMware Identity Manager 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 VMware Identity Manager to the Active Directory domain to access the network share.</p> <hr/> <p><b>Note</b> In the VMware Identity Manager console, you must complete the Join Domain page before you can use the ThinApp Packages page.</p> <hr/> <p><b>Note</b> 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 VMware Identity Manager 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 <a href="#">Command-Line Installer Options for VMware Identity Manager Desktop</a> .</p> <hr/> <p><b>Important</b> 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, VMware Identity Manager, 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"> <li>■ 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.</li> </ul> <p>VMware Identity Manager uses the share user account to retrieve the packages from the repository.</p> <ul style="list-style-type: none"> <li>■ 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.</li> </ul>

Access Type	Network Share Type	Requirements on VMware Identity Manager	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 VMware Identity Manager 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 VMware Identity Manager Desktop application on a Windows system by running the graphical version of the client's installer program.</p> <p>VMware Identity Manager must be configured for account-based access for the attempt to download the packages using HTTP_DOWNLOAD mode to succeed.</p> <hr/> <p><b>Important</b> 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 VMware Identity Manager 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 VMware Identity Manager Manages](#).

## Create a Network Share for ThinApp Packages That VMware Identity Manager Manages

If you want to enable the VMware ThinApp management capabilities of VMware Identity Manager 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.

VMware Identity Manager obtains the metadata it needs about the ThinApp packages from the network file share.

### Prerequisites

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

### Procedure

- 1 Create a network share that meets the VMware Identity Manager 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 VMware Identity Manager. 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 VMware Identity Manager access to the ThinApp packages.

## Configuring VMware Identity Manager Access to ThinApp Packages

To configure VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager console requires the completion of the Join Domain page before you can use the ThinApp Packages page.

To enable domain-based access, you must also join VMware Identity Manager 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 VMware Identity Manager 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 [VMware Identity Manager 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 If the VMware Identity Manager Linux connector is not already domain-joined, join it to the Active Directory domain.
  - a Log in to the VMware Identity Manager 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 VMware Identity Manager console.

Option	Description
<b>AD Domain</b>	Type the fully qualified domain name of the Active Directory. An example is <b>HS.TRDOT.COM</b> .
<b>AD Username</b>	Type the username of an account in the Active Directory that has permissions to join systems to that Active Directory domain.
<b>AD Password</b>	Type the password associated with the <b>AD Username</b> . This password is not stored by VMware Identity Manager.

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
<b>Name</b>	Enter a unique name for the ThinApp collection.
<b>Connector</b>	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 <b>Host</b> 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
<b>Path</b>	<p>The path to the shared folder where the ThinApp packages' folders are located, in the UNC path format \\server\share\subfolder. For example: \\DirectoryHost\ThinAppFileShare. 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>
<b>Enable Account Based Access</b>	<p>Account based access is required in the following cases:</p> <ul style="list-style-type: none"> <li>■ For NetApp storage systems and other brands of DFS network shares</li> <li>■ If you are using HTTP download deployment mode</li> <li>■ If you want users to be able to use their entitled ThinApp packages on non-domain-joined Windows systems</li> </ul>
<b>Share User</b>	<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>
<b>Share Password</b>	<p>The password associated with the <b>Share User</b> user account.</p>
<b>Sync Frequency</b>	<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 <b>Manual</b>, you must click <b>Sync</b> 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>
<b>Activation Policy</b>	<p>Select how you want to make resources in this collection available to users in the Workspace ONE portal and app. If you intend to set up an approval flow, select <b>User-Activated</b>, otherwise select <b>Automatic</b>.</p> <p>With both the <b>User-Activated</b> and <b>Automatic</b> options, the resources are added to the Catalog page. Users can use the resources from the Catalog page or move them to the Bookmarks 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 <b>Users &amp; Groups</b> 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 VMware Identity Manager.



## Results

VMware Identity Manager 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 VMware Identity Manager Desktop application installed on their Windows systems.

## What to do next

Entitle groups and users to ThinApp packages.

# Entitle Users and Groups to ThinApp Packages

You can entitle users and groups to Windows applications that are captured as ThinApp packages.

You can only entitle VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager. When the ThinApp packages are synced to your catalog, you can entitle them to your users and groups.

## Procedure

- 1 Log in to the VMware Identity Manager console.

## 2 Entitle users to a ThinApp package.

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

### Results

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

### What to do next

Verify that the VMware Identity Manager Desktop application is installed on users' Windows systems.

## Distributing and Managing ThinApp Packages with VMware Identity Manager

Before your VMware Identity Manager users can run their ThinApp packages that are registered to them using VMware Identity Manager, those users must have the VMware Identity Manager 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. VMware Identity Manager can distribute and manage ThinApp packages that are compatible with VMware Identity Manager.

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 VMware Identity Manager.
- 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 VMware Identity Manager Desktop application whether that ThinApp package is registered on that Windows desktop for that user. The locally installed VMware Identity Manager Desktop application determines whether that application is registered for that user without communicating with VMware Identity Manager. If the application is registered on that Windows desktop for that user, the VMware Identity Manager Desktop application checks to see when it last synced with VMware Identity Manager. If the VMware Identity Manager 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 VMware Identity Manager Desktop application is installed, and because the `hws-desktop-client.exe` process is running if the VMware Identity Manager Desktop application is running on that system, the VMware Identity Manager Desktop application must be installed on the Windows system to run ThinApp packages that are distributed and managed by VMware Identity Manager.

## Deploying the VMware Identity Manager Desktop Application To Use ThinApp Packages

The VMware Identity Manager 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 VMware Identity Manager Desktop application by double-clicking its installer EXE file, see the *VMware Identity Manager User Guide*.

The configuration of the installed application determines how a ThinApp package that is distributed by VMware Identity Manager is deployed to that Windows system. By default, when the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager Desktop application on the Windows endpoint determines whether a ThinApp package that is distributed using VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager Desktop application synchronizes with VMware Identity Manager, 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 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 VMware Identity Manager 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"> <li>■ Horizon desktops, either stateless or persistent, with excellent connectivity to the file share on which the ThinApp packages reside.</li> <li>■ 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.</li> </ul> <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"> <li>■ Persistent Horizon desktops</li> <li>■ LAN-connected desktops that are periodically offline</li> <li>■ A LAN with poor network latency</li> </ul> <p>VMware Identity Manager 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 VMware Identity Manager is configured for account-based access to the ThinApp packages' network share.</p> <p>When the AUTO_TRY_HTTP option is enabled and VMware Identity Manager 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 VMware Identity Manager 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><b>Important</b> If VMware Identity Manager 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 VMware Identity Manager console when you configure access from VMware Identity Manager 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 *VMware Identity Manager Installation and Configuration*.

## Offline Grace Period and ThinApp Packages

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 VMware Identity Manager.

ThinApp packages are virtualized Windows applications, and VMware Identity Manager can distribute these applications to Windows systems. When VMware Identity Manager 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 VMware Identity Manager, 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 VMware Identity Manager 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 VMware Identity Manager Desktop application syncs with VMware Identity Manager 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 VMware Identity Manager at any time within a 30-day timespan, the application can sync with VMware Identity Manager and virtualized applications can run.

However, if the Windows system has no network connectivity to connect to VMware Identity Manager, the application cannot sync with VMware Identity Manager. 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 VMware Identity Manager

After adding a ThinApp package to your organization's catalog and entitling your VMware Identity Manager 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 VMware Identity Manager. This ThinApp update mechanism is different from other update mechanisms for ThinApp packages used outside of a VMware Identity Manager environment. The updated ThinApp package must have been updated with this mechanism for you to be able to deploy the updated package in VMware Identity Manager and have users automatically see the newer version.

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

### AppID

The unique identifier for the ThinApp package in VMware Identity Manager. All entry points (executables) for the package's application are assigned the same AppID. After a ThinApp package is synced to your organization's VMware Identity Manager 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
```

VMware Identity Manager considers any ThinApp package with the same AppID to be versions of the same application.

### VersionID

The version number of the ThinApp package. VMware Identity Manager 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 VMware Identity Manager*. When VMware Identity Manager 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. VMware Identity Manager 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 VMware Identity Manager.

---



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 Managed ThinApp Package

Updating a ThinApp package that is already managed by VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager.

### Prerequisites

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

### What to do next

Your VMware Identity Manager 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 VMware Identity Manager console.

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

To ensure that VMware Identity Manager 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 VMware Identity Manager. The AppID and VersionID values are displayed on pages in the ThinApp package's resource page in the VMware Identity Manager console.

### Procedure

- 1 In the VMware Identity Manager 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 VMware Identity Manager 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

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 VMware Identity Manager. For information about specific ThinApp versions, see the *VMware Product Interoperability Matrixes* at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php).

## Procedure

- ◆ Using a version of the ThinApp program that is supported by VMware Identity Manager, create the updated ThinApp package using one of the available methods.

Option	Description
<p><b>Recapture using Setup Capture.</b></p>	<p>Use this method when the project folder for the existing ThinApp package managed by VMware Identity Manager is unavailable. To create an updated package with Setup Capture, you need only the following items:</p> <ul style="list-style-type: none"> <li>■ The application executables from the existing ThinApp package</li> <li>■ The application installer</li> <li>■ Setup Capture and the ThinApp program at a version supported by VMware Identity Manager.</li> </ul> <p>During the capture process, select to manage the package with VMware Identity Manager 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 AppID or VersionID 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 AppID of the prior package and reuses it for the updated package. The process also provides an incremented VersionID for the updated package, and assigns the same InventoryName.</p>
<p><b>Update the Package.ini file manually and then rebuild the package.</b></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 relink 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 Package.ini parameter that you want to set.</p> <p>To mark the new package as an update, edit the following VMware Identity Manager parameters in the [Build Options] section of the Package.ini file:</p> <ul style="list-style-type: none"> <li>■ Set the AppID parameter to match the AppID value of the currently managed ThinApp application. You cannot reuse a value of genid for AppID, because then a new AppID value will be generated for the updated package and VMware Identity Manager will not recognize the new package as an update to the existing one.</li> <li>■ Increment the value of the VersionID parameter to a higher integer than the currently managed ThinApp package. If there is no VersionID parameter set for the currently managed package, its value is 1 by default, and you would add a line for the VersionID parameter to Package.ini and set it to a value of 2 (VersionID = 2).</li> <li>■ Make sure the InventoryName parameter value matches the InventoryName value of the currently managed package. The InventoryName values for the current package and the updated package must be identical.</li> </ul>
<p><b>Use the relink -h command with the AppID and VersionID options.</b></p>	<p>Use this method in one of the following situations:</p> <ul style="list-style-type: none"> <li>■ You do not have the project folder for the application.</li> </ul>

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 VMware Identity Manager environment, and the only remaining steps are to enable the updated package for VMware Identity Manager and place it in the network share used by VMware Identity Manager.</li> <li data-bbox="635 359 1428 447">■ You are updating the package only to update the ThinApp runtime for the package to incorporate bug fixes available in that new ThinApp version.</li> </ul> <p data-bbox="635 462 1428 646">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 VMware Identity Manager. The final stage of updating the application is to enable it for VMware Identity Manager. 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="635 667 1428 730"><b>Note</b> The ThinApp runtime is always updated when you run the <code>relink -h</code> command on a ThinApp package.</p> <hr/> <p data-bbox="635 751 1428 814">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="635 825 1428 909">When the existing ThinApp package is already enabled for use by VMware Identity Manager, you can run the following command to reuse the package's existing AppID and increment the VersionID:</p> <div data-bbox="643 919 1428 972" style="background-color: #f0f0f0; padding: 5px;"> <pre data-bbox="651 930 1420 961">relink -h -VersionID + executable-folder/*.*</pre> </div> <p data-bbox="635 993 1428 1056">Where <i>executable-folder</i> is a folder containing the executables of the ThinApp package you want to update.</p> <hr/> <p data-bbox="635 1077 1428 1297"><b>Important</b> 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 VMware Identity Manager 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 1318 1428 1402">Other use cases for the <code>relink</code> command, including enabling a ThinApp package for use in a VMware Identity Manager environment, are covered in the VMware knowledge base article at <a href="http://kb.vmware.com/kb/2021928">http://kb.vmware.com/kb/2021928</a>.</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.

## 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, VMware Identity Manager 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 VMware Identity Manager. 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 VMware Identity Manager with the network share from the Packaged Apps - ThinApp page of the VMware Identity Manager console.

When VMware Identity Manager 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. VMware Identity Manager 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.

## Make Existing ThinApp Packages Compatible with VMware Identity Manager

You can convert a ThinApp package from one that is not compatible with VMware Identity Manager to one that VMware Identity Manager 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 VMware

Identity Manager parameters, or recapture the Windows application with the appropriate VMware Identity Manager settings selected in the ThinApp Setup Capture program.

---

**Note** A ThinApp package that is compatible with VMware Identity Manager can only be used for a VMware Identity Manager deployment. Only VMware Identity Manager users who have the VMware Identity Manager 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 VMware Identity Manager. Because the DLL is installed with the VMware Identity Manager Desktop application, such ThinApp packages can only be run on Windows systems on which the VMware Identity Manager 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 VMware Identity Manager and that you can make subfolders and copy files to it.

## Procedure

- ◆ Using a version of the ThinApp program that is supported by VMware Identity Manager, create a compatible ThinApp package using one of the available methods.

Option	Description
<p><b>Use the <code>relink -h</code> command.</b></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"> <li>■ You cannot use the rebuild method because you do not have the project folder.</li> <li>■ Using Setup Capture to recapture the application would take too long.</li> <li>■ You do not have the application installer that is required for recapturing with Setup Capture.</li> </ul> <p><b>Note</b> 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 data-bbox="630 861 1434 919">relink -h executable-folder/*.*</pre> <p>Where <code>executable-folder</code> is a folder containing the executables of the ThinApp package you want to update..</p> <p><b>Important</b> 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 VMware Identity Manager 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 <a href="http://kb.vmware.com/kb/2021928">http://kb.vmware.com/kb/2021928</a>.</p>
<p><b>Update the <code>Package.ini</code> file manually with the necessary parameters, and then rebuild the package.</b></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 <code>Package.ini</code> parameter that you want to set.</p> <p>In the [Build Options] section of the <code>Package.ini</code> file, add the following parameters:</p> <pre data-bbox="630 1680 1434 1808">;--- VMware Identity Manager Parameters --- AppID=genid NotificationDLLs=hzntaploginlogin.dll</pre>

Option	Description
	<p>hzntapplugin.dll is the DLL that the ThinApp runtime calls to verify the VMware Identity Manager user's entitlement to use the virtualized application.</p> <p>You can optionally include the <code>HorizonOrgURL</code> parameter and set it to your VMware Identity Manager fully qualified domain name. See <i>VMware Identity Manager Installation and Configuration</i>.</p>
<p><b>Recapture using Setup Capture, and select the necessary VMware Identity Manager settings.</b></p>	<p>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 VMware Identity Manager during the capture process. See the <i>ThinApp User's Guide</i> for details on the capture process.</p>

## Results

You have a set of files (EXE files, and optionally DAT files) for a ThinApp package that VMware Identity Manager 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 VMware Identity Manager Manages](#).

# Change the ThinApp Packages Share Folder

After you configure VMware Identity Manager 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 VMware Identity Manager 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 [VMware Identity Manager Requirements for ThinApp Packages and the Network Share Repository](#).

## Procedure

- 1 Log in to the VMware Identity Manager 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

The default access policy set applies to all applications and desktops in your 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.

For detailed information on access policies and how they are applied, see the *VMware Identity Manager Administration Guide*.

### Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
  - a In the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager Desktop

# 7

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

The VMware Identity Manager 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 VMware Identity Manager Desktop application on the Windows endpoint determines whether a ThinApp package that is distributed using VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 [ThinApp Packages Fail to Launch from the User Portal](#).

---

This chapter includes the following topics:

- [Command-Line Installer Options for VMware Identity Manager Desktop](#)
- [Install the VMware Identity Manager Desktop Application with Identical Settings to Multiple Windows Systems](#)

- [Add VMware Identity Manager Desktop Installer Files to VMware Identity Manager Virtual Appliances](#)
- [Using the Command-Line hws-desktop-ctrl.exe Application](#)

## Command-Line Installer Options for VMware Identity Manager Desktop

You can set various options for the VMware Identity Manager Desktop application when you run its installer program using the command line or a deployment script.

### Available Command-Line Options for the VMware Identity Manager 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 <a href="#">Windows Installer documentation</a> .
/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 VMware Identity Manager 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 %TEMP% is used.
/x		Unpacks the installer into the %TEMP% 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_SERVER	Host name or URL of the VMware Identity Manager service	<p>Provides the VMware Identity Manager service host name or URL, to allow the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager.</p> <ul style="list-style-type: none"> <li> <b>COPY_TO_LOCAL:</b> 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><b>Important</b> COPY_TO_LOCAL mode requires the ThinApp share to be reachable from the user's Windows system.</p> </li> <li> <b>HTTP_DOWNLOAD:</b> 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 VMware Identity Manager Desktop application uses the user's VMware Identity Manager system account to authenticate to VMware Identity Manager to obtain the list of the user's entitled packages to download. The share user account provided in the VMware Identity Manager console for enabling account-based access to the ThinApp packages' network share is the account used by VMware Identity Manager to access the ThinApp packages from the repository. That share user account for VMware Identity Manager 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 VMware Identity Manager 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           </li> </ul>

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

Key	Value	Description
		<p>to which the 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.</p> <hr/> <p><b>Important</b> For the HTTP_DOWNLOAD option to work, the ThinApp packages integration in VMware Identity Manager must be configured for account-based access. See <i>VMware Identity Manager Installation and Configuration</i>.</p> <hr/> <p><b>Important</b> For VMware Identity Manager 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 VMware Identity Manager or enable TLS 1.1 or 1.2 in the Windows 2008 R2 or Windows 7 system. To enable TLS 1.0 in VMware Identity Manager, see <a href="#">Knowledge Base article 2144805</a>. To enable TLS 1.1 or 1.2 on the Windows system, see the Microsoft documentation at <a href="https://support.microsoft.com/en-us/kb/3140245">https://support.microsoft.com/en-us/kb/3140245</a>.</p> <hr/> <p><b>Important</b> HTTP_DOWNLOAD mode requires the IDP URL to be reachable from the user's Windows system.</p> <hr/> <ul style="list-style-type: none"> <li>■ <b>RUN_FROM_SHARE:</b> 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.</li> </ul> <hr/> <p><b>Important</b> RUN_FROM_SHARE mode requires the ThinApp share to be reachable from the user's Windows machine.</p> <hr/> <p>The default value is COPY_TO_LOCAL.</p> <p>For all of the modes, the network share must have the appropriate file and sharing permissions configured. See <i>VMware Identity Manager Installation and Configuration</i>.</p> <hr/> <p><b>Important</b> When installing VMware Identity Manager Desktop in floating Horizon desktops, use the RUN_FROM_SHARE option to avoid copying the ThinApp packages into those stateless Horizon desktop systems.</p> <hr/> <p>When the VMware Identity Manager 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:</p> <ul style="list-style-type: none"> <li>■ The RUN_FROM_SHARE option</li> </ul>

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

Key	Value	Description
		<ul style="list-style-type: none"> <li>■ The COPY_TO_LOCAL option, without also having the AUTO_TRY_HTTP option enabled and account-based access configured in VMware Identity Manager</li> </ul>
POLLING_INTERVAL	<i>Frequency in seconds</i>	<p>Sets the frequency, in seconds, of synchronization between the installed VMware Identity Manager Desktop application and VMware Identity Manager 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>Enables or disables the automatic update check and download activity. If enabled, the installed VMware Identity Manager Desktop application automatically checks if a newer application is available for download. If a newer version is available, the VMware Identity Manager Desktop application automatically downloads and updates itself to the newer version. This option is enabled by default.</p> <p>Set the value of this variable to 0 to disable automatic update. 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><b>Note</b> If you specify a shared cache, the VMware Identity Manager 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 VMware Identity Manager 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	<p>When the VMware Identity Manager Desktop application is installed with the COPY_TO_LOCAL option and account-based access is configured for VMware Identity Manager, 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 to disable automatically trying the HTTP protocol for the download.</p> <hr/> <p><b>Important</b> For the AUTO_TRY_HTTP option to work, the ThinApp packages integration in VMware Identity Manager must be configured for account-based access. See <a href="#">VMware Identity Manager Requirements for ThinApp Packages and the Network Share Repository</a>.</p>
INSTALL_MODULES	thinapps	<p>A comma-separated list specifying which modules to install. Currently, only the thinapp module is available.</p>
MIGRATE_ACTION	One of the following: MOVE COPY NONE	<p>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.</p> <p>The following settings are moved, copied, or ignored, depending on the value you specify.</p> <p><b>Cached ThinApp Packages</b></p> <p>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.</p> <hr/> <p><b>Important</b> Properties set for VMware Identity Manager 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.</p>

## Example: Using the VMware Identity Manager Desktop Command-Line Installer Options

If your VMware Identity Manager instance has a URL of `https://identitymanagerFQDN`, and VMware Identity Manager is configured for account-based access to your ThinApp packages' network share, and you want to silently install the VMware Identity Manager Desktop application to multiple desktops of that VMware Identity Manager 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. VMware Identity Manager is appropriately configured for account-based access to the ThinApp packages' network share.
- The clients check for new packages and entitlements with VMware Identity Manager 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 the name of your downloaded VMware Identity Manager Desktop installer.

## Install the VMware Identity Manager Desktop Application with Identical Settings to Multiple Windows Systems

To deploy the VMware Identity Manager 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 VMware Identity Manager Desktop application using the command-line installation options.

**Important** Error messages do not appear on screen when you deploy VMware Identity Manager 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. For a description of settings to use for non-persistent, also known as floating or stateless, Horizon desktops, see [Reducing Resource Usage and Increasing Performance of VMware Identity Manager](#).

### Prerequisites

- Verify that the Windows systems are running Windows operating systems that are supported for the version of the VMware Identity Manager Desktop application you are installing. See the *VMware Identity Manager User Guide* or 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 the [Command-Line Installer Options for VMware Identity Manager](#).

### Procedure

- 1 Obtain the VMware Identity Manager 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 VMware Identity Manager system's download page. If you have set up your VMware Identity Manager 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.

- 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 VMware Identity Manager 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 VMware Identity Manager 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-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 that of your downloaded file.

- Run the deployment script against the Windows systems.

### Results

If the silent installation is successful, the VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager Desktop is properly installed on the Windows systems by trying some of the typical user tasks.

## Add VMware Identity Manager Desktop Installer Files to VMware Identity Manager Virtual Appliances

When new versions of VMware Identity Manager Desktop are released, you copy and install the zip file from the VMware Downloads page to each VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager virtual appliances during a maintenance window since the virtual appliance is restarted and this might interrupt user access.

## Procedure

1 Download the VMware Identity Manager Desktop zip file from the My VMware Downloads page to a computer that can access the VMware Identity Manager 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-nnnnnn.zip
```

This script automatically unzips the file and copies the VMware Identity Manager 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 VMware Identity Manager virtual appliance in your environment.

Users can download the Identity Manager Desktop application from their VMware Identity Manager accounts or via the download link, <https://IdentityManagerFQDN/download>. Users' Identity Manager Desktop applications are automatically updated when they download the new version.

## Using the Command-Line `hws-desktop-ctrl.exe` Application

The VMware Identity Manager 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 VMware Identity Manager Desktop application installs `hws-desktop-ctrl.exe` in the `HorizonThinApp` folder in the Windows directory location where the VMware Identity Manager 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 VMware Identity Manager Desktop application. Any newly entitled or updated ThinApp packages are synced.
<code>hws-desktop-ctrl.exe set InstallMode=<i>install_mode</i></code>	<p>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.</p> <p>Available values for <i>install_mode</i> are:</p> <ul style="list-style-type: none"> <li>■ CopyToLocal</li> <li>■ RunFromShare</li> <li>■ HttpDownload</li> </ul>
<code>hws-desktop-ctrl.exe authorize guid=<i>ThinApp_GUID</i> path=<i>package_path</i></code>	<p>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</p> <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 VMware Identity Manager console.</p>
<code>hws-desktop-ctrl.exe quit</code>	This command tells the VMware Identity Manager Desktop application to exit cleanly.
<code>hws-desktop-ctrl.exe launch app=<i>package_path</i> url=<i>launch_url</i></code>	<p>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 VMware Identity Manager protocol URL for that package, in the form <code>horizon://package_path</code>. An example is</p> <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



You can integrate your Citrix deployment with VMware Identity Manager to provide Workspace ONE users access to Citrix-published resources.

This chapter includes the following topics:

- [Overview of Citrix-Published Resources Integration](#)
- [Components Required for Citrix Integration](#)
- [High-level Integration Design](#)
- [Prerequisites for Citrix Integration](#)
- [Configuring Citrix Server Farms in VMware Identity Manager](#)
- [Configuring Citrix Resource Launch in VMware Identity Manager](#)
- [Configuring VMware Identity Manager Settings for Citrix Integration](#)
- [Upgrade Impact on Citrix-Published Resources Integration](#)

## Overview of Citrix-Published Resources Integration

You can provide Workspace ONE users access to Citrix-published resources by integrating your Citrix deployment with VMware Identity Manager. Citrix-published resources include applications and desktops within 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 administrative interface. You also set user and group entitlements in the Citrix interface, not in the VMware Identity Manager service. You must sync these users and groups to the VMware Identity Manager service from Active Directory before integrating with the Citrix server farms.

To integrate Citrix server farms with VMware Identity Manager, you create one or more virtual app collections in the VMware Identity Manager 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 VMware Identity Manager service.

After you integrate the Citrix server farms, you can view the synced resources and entitlements in the VMware Identity Manager console. You can also edit ICA session settings, such as the settings that control resolution or compression. You can configure the settings globally for all the Citrix resources in the VMware Identity Manager catalog, or for individual Citrix resources.

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

---

**Note** VMware Identity Manager supports Citrix deployments that include Citrix NetScaler.

---

## Supported Versions

- VMware Identity Manager supports Citrix XenApp 6.0 and 6.5, XenApp and XenDesktop 7.x, and Citrix Virtual Apps and Desktops 7 1808 and 1912.

---

**Note** Beginning with VMware Identity Manager 3.3, XenApp 5.x is no longer supported.

---

- VMware Identity Manager supports Citrix StoreFront API 2.6 and later.
- Supported operating systems for the Integration Broker, the VMware Identity Manager component that communicates with the Citrix server farm, are Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016.
- Integration Broker version requirements:

VMware Identity Manager or Connector Version	Integration Broker Version Supported
VMware Identity Manager 19.03	19.03
VMware Identity Manager Connector 19.03.0.0	19.03
VMware Identity Manager 3.3	3.3
VMware Identity Manager Connector 2018.8.1.0 (connector released with VMware Identity Manager 3.3)	3.3
VMware Identity Manager 3.2	3.2
VMware Identity Manager Connector 2018.1.1.0 (connector released with VMware Identity Manager 3.2)	3.2
VMware Identity Manager 3.1	3.1
VMware Identity Manager Connector 2017.12.1.0 (connector released with VMware Identity Manager 3.1)	3.1
VMware Identity Manager 3.0	3.0
Mware Identity Manager Connector 2017.8.1.0 (connector released with VMware Identity Manager 3.0)	3.0

---

VMware Identity Manager or Connector Version	Integration Broker Version Supported
VMware Identity Manager 2.9.1 or earlier	2.9.1 or earlier
VMware Identity Manager Connector 2.9.1 or earlier	2.9.1 or earlier

**Note** To use the Citrix StoreFront API, Integration Broker 2.9.1 or later is required. For XenApp or XenDesktop 7.x, Integration Broker 2.6 or later is required. To use the NetScaler feature, Integration Broker 2.4 or later is required.

**Note** Using the latest available version of VMware Identity Manager and its components is recommended.

## Supported Authentication Methods

VMware Identity Manager only supports user name and password authentication on the XenApp server or NetScaler server. It does not support other authentication methods such as the following:

- Smart Card
- HTML 5
- 2 factor authentication
- SAML authentication (Citrix FAS)

## Supported Features

VMware Identity Manager supports the following XenApp and XenDesktop features.

- Application and desktop launch with Citrix StoreFront API 2.6 and later
- Application group functionality

VMware Identity Manager supports the application group feature introduced in XenApp and XenDesktop 7.9. Application groups are a logical grouping of applications and desktops, and entitlements can be provided at the application group level.

- External launch with NetScaler
- 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 VMware Identity Manager.

- Limiting visibility for an application

This feature sets the visibility for an application. VMware Identity Manager 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

VMware Identity Manager 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 VMware Identity Manager.

## Components Required for Citrix Integration

To integrate a Citrix deployment with the VMware Identity Manager service, you need the following components.

- A VMware Identity Manager instance installed on premises.
- An Integration Broker instance installed on a supported Windows server on premises. The Integration Broker, a component of VMware Identity Manager, is the component that communicates with Citrix server farms.

You can download the Integration Broker from <https://my.vmware.com>.

- A Citrix deployment on premises.

While deploying the components, ensure that you meet these requirements:

- The VMware Identity Manager service must be able to communicate with the Integration Broker. If you deploy multiple instances of the service appliance, ensure that all of them can communicate with the Integration Broker.
- The Integration Broker must be able to communicate with the Citrix server farm.

---

**Note** Using the latest available version of VMware Identity Manager and its components is recommended.

---

## High-level Integration Design

VMware Identity Manager uses the Integration Broker and other components to synchronize Citrix-published resources to VMware Identity Manager and to launch the resources from the Workspace ONE portal or app.

## Synchronization of Citrix-published Resources and Entitlements

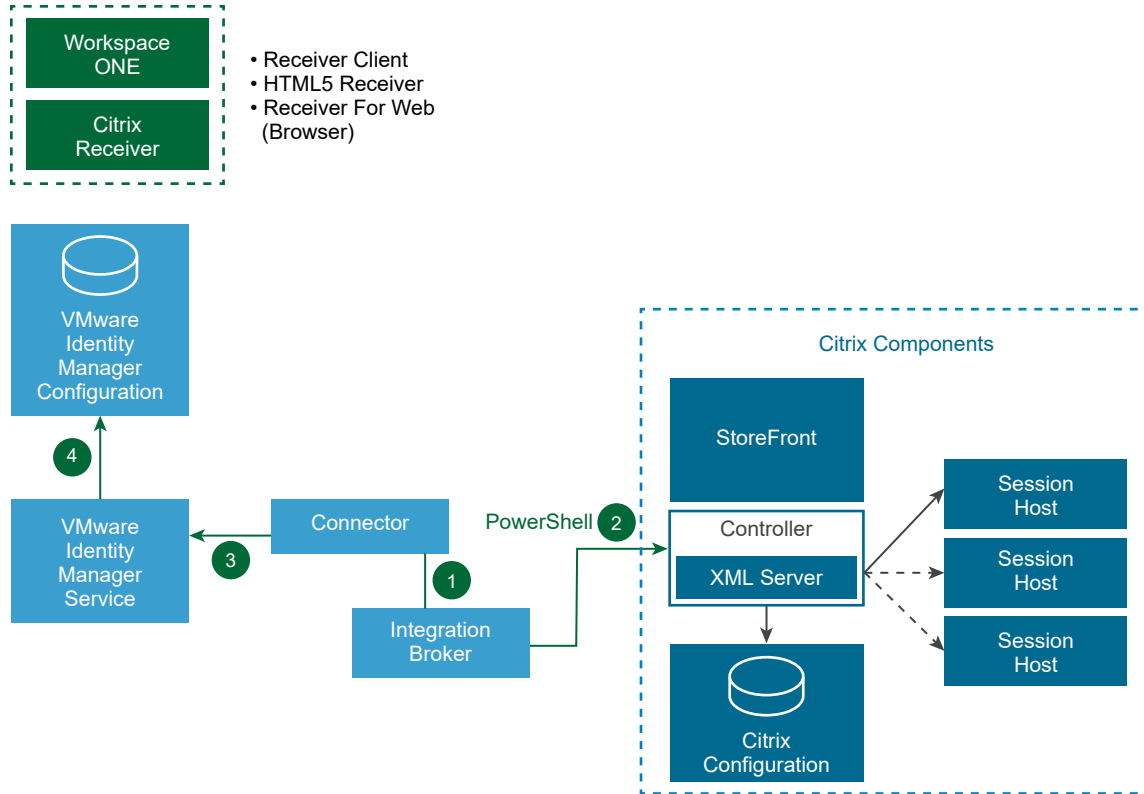
VMware Identity Manager synchronizes Citrix-published applications and desktops, and user entitlements, from the Citrix server farm to the VMware Identity Manager service. You can set a sync schedule to sync the resources and entitlements at regular intervals.

The Citrix farm is the single source of truth for all supported operations in VMware Identity Manager. 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 VMware Identity Manager after a sync.

## Synchronization Architecture Diagram

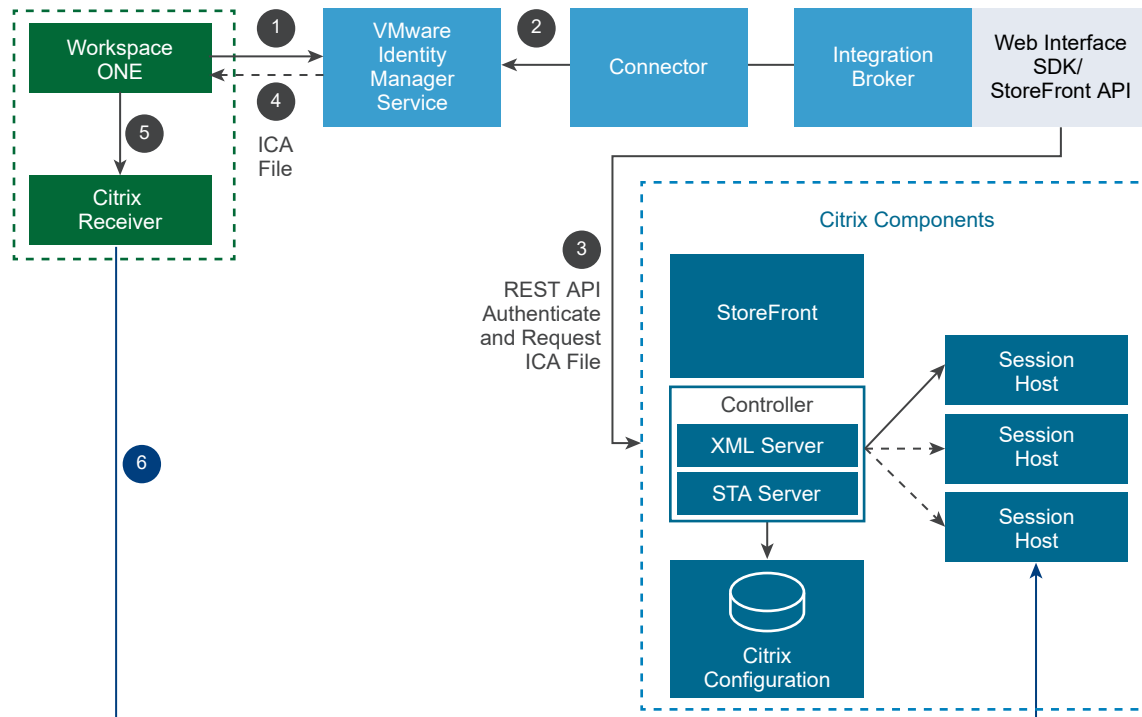


- 1 The VMware Identity Manager connector connects with the Integration Broker and requests application, delivery group, and entitlements information.
- 2 The Integration Broker fetches the resources and entitlements information from the Citrix XML server.
- 3 The connector compares the new information with the existing resources and entitlements information and sends the differences to the VMware Identity Manager service.
- 4 The VMware Identity Manager service stores the results in the VMware Identity Manager database.

## Launch of Citrix-published Applications and Desktops

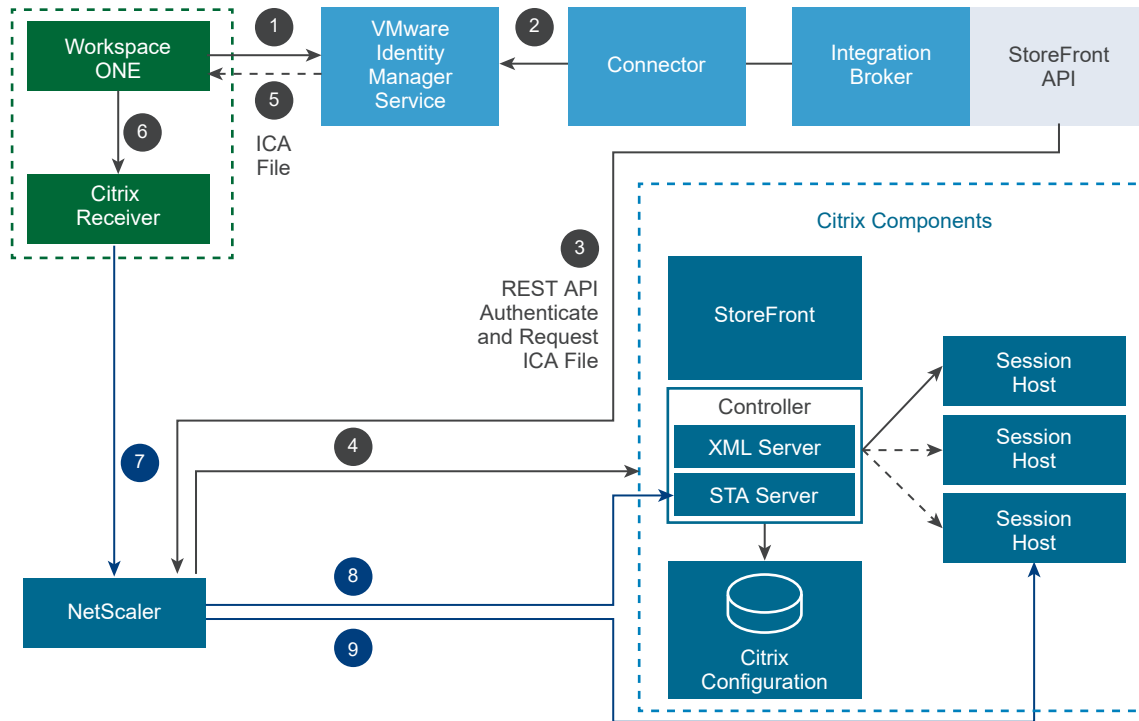
VMware Identity Manager uses the Integration Broker component and the Citrix Web Interface SDK or Citrix StoreFront REST API to launch Citrix-published applications from the Workspace ONE portal or app. You can configure internal and external access to the Citrix-published resources. End users must install Citrix Receiver on their systems or devices to launch the applications and desktops.

## Launch Architecture Diagram (Internal Access)



- 1 A user launches a Citrix-published application or desktop from the Workspace ONE portal or app.
- 2 The request goes to the VMware Identity Manager service, connector, and Integration Broker.
- 3 The Integration Broker communicates with the Citrix server farm through the Web Interface SDK or StoreFront REST API to authenticate and request the ICA file.
- 4 The ICA file is retrieved and passed to the Workspace ONE portal or app.
- 5 The ICA file is passed to the Citrix Receiver.
- 6 The Citrix Receiver launches the application or desktop.

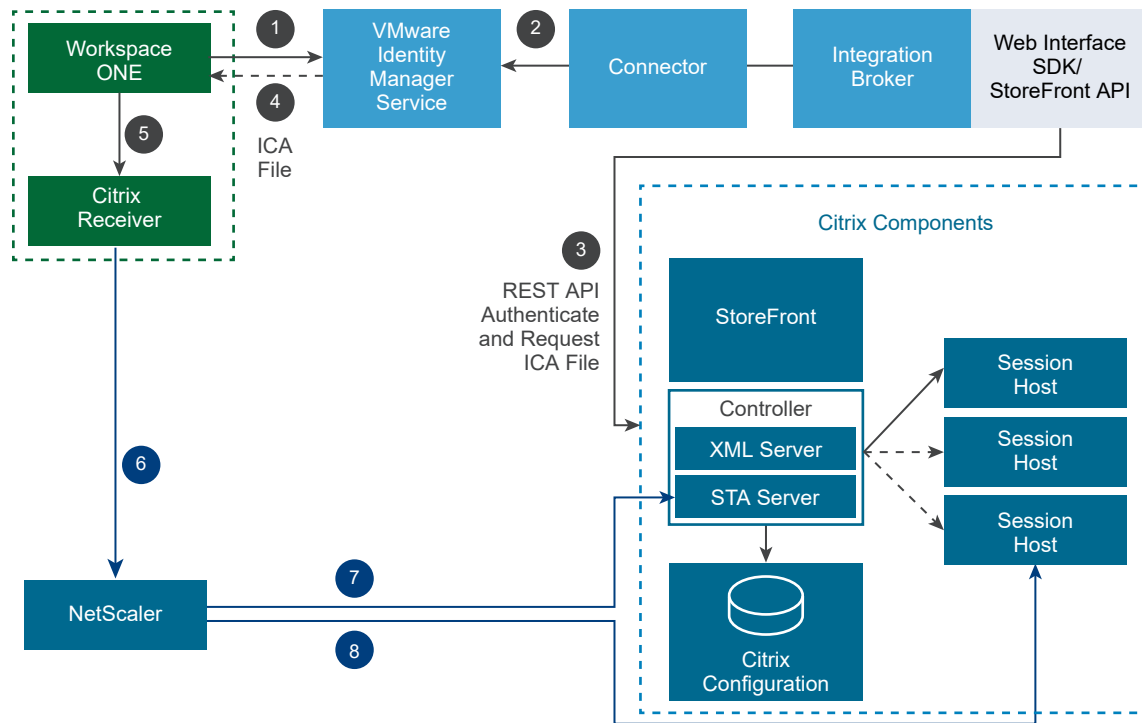
## Launch Architecture Diagram (External Access with StoreFront)



- 1 A user launches a Citrix-published application or desktop from the Workspace ONE portal or app.
- 2 The request goes to the VMware Identity Manager service, connector, and Integration Broker.
- 3 To communicate with the Citrix server farm to authenticate and request the ICA file, the Integration Broker 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 Workspace ONE portal or app.
- 6 The ICA file is passed to the Citrix Receiver.
- 7 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 the Citrix VDA server. In version 6.5, it is the Citrix Worker server.

## Launch Architecture Diagram (External Access with Web Interface SDK)



- 1 A user launches a Citrix-published application or desktop from the Workspace ONE portal or app.
- 2 The request goes to the VMware Identity Manager service, connector, and Integration Broker.
- 3 The Integration Broker communicates with the Citrix server farm through the Web Interface SDK to authenticate and request the ICA file.
- 4 The ICA file is retrieved and passed to the Workspace ONE portal or app.
- 5 The ICA file is passed to the Citrix Receiver.
- 6 Citrix Receiver communicates with Netscaler.
- 7 NetScaler communicates with the Citrix STA server with the STA ticket and gets the Citrix session server information.
- 8 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 the Citrix VDA server. In version 6.5, it is the Citrix Worker server.

## Using StoreFront REST API or Web Interface SDK for Launch

The Integration Broker can use the Citrix Web Interface SDK and the Citrix StoreFront REST API to communicate with your Citrix deployment to launch applications or desktops. When the StoreFront REST API is used, the Integration Broker acts like a REST client. The Web Interface SDK and the StoreFront REST API are used to authenticate with and generate the ICA file from the Citrix deployment.

You can specify which option to use by selecting the Use StoreFront or Use Web Interface SDK option in the Citrix configuration page in the VMware Identity Manager console.

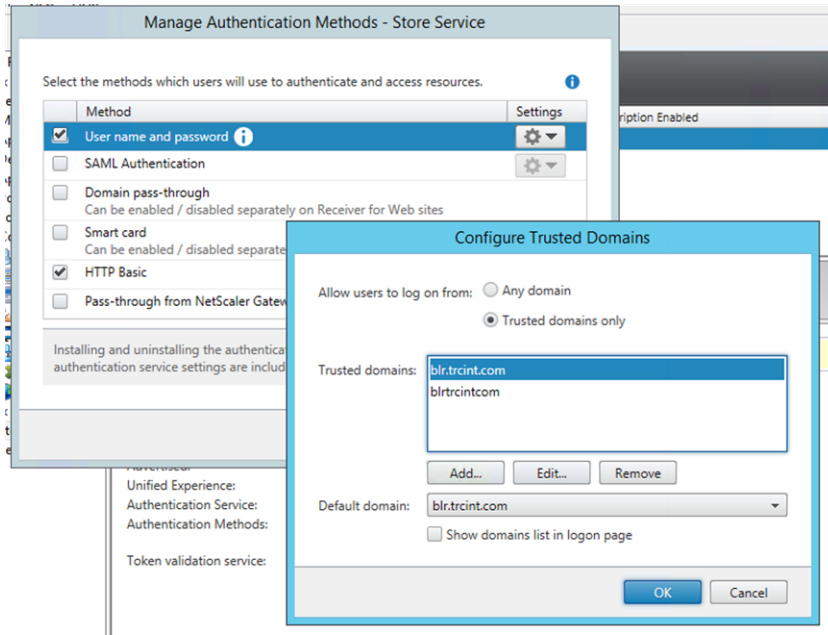
An Integration Broker instance can use both the Web Interface SDK and the StoreFront REST API. If you want to communicate with one Citrix farm using the Web Interface SDK and another Citrix farm using the StoreFront REST API, make the appropriate selections for each.

To use the StoreFront REST API option, which is available from VMware Identity Manager (formerly called VMware Identity Manager) 2.9.1 onwards, ensure the following requirements are met.

- Use StoreFront API 2.6 or later.
- Install Integration Broker 2.9.1 or later.
- Ensure that StoreFront is supported by the XenApp or XenDesktop version you are using.
- Ensure that the Integration Broker can communicate with the StoreFront server.

When you enable the StoreFront REST API, the Integration Broker communicates with the StoreFront server to generate the ICA file.

- 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. VMware Identity Manager 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 installation.

## Supported Authentication Methods on Citrix Server

VMware Identity Manager only supports user name and password authentication on the XenApp server or NetScaler server. It does not support other authentication methods such as the following:

- Smart Card
- HTML 5
- 2 Factor Authentication
- SAML Authentication (Citrix FAS)

## Prerequisites for Citrix Integration

Before you configure Citrix server farm details in the VMware Identity Manager console, you must complete certain prerequisite tasks. You must deploy and configure the Integration Broker, a VMware Identity Manager component, on a supported Windows Server and set up Citrix PowerShell remoting to enable communication between the Integration Broker and the Citrix server farm.

The high-level tasks include the following:

- Prepare the Windows Server for the Integration Broker installation.
  - Add roles and features.
  - Install Microsoft J# 2.0 Redistributable Package.

Microsoft J# 2.0 is not required if you plan to use the StoreFront REST API instead of the Citrix Web Interface SDK to connect to the Citrix server farm.

- Install Integration Broker.
  - Download and install the Integration Broker.
  - Configure IIS Manager settings for the Integration Broker.
  - Set up HTTPS bindings for the Integration Broker.
- Set up Citrix PowerShell remoting to enable remote invocations between the Integration Broker server and the Citrix server farm.
  - Install Citrix PowerShell SDK on the Integration Broker server.
  - Enable PowerShell remoting on the Citrix servers (Citrix 6.0 only).
- Download and copy Citrix Web Interface SDK dll files.

Citrix Web Interface SDK is not required if you plan to use the StoreFront REST API to connect to the Citrix server farm.

You can watch the following video for an overview of the process.



Installing Integration Broker for Citrix Published Applications and Desktops  
[http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_integration\\_broker\\_citrix](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_integration_broker_citrix)

## About Deploying the Integration Broker

The Integration Broker is a VMware Identity Manager component that is used to communicate with the Citrix server farm. You install the Integration Broker on premises on a supported Windows server.

Follow these guidelines when you deploy the Integration Broker.

- You can install the Integration Broker on Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

**Table 8-1. Integration Broker Server Requirements**

Requirement	Notes
Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2 with dual core processor	
4 GB RAM	
30 GB	This includes the storage required for the Windows OS.

- Integration Broker version requirements:

VMware Identity Manager or Connector Version	Integration Broker Version Supported
VMware Identity Manager 19.03	19.03
VMware Identity Manager Connector 19.03.0.0	19.03

VMware Identity Manager or Connector Version	Integration Broker Version Supported
VMware Identity Manager 3.3	3.3
VMware Identity Manager Connector 2018.8.1.0 (connector released with VMware Identity Manager 3.3)	3.3
VMware Identity Manager 3.2	3.2
VMware Identity Manager Connector 2018.1.1.0 (connector released with VMware Identity Manager 3.2)	3.2
VMware Identity Manager 3.1	3.1
VMware Identity Manager Connector 2017.12.1.0 (connector released with VMware Identity Manager 3.1)	3.1
VMware Identity Manager 3.0	3.0
VMware Identity Manager Connector 2017.8.1.0 (connector released with VMware Identity Manager 3.0)	3.0
VMware Identity Manager 2.9.1 or earlier	2.9.1 or earlier
VMware Identity Manager Connector 2.9.1 or earlier	2.9.1 or earlier

**Note** To use the Citrix StoreFront REST API, Integration Broker 2.9.1 or later is required. For XenApp or XenDesktop 7.x, Integration Broker 2.6 or later is required. To use the NetScaler feature, Integration Broker 2.4 or later is required.

**Note** Using the latest available version of VMware Identity Manager and its components is recommended.

- The VMware Identity Manager connector must be able to communicate with the Integration Broker. If you set up multiple connector instances, ensure that all of them can communicate with the Integration Broker.

**Note** You must connect over SSL to any Integration Broker instance that is used for launch.

- A single Integration Broker instance can support multiple Citrix environments.
- If you are using the Windows version of the VMware Identity Manager connector, follow these guidelines.
  - Installing the Integration Broker and the VMware Identity Manager connector on different servers is recommended.
  - If you are installing the Integration Broker on the same server as the connector, ensure that the HTTP and HTTPS binding ports do not conflict with the ports used by the VMware Identity Manager Connector.

The VMware Identity Manager Connector always uses port 80. It also uses 443, unless a different port is configured during installation.



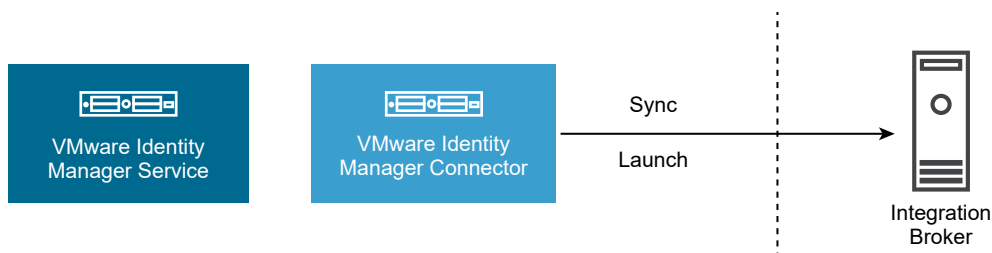
- A self-signed certificate is generated during the connector installation. If you are installing the Integration Broker on the same server as the connector, you can use this certificate. Install the certificate in the Microsoft store and use it for the HTTPS binding.
- Before you start, plan your deployment strategy. See [Integration Broker Deployment Models](#) for recommendations for common scenarios.

## Integration Broker Deployment Models

Deploy one or more instances of the Integration Broker, depending on your business needs. The following deployment models are based on common scenarios.

### Proof of Concept Environments

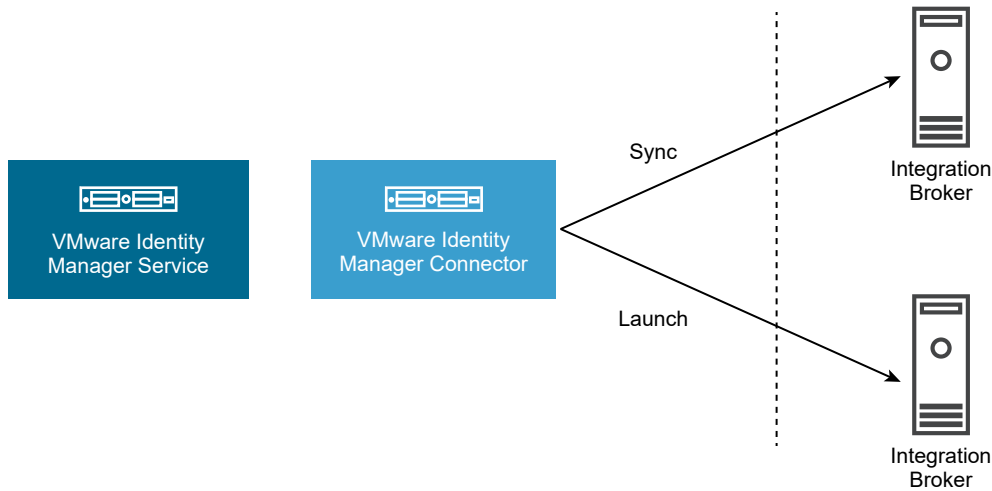
In proof of concept environments, where you are configuring only a few Citrix published applications in VMware Identity Manager to get familiar with the integration process and the end user experience, setting up a single Integration Broker instance is recommended. Select the same Integration Broker instance as the Sync Integration Broker and SSO Integration Broker in the virtual apps collection.



### Test Environments

In small test environments, where you want to test the entire flow including sync and launch, deploying two Integration Broker instances is recommended, one for syncing resources and entitlements and the other for launching resources. In this scenario, you typically integrate only a few applications and do not expect a large number of users to start applications concurrently.

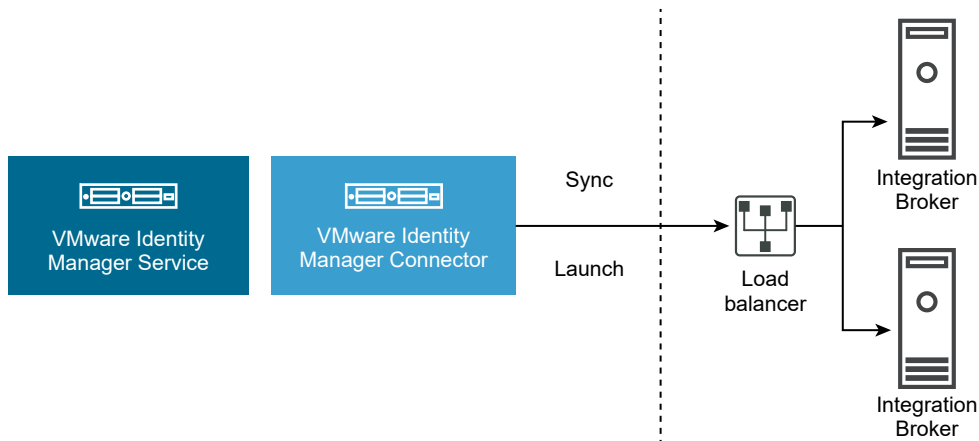
Select one of the instances as the Sync Integration Broker and the other as the SSO Integration Broker in the virtual apps collection.



### Production Environments

In production environments, setting up a cluster of Integration Broker instances behind a load balancer is recommended for high availability and load balancing purposes. If one of the Integration Broker instances is not available, sync and launch remain available as the requests are redirected to another instance in the cluster.

Enter the load balancer information in the Sync Integration Broker and SSO Integration Broker fields in the virtual apps collection.



### Large Scale Production Environments

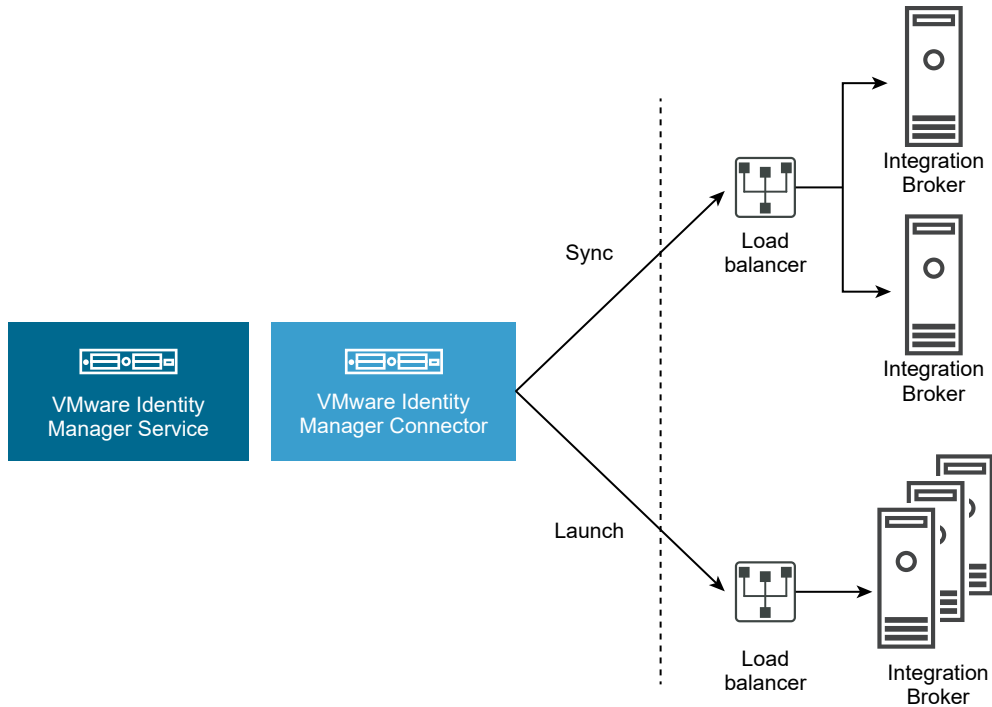
In large production environments that integrate a large number of applications and experience heavy traffic, setting up separate Integration Broker clusters for sync and launch is recommended. Set up each cluster behind a load balancer. This setup provides you the flexibility of increasing the number of instances based on specific needs. For example, if you experience delays because of a high number of concurrent launches, you can add more Integration Broker instances to the cluster used for launch.

Enter the appropriate load balancers in the Sync Integration Broker and SSO Integration Broker fields in the virtual apps collection.

---

**Note** For an Integration Broker instance that is used only for launch and not for sync, you do not need to set up Citrix PowerShell remoting. Also, if you use the StoreFront REST API to connect to the Citrix server farm, you do not need to download the Citrix Web Interface SDK.

---



## Prepare Windows Server for the Integration Broker Installation

Before you install Integration Broker, you must configure the Windows server.

The following operating systems are supported for the Integration Broker server.

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

---

**Note** Windows Server 2016 is supported in VMware Identity Manager 3.2.0.1 and later.

---

**Note** See the VMware Product Interoperability Matrixes at [http://www.vmware.com/resources/compatibility/sim/interop\\_matrix.php](http://www.vmware.com/resources/compatibility/sim/interop_matrix.php) for the latest information about supported versions.

---

## Add Windows Server Roles and Features (Windows Server 2012 R2, 2012, or 2008 R2)

Add the required roles, features, and role services in the Integration Broker server.

**Note** The steps in this procedure refer to the Windows Server 2012 R2 or Windows Server 2012 user interface. Where applicable, any differences for Windows Server 2008 R2 are noted.

To add roles and services on Windows Server 2016, see [Add Windows Server Roles and Features \(Windows Server 2016\)](#).

### Prerequisites

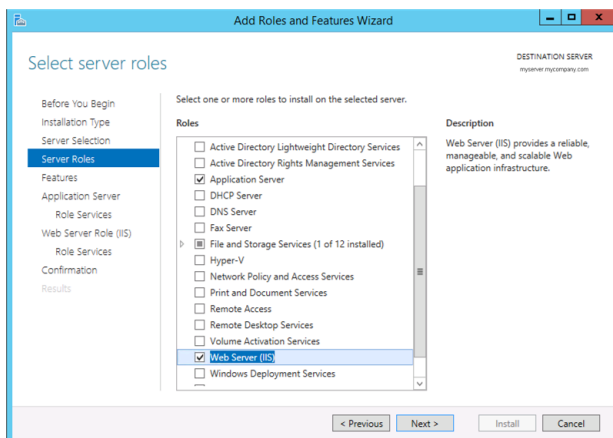
- Verify that Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 is installed with the latest updates. To check for updates, select **Control Panel > Windows Update**.
- Create an application pool, if necessary. You can use the default application pool or create an application pool that is dedicated to Integration Broker.

### Procedure

- 1 Select **Start > Server Manager**.
- 2 In Server Manager, select **Manage > Add Roles and Features**.
- 3 In the Add Roles and Features wizard, click **Next** until the **Server Roles** page appears.
- 4 Select the following roles, then click **Next**.

- Roles
- Application Server
  - File and Storage Services
  - Web Server (IIS)

**Note** When you select Web Server (IIS), a dialog box appears prompting you to confirm features that are required for Web Server (IIS). Verify that **Management Tools** is included, then click **Add Features**.



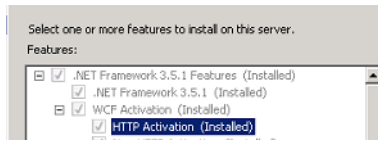
5 In the Features page, select the following features.

- Features
  - .NET Framework 3.5 Features
    - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
    - HTTP Activation

When you select HTTP Activation, a dialog box appears prompting you to confirm features that are required for HTTP Activation. Click **Add Features**.

**Note** On Windows Server 2008 R2, you select these options:

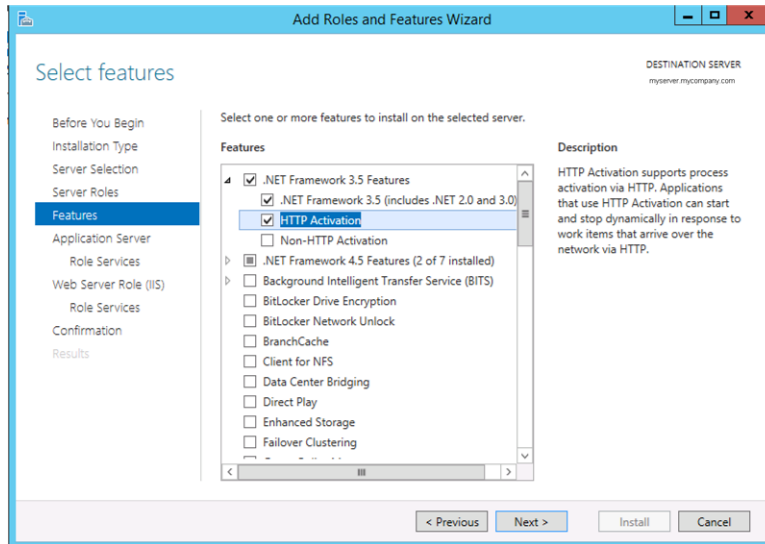
- .NET Framework 3.5 Features
  - .NET Framework 3.5
  - WCF Activation
    - HTTP Activation



- IIS Hostable Web Core
- Windows Process Activation Service
- WinRM IIS Extension

For example:

Figure 8-1. Windows Server 2012 R2



6 Click **Next**, then click **Next** again to display the Application Server Role Services page.

**7** In the Application Server Role Services page, select the following role services.

Application  
Server Role  
Services

**Application Server Role Services**

- .NET Framework 4.5 (do not change if preselected)
- Web Server (IIS) Support

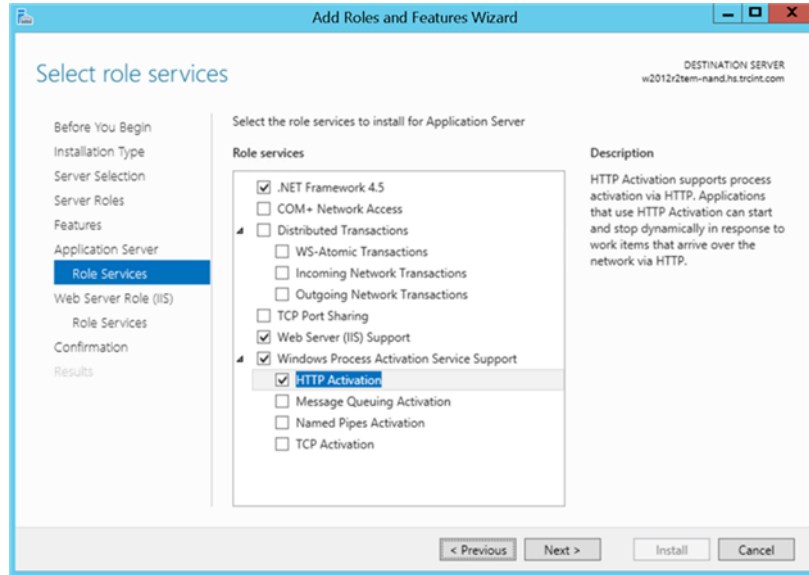
---

**Note** When you select Web Server (IIS), a dialog box appears prompting you to confirm features that are required for Web Server (IIS). Click **Add Features**.

---

- Windows Process Activation Service Support
  - HTTP Activation

For example:

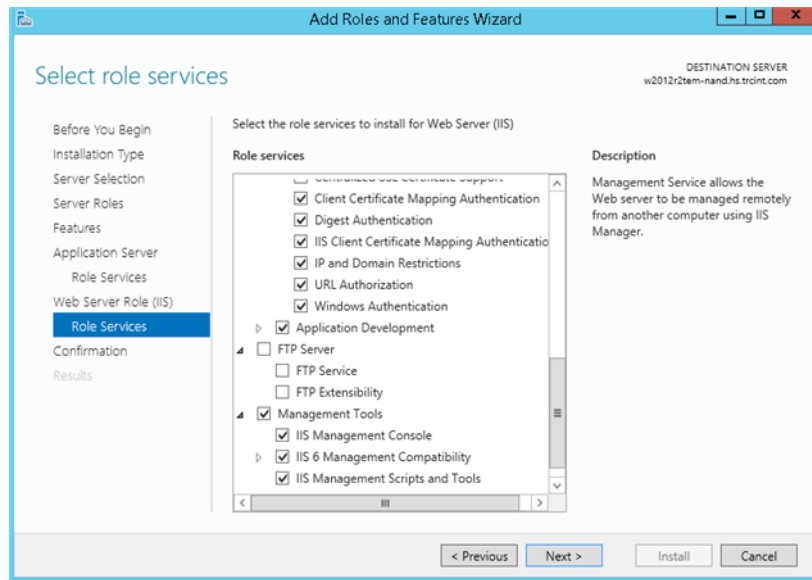


**8** Click **Next** and click **Next** again to display the Web Server Role (IIS) Role Services page.

9 In the Web Server Role (IIS) Role Services page, select the following role services.

- Web Server Role (IIS)
  - Role Services
    - Web Server
      - Accept the default selections
      - Enable the following option:
        - Management Tools
          - IIS Management Console
          - IIS 6 Management Compatibility

For example:



10 Click **Next**.

11 Click **Install**.

12 When the installation is finished, click **Close** to close the Add Roles and Features wizard.

#### What to do next

Install Microsoft Visual J# 2.0 Redistributable Package, if necessary.

### Add Windows Server Roles and Features (Windows Server 2016)

Add the required Windows Server roles and features in the Integration Broker server.

**Note** The steps in this procedure refer to the Windows Server 2016 user interface. For Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2, see [Add Windows Server Roles and Features \(Windows Server 2012 R2, 2012, or 2008 R2\)](#).

#### Prerequisites

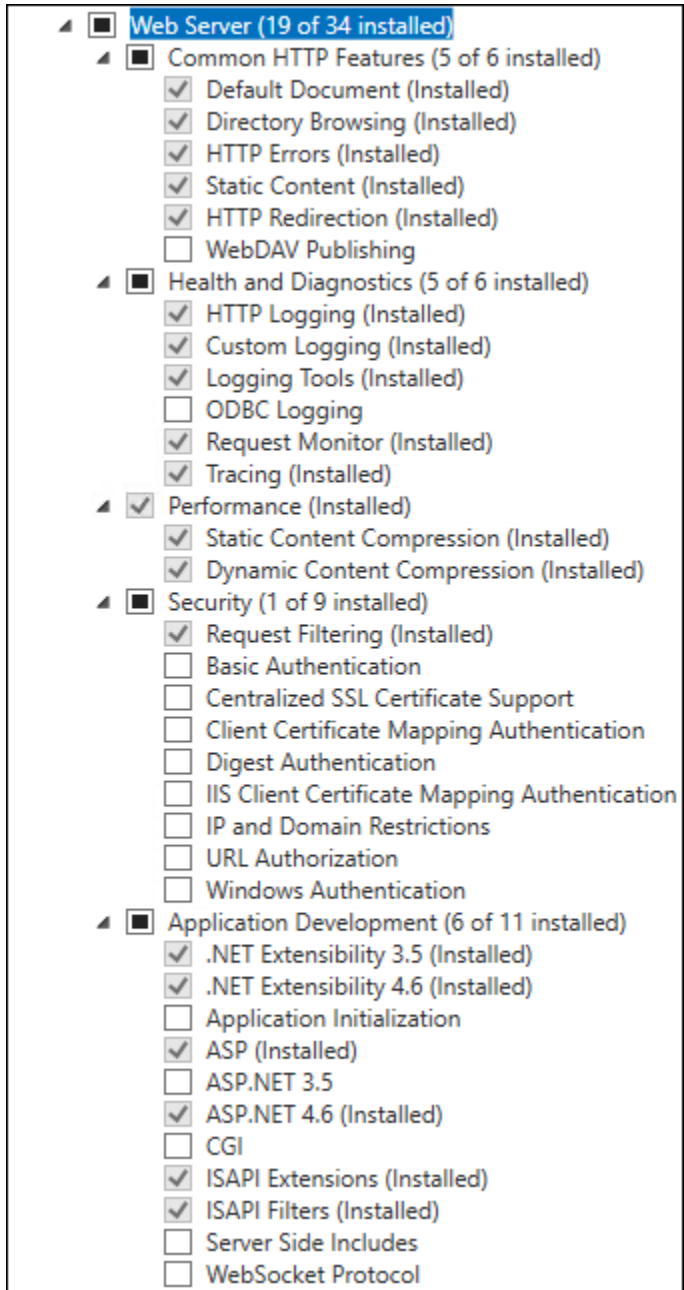
- You are using VMware Identity Manager 3.2.0.1 or later. Installing Integration Broker on Windows Server 2016 is supported in VMware Identity Manager 3.2.0.1 and later.
- Verify that Windows Server 2016 is installed with the latest updates.

- Create an application pool, if necessary. You can use the default application pool or create an application pool that is dedicated to Integration Broker.

#### Procedure

- 1 Select **Start > Server Manager**.
- 2 In Server Manager, select **Manage > Add Roles and Features**.
- 3 In the Add Roles and Features wizard, click **Next** until the **Server Roles** page appears.
- 4 In the Server Roles page, select the following roles.
  - File and Storage Services
    - Storage Services
  - Web Server (IIS)
    - Web Server





■ Management Tools

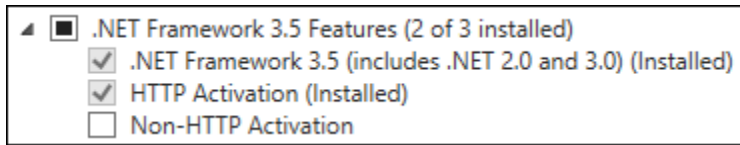


5 Click **Next**.

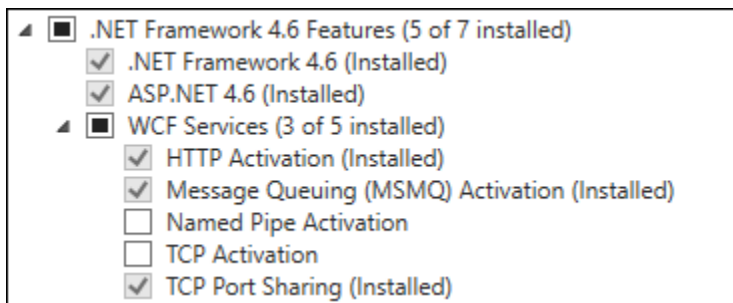
6 In the Features page, select the following features.

- .NET Framework 3.5 Features
  - .NET Framework 3.5 (includes .NET 2.0 and 3.0)
  - HTTP Activation

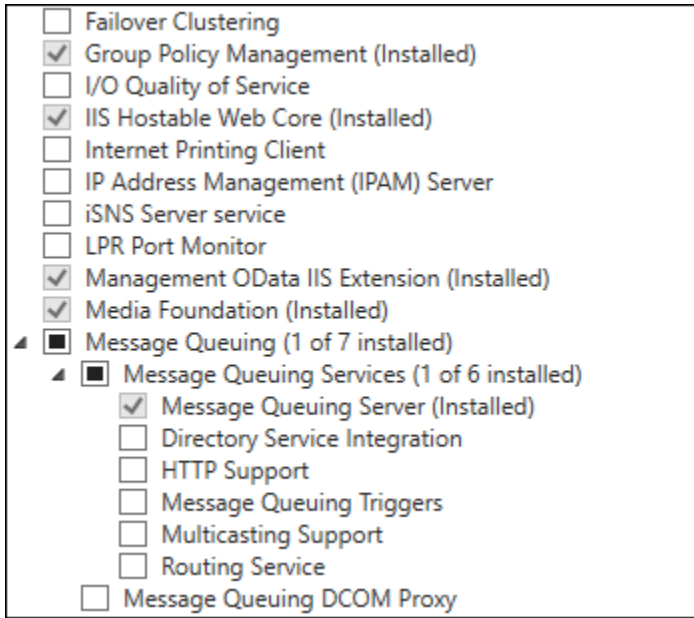
When you select HTTP Activation, a dialog box appears prompting you to confirm features that are required for HTTP Activation. Click **Add Features**.



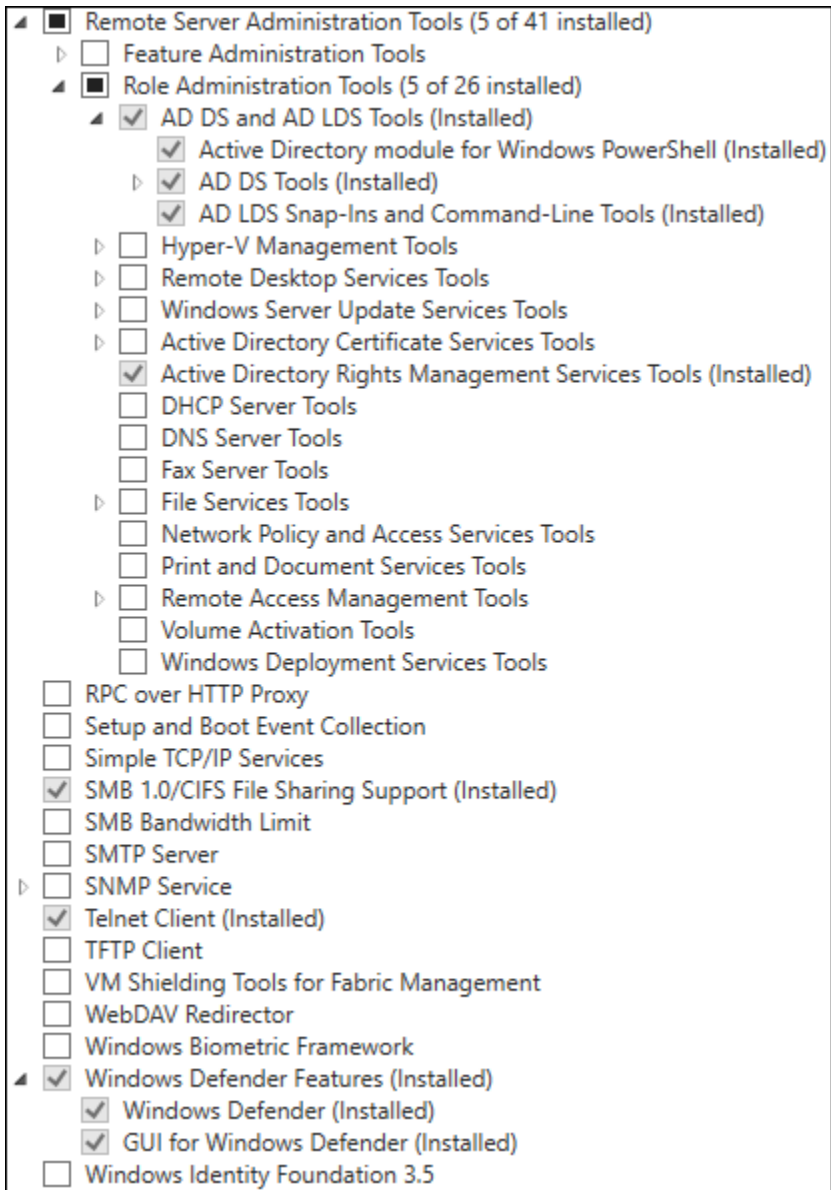
- .NET Framework 4.6 Features
  - .NET Framework 4.6
  - ASP.NET 4.6
  - WCF Services



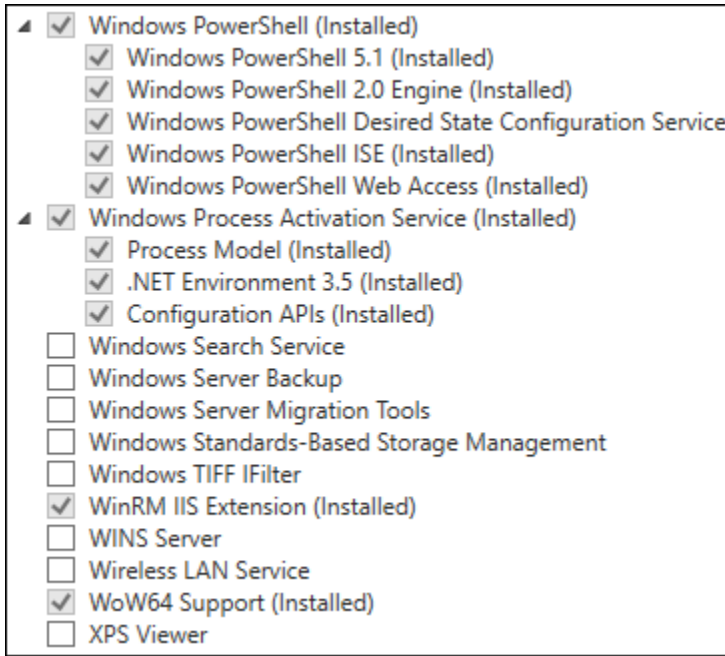
- Group Policy Management
- IIS Hostable Web Core
- Management OData IIS Extension
- Media Foundation
- Message Queueing
  - Message Queuing Services



- Remote Server Administration Tools
- SMB 1.0/CIFS File Sharing Support
- Telnet Client
- Windows Defender Features



- Windows PowerShell
- Windows Process Activation Service
- WinRM IIS Extension
- Wow64 Support



7 Click **Next** and in the Confirmation page, click **Install**.

8 When the installation is finished, click **Close** to close the Add Roles and Features wizard.

#### What to do next

Install Microsoft Visual J# 2.0 Redistributable Package, if necessary.

### Install Microsoft Visual J# 2.0 64-bit Redistributable Package

Download and install Microsoft Visual J#® 2.0 64-bit Redistributable Package - Second Edition. This step is not required if you plan to use the Citrix StoreFront REST API instead of the Citrix Web Interface SDK to connect to the Citrix server farm.

#### Procedure

- 1 Download the Microsoft Visual J# 2.0 64-bit Redistributable Package - Second Edition from the Microsoft web site.
- 2 Double-click the vjredist.exe file and follow the wizard to install the package.

## Deploy Integration Broker

To deploy Integration Broker, you download and install the Integration Broker on a supported Windows server, configure IIS Manager settings for it, and set up HTTPS and HTTP bindings.

### Install Integration Broker

Install Integration Broker on the Windows server that you configured.

#### Prerequisites

- Prepare the Windows server. See [Prepare Windows Server for Integration Broker Installation](#).

- Download Integration Broker from the VMware Identity Manager product page on [My VMware](#).

#### Procedure

- 1 Log in as a Windows administrator.
- 2 Click the `setup.exe` file to run the Integration Broker installer.
- 3 Accept the end user license agreement.
- 4 Select the Web location where you want to install the Integration Broker.
- 5 (Optional) If you created a separate application pool for the Integration Broker, select the application pool.

---

**Caution** Do not change the **Virtual Directory** name.

---

- 6 Click **Next** to finish installing Integration Broker.

#### What to do next

Configure IIS Manager Settings.

### Configure IIS Manager Settings for the Integration Broker Component of VMware Identity Manager

Configure the required IIS Manager settings for the Integration Broker deployed with VMware Identity Manager.

---

**Note** The steps in this procedure refer to the Windows Server 2012 or Windows Server 2012 R2 user interface.

---

#### Prerequisites

The credentials for the Identity user. The Identity user must meet the following requirements:

- Domain user
- Privileges to enable PowerShell Remoting on the Integration Broker server:
  - a Launch PowerShell with administrator privileges
  - b Run `Enable-PSRemoting`
- One of the following roles on the Citrix server:
  - At least Read Only Administrator (version 7.x) or View Only Administrator (version 6.x)
  - A custom administrator role that has the permissions to execute the following PowerShell cmdlets. These cmdlets are used to retrieve applications, server, farm, and icon information from the Citrix server farm.

On XenApp 6.5:

`Get-XAApplication`

Get-XAServer

Get-XAAccount

Get-XAApplicationIcon

Get-XAFarm

On XenApp or XenDesktop 7.x:

Get-BrokerApplication

Get-BrokerIcon

Get-BrokerDesktopGroup

Get-BrokerAccessPolicyRule

Get-BrokerAppEntitlementPolicyRule

Get-BrokerIcon

Get-BrokerEntitlementPolicyRule

#### Procedure

- 1 Click **Start > Server Manager**.
- 2 In Server Manager, select **Tools > Internet Information Services (IIS) Manager**.
- 3 In IIS Manager, configure the application pool that you selected while installing the Integration Broker.

---

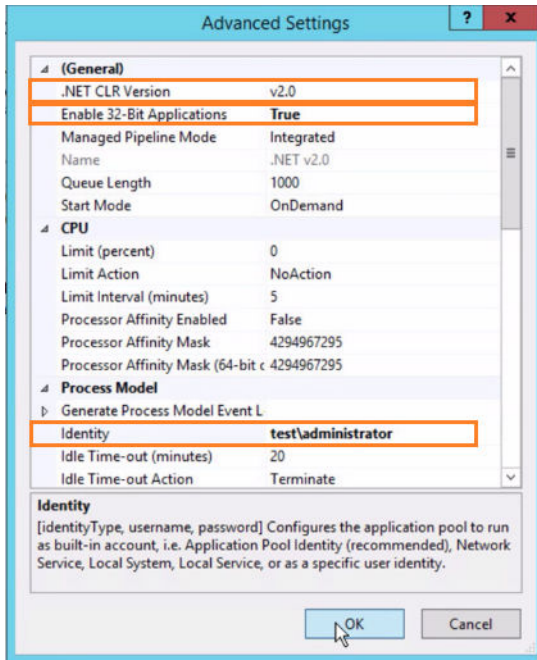
**Tip** To verify the correct application pool, click **Application Pools** in the left pane, right-click the application pool and select **View Applications**, and verify that the Integration Broker appears in the list.

---

- a In the left pane, click **Application Pools**.
- b Select the application pool that you are using for the Integration Broker.
- c Click **Advanced Settings** in the right pane.

d In the Advanced Settings dialog box, configure the following settings.

Option	Description
<b>.NET CLR Version</b>	For Citrix 7 1912 and later versions, set the value to <b>v4.0</b> . For prior versions, set the value to <b>v2.0</b> .  <b>Note</b> In Windows 2012 and Windows 2012 R2, the application pool may have been configured to a different .NET version by default. Ensure that you configure it to the appropriate version.
<b>Enable 32-bit Applications</b>	Set the value to <b>True</b> .
<b>Identity</b>	<ol style="list-style-type: none"> <li>1 Click <b>Identity</b>.</li> <li>2 Click the ... icon.</li> <li>3 In the Application Pool Identity dialog box that opens, click <b>Custom Account</b>, then click <b>Set</b>.</li> <li>4 Enter the user name and password for the Identity user. See the requirements for the Identity user in the Prerequisites section.</li> <li>5 Click <b>OK</b> and click <b>OK</b> again.</li> </ol>



e Click **OK** to close the Advanced Settings dialog box.



## Set HTTPS Site Binding for the Integration Broker

You must set the HTTPS site binding for the Integration Broker. To set the binding, you need an SSL certificate for the Integration Broker server. You can obtain a certificate from a Certificate Authority or create a self-signed certificate.

---

**Note** If you are using the Windows version of the VMware Identity Manager connector and you are installing the Integration Broker on the same server as the connector, ensure that the HTTP and HTTPS binding ports do not conflict with the ports used by the connector.

The VMware Identity Manager Connector always uses port 80. It also uses 443, unless a different port is configured during installation. For more information on the ports used, see *Installing and Configuring VMware Identity Manager Connector (Windows)*.

Installing the Integration Broker and the VMware Identity Manager Connector on different servers is recommended.

---

### Prerequisites

- Obtain an SSL certificate for the Integration Broker server. You can get a certificate from a Certificate Authority or create a self-signed certificate. Install the certificate in the Microsoft store in the Integration Broker server.

See [Example: Create a Self-signed Certificate Using IIS Manager](#) and [Example: Create a Self-signed Certificate Using OpenSSL](#).

---

**Note** If you are using the Windows version of the VMware Identity Manager connector and have installed the Integration Broker on the same server as the connector, you can use the self-signed certificate that is generated during the connector installation. Install the certificate in the Microsoft store and use it for the HTTPS binding.

---

### Procedure

- 1 In IIS Manager, in the left pane, click the web site under which you installed the Integration Broker.

---

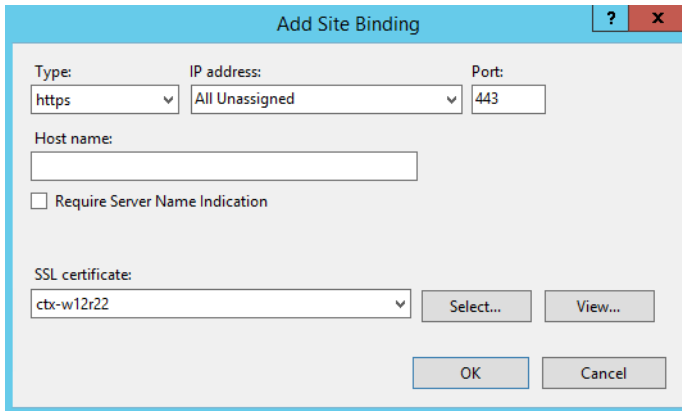
**Tip** To verify the correct web site, you can expand the site in the left pane and check that the Integration Broker is listed under it.

---

- 2 In the right pane, under **Edit Site**, click **Bindings**.
- 3 Add the HTTPS binding using the certificate you created.
  - a Click **Add**.
  - b In the **Type** field, select **https**.
  - c If you are using IIS 8.0 or later, verify that the **Host name** field is empty. It must not have any value.

- d In the **SSL Certificate** field, select the SSL certificate you created.

For example:



- e Click **OK**.

**4** Restart IIS.

- a Open the Command Prompt window as administrator.
- b Type `iisreset`.

**What to do next**

Verify the bindings.

- Verify that the HTTP binding produces the expected output by typing `http://hostname/IB/API/RestServiceImpl.svc/ibhealthcheck` in the address bar of a browser.

Expected output:

All ok

- Verify that the HTTPS binding produces the expected output by typing `https://hostname/IB/API/RestServiceImpl.svc/ibhealthcheck` in the address bar of a browser.

Expected output:

All ok

---

**Note** In Internet Explorer, the All ok output is not displayed directly. Instead, the output file is downloaded. Open the file to view the output.

---

**Example: Create a Self-Signed Certificate Using IIS Manager**

You can create a self-signed certificate for the Integration Broker server using IIS Manager.

**Procedure**

- 1 Start IIS Manager.
- 2 Navigate to **Server Certificates**.
- 3 In the right pane, under **Action**, select **Create Self-signed Certificate**.

#### 4 Follow the wizard to generate the self-signed certificate.

The certificate is installed automatically in the Microsoft store in the Integration Broker server.

#### What to do next

Use the certificate for the HTTPS binding for the Integration Broker web site.

#### Example: Create a Self-signed Certificate Using OpenSSL

These instructions provide a sample for how to set a self-signed certificate using OpenSSL for Integration Broker.

#### Procedure

- 1 Create a self-signed certificate for the Integration Broker server.
- 2 Create the `ibcerts` folder to use as the working directory.
- 3 Create a configuration file using the `vi openssl_ext.conf` command.
  - a Copy and paste the following OpenSSL commands into the configuration file.

```
# openssl x509 extfile params
extensions = extend
[req] # openssl req params
prompt = no
distinguished_name = dn-param
[dn-param] # DN fields
C = US
ST = CA
O = VMware (Dummy Cert)
OU = Horizon Workspace (Dummy Cert)
CN = hostname (Virtual machine hostname where the Integration Broker is installed. )
emailAddress = EMAIL PROTECTED
[extend] # openssl extensions
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always
keyUsage = digitalSignature,keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
[policy] # certificate policy extension data
```

---

**Note** Type the CN value before you save the file.

---

- b Run this command to generate a private key.

```
openssl genrsa -des3 -out server.key 1024
```

- c Type the passphrase for *server.key*, for example, *vmware*.

- d Rename the `server.key` file to `server.key.orig`.

```
mv server.key server.key.orig
```

- e Remove the password associated with the key.

```
openssl rsa -in server.key.orig -out server.key
```

- 4 Create a CSR (certificate signing request) with the generate key. The `server.csr` is stored in your working directory.

```
openssl req -new -key server.key -out server.csr -config ./openssl_ext.conf
```

- 5 Sign the CSR.

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt -extfile openssl_ext.conf
```

The expected output displays.

```
Signature ok subject=/C=US/ST=CA/O=VMware (Dummy Cert)/OU=Horizon Workspace
(Dummy Cert)/CN=w2-hwdog-xa.vmware.com/emailAddress=EMAIL_PROTECTED Getting
Private key
```

- 6 Create P12 format.

```
openssl pkcs12 -export -in server.crt -inkey server.key -out server.p12
```

- a Press **Enter** at the prompt for an export password.

---

**Important** Do not enter a password.

---

The expected output is `server.p12` file.

- b Move the `server.p12` file to the Windows machine where Integration Broker is installed.
  - c From the Command Prompt, type **mmc**.
  - d Click **File > Add or Remove Snap-ins**.
  - e In the Snap-in window, click **Certificates** and click **Add**.
  - f Select the **Computer account** radio button.
- 7 Import the certificate into the root and personal store certificates.
    - a Choose **All Files** in the dialog.
    - b Select the `server.p12` file.
    - c Click the **Exportable** check box.
    - d Leave the password blank.
    - e Accept the defaults for the subsequent steps.

- 8 Copy the certificate into the Trusted Root CAs in the same mmc console.
- 9 Verify that the content of the certificate includes these elements.
  - Private key
  - CN in the subject attribute that matches the Integration Broker Host Name
  - Extended key usage attribute with both client and server authentication enabled

## Enable Citrix PowerShell Remoting

You must enable remote invocations between the Integration Broker and the Citrix server farm by setting up Citrix PowerShell Remoting.

To set up Citrix PowerShell remoting, you install the Citrix PowerShell SDK on the Integration Broker server and verify that PowerShell remoting is enabled on the Citrix servers.

On the Integration Broker server, you must install the appropriate version of the Citrix PowerShell SDK. If you connect to multiple versions of Citrix server farms, install all the required versions of the Citrix PowerShell SDK on the Integration Broker server as the SDKs are not backwards compatible.

PowerShell remoting must be enabled on Citrix servers so that the Integration Broker server can connect to them and retrieve required information such as resources information, entitlements, and icons. You need to enable PowerShell remoting only on the Delivery Controllers or XML Brokers that you will configure in VMware Identity Manager, not on all the servers in your server farm. In XenApp or XenDesktop 7.x, these are the Delivery Controllers, which also act as XML Brokers. In Citrix server farms 6.5 and 6.0, these are the XML Broker servers.

For Citrix server farm 6.0, Citrix PowerShell Remoting requires a secure HTTPS channel to make remote calls. Ensure that the Citrix Delivery Controllers or XML Brokers have valid SSL certificates.

## Install Citrix PowerShell SDK on the Integration Broker Server

You must install the Citrix PowerShell SDK on the Integration Broker server to enable connections between the Integration Broker server and the Citrix server farm.

Download and install the Citrix PowerShell SDK version that corresponds to the Citrix server farm that you are integrating with VMware Identity Manager. If you connect to multiple versions of Citrix server farms, install all the required versions of the Citrix PowerShell SDK on the Integration Broker server as the SDKs are not backwards compatible.

### Procedure

- 1 Log in to the Integration Broker server.

2 If you are connecting to XenApp or XenDesktop 7.x, follow these steps.

a Download and install Citrix Studio on the Integration Broker server.

b Verify the installation.

1 Open Windows PowerShell as administrator.

2 Enter this command:

```
Add-PSSnapin Citrix*
```

3 Enter the following commands:

```
Get-BrokerDesktopGroup -AdminAddress CitrixDeliveryController
```

```
Get-ConfigSite -AdminAddress CitrixDeliveryController
```

---

**Note** If you get an authentication error, set the execution policy with the `set-executionpolicy remotesigned` command, then try the commands again.

---

3 If you are connecting to Citrix server farm 6.5, follow these steps.

a Download and install Citrix PowerShell SDK 6.5 on the Integration Broker server.

b Verify the installation.

1 Open **Program Files > Citrix PowerShell Module**.

2 Enter this command:

```
Get-XAApplication -ComputerName CitrixServer
```

Verify that the list includes all the applications hosted by Citrix.

---

**Note** If the command fails, verify that the XenApp Commands Remoting service is running on the Citrix server.

---

4 If you are connecting to Citrix server farm 6.0, download and install Citrix PowerShell SDK 6.0 on the Integration Broker server.

## Enable Citrix PowerShell Remoting on the Citrix Server Farm

Enable Citrix PowerShell remoting on the Citrix server farm, if necessary.

- On Citrix XenApp or XenDesktop 7.x, verify that PowerShell remoting is enabled on the Delivery Controllers to which VMware Identity Manager will connect.
- On Citrix 6.5, verify that the Citrix XenApp Commands Remoting service is running on the XML Brokers to which VMware Identity Manager will connect.
- On Citrix 6.0, enable PowerShell Remoting. See [Setting up Citrix PowerShell Remoting on Citrix Server Farm 6.0](#).

## Setting up Citrix PowerShell Remoting on Citrix Server Farm 6.0

You must enable Citrix PowerShell remoting on the Citrix XML Broker servers that you are integrating with VMware Identity Manager. Citrix PowerShell remoting enables connections between Integration Broker and the Citrix server farm.

---

**Note** You need to enable Citrix PowerShell remoting only on the XML Brokers that will be configured in VMware Identity Manager, not on all the servers in your server farm.

---

### Prerequisites

- If you do not have Winrm installed, download and install Winrm from the Microsoft Web site.
- Verify that the Citrix XML Brokers have valid SSL certificates. Also, click **Properties** and verify that Server Authentication is enabled for the certificates.

### Procedure

- 1 Open PowerShell in administrator mode.
- 2 Enable Citrix PowerShell Remoting.
  - a Type the `Get-Service winrm` command to verify that Winrm is installed on the server.
  - b Type the `Enable-PSRemoting` command.

This command enables PowerShell Remoting on the server.
  - c Install Citrix PowerShell SDK 6.0.
  - d Enable winrm HTTPS listener from the command prompt.
    - 1 Create a certificate on the server.
    - 2 Record the certificate's thumb print.
    - 3 Verify that the certificate's thumb print is configured.

```
winrm quickconfig -transport:https
```

- e Verify that the listener was created.

```
winrm e winrm/config/listener
```

This server is ready to use.

- f After the listener is created, go to the Integration Broker server to verify that PowerShell remoting is installed correctly.

```
winrm identify -r:https://XENAPP_HOSTNAME:5986 -u:USERNAME
```

Output:

```
IdentifyResponse
```

```
ProtocolVersion=http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
```

```
ProductVendor=Microsoft Corporation
```

```
ProductVersion=OS: 6.0.6002 SP: 2.0 Stack: 2.0
```

## Enabling Integration Broker to Use TLS 1.2

If you enable TLS 1.2 on the Integration Broker server and you plan to use the Citrix StoreFront REST API to communicate with Citrix servers to launch applications and desktops, you must also update the Windows registry to enable the Integration Broker to communicate over TLS 1.2.

Update the Windows Registry on the Integration Broker server to include the following keys:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v2.0.50727]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

For more information, see the Microsoft documentation at <https://docs.microsoft.com/en-us/dotnet/framework/network-programming/tls>.

## Verify the Connection to the Citrix Server Farm

After you deploy the Integration Broker and set up PowerShell remoting, verify the connection to the Citrix server farm.

### Procedure

- 1 In a browser, enter the appropriate URL for your Citrix farm version.
  - Citrix XenApp or XenDesktop server farm 7.x
 

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenAppServerHostname&xenappversion=Version7x
```
  - Citrix server farm 6.5



```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?
computerName=XenAppServerHostname&xenappversion=Version65orLater
```

- Citrix server farm 6.0

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?
computerName=XenAppServerHostname&xenappversion=Legacy
```

## 2 Review the output.

If Integration Broker is properly configured, the page displays Citrix server farm information, such as the following:

```
"[{"FarmName\":\"test data\",\"ServerVersion\":\" 6.0.6410\",\"AdministratorType\":\"Full
\",\"SessionCount\":\"2\",\"MachineName\":\"test data\"}]"
```

If the Web page does not display the server farm information, review the logs on the Integration Broker server at %programdata%/VMware/HorizonIntegrationBroker.

## Download Citrix Web Interface SDK 5.4

The Citrix Web Interface SDK is used to authenticate with and generate the ICA file from the Citrix Delivery Controllers or XML Brokers to launch Citrix-published applications and desktops.

---

**Note** If you plan to use the Citrix StoreFront REST API to communicate with the Citrix farm to generate the ICA file, you do not need to install the Citrix Web Interface SDK.

---

### Procedure

- 1 Download the Citrix Web Interface SDK 5.4 (WISDK zip file) from the Citrix Web site.
- 2 Unzip the wisdk.zip file.
- 3 Copy the contents from the WI5\_4\_0\_SDK/zipfiles/sdkdemo/wisdk directory to the Integration Broker default bin directory at c:\inetpub\wwwroot\IB\bin.
- 4 Restart IIS.
  - a Open the Command Prompt window as administrator.
  - b Type `iisreset`.

## Configuring Citrix Server Farms in VMware Identity Manager

To configure Citrix XenApp and XenDesktop server farms in VMware Identity Manager, you create one or more virtual apps collections in the Virtual Apps Configuration page, which contain configuration information such as the Citrix servers from which to sync resources and entitlements, the Integration Broker to use for sync and SSO, the VMware Identity Manager connector to use for sync, and administrator settings such as the default launch client.

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 different connectors. 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 VMware Identity Manager, ensure that you meet all the prerequisites.

Also follow these guidelines for Citrix server farm settings.

- **Syncing Delivery Groups**

A delivery group's Delivery Type setting in Citrix determines how VMware Identity Manager syncs the delivery group.

VMware Identity Manager 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 VMware Identity Manager catalog.

Configure your delivery groups accordingly.

- In XenDesktop and XenApp 7.9, 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, sync to VMware Identity Manager will not work.
- 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 Citrix-published resources 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 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. VMware Identity Manager does not support this setting. To ensure that users have the correct entitlements in VMware Identity Manager, set explicit entitlements for the users and groups.
- VMware Identity Manager does not support the Citrix anonymous user group feature.

---

**Note** Beginning with VMware Identity Manager 3.3, XenApp 5.x is no longer supported. You cannot update or save existing configurations that include a XenApp 5.x server unless you remove the server from the configuration. After you remove the 5.x server from the configuration and save the configuration, all resources associated with the 5.x server will be removed from the catalog during the next sync. Users will be able to run the resources until they are removed from the catalog.

---

## Prerequisites

- Configure VMware Identity Manager. See *Installing and Configuring VMware Identity Manager* and *VMware Identity Manager Administration* for information.
- Make sure that users and groups with Citrix entitlements have been synced from your enterprise directory to VMware Identity Manager using directory sync.

While creating the directory, ensure that you make **userPrincipalName** a required attribute.

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

- Deploy the Integration Broker and ensure that you have met all the prerequisites described in [Prerequisites for Citrix Integration](#).
- If you are using a load balancer in front of the Integration Broker, note the host name or IP address of the load balancer for use during this task.
- If you want to use the StoreFront option, available in VMware Identity Manager 2.9.1 and later, ensure the following requirements are met.
  - Install Integration Broker 2.9.1 or later.
  - Ensure that StoreFront is supported by the XenApp or XenDesktop version you are using.
  - Ensure that the Integration Broker can communicate with the StoreFront server.

When you enable the StoreFront REST API, the Integration Broker communicates with the StoreFront server to generate the ICA file.

- In the StoreFront server, if you configure trusted domains for the "User name and password" authentication method, ensure that you add domain names in the fully qualified domain name format to the "Trusted domains" list. VMware Identity Manager requires the fully qualified domain name. For more information, see [Launch of Citrix-published Applications and Desktops](#).
- If your Citrix deployment includes a Citrix NetScaler Gateway server and you intend to connect to the Citrix server farm using the Web Interface SDK, obtain the URL of the Citrix Secure Ticket Authority (STA) server associated with the NetScaler Gateway server. See [Obtain the STA Server URL for the NetScaler Gateway](#).
- Review Citrix documentation for your version of Citrix XenApp or XenDesktop.
- To perform this procedure in VMware Identity Manager, 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 VMware Identity Manager console.

- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click **New**.
- 4 Select **Citrix Published Application** as the source type.
- 5 In the New Citrix XenApp wizard, enter the following information in the Connector and Broker page.

Option	Description
<b>Name</b>	Enter a unique name for the Citrix virtual apps collection.
<b>Connector</b>	<p>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 <b>Host</b> list and you can arrange them in failover order for this collection. To rearrange the list, click and drag the rows to the desired position.</p>
	<p><b>Important</b> After you create the collection, you cannot select a different directory.</p>

Option	Description
<b>Sync Integration Broker</b>	<p>Enter the connection information for the Integration Broker instance that you want to use to sync the resources in this collection.</p> <ul style="list-style-type: none"> <li>■ <b>Host:</b> Enter the fully qualified domain name of the Integration Broker instance. For example, ibserver.example.com.</li> </ul> <p>If you have configured a load balancer in front of multiple Integration Broker instances dedicated to sync, enter the host name or IP address of the load balancer.</p> <ul style="list-style-type: none"> <li>■ <b>Port:</b> Enter the port number of the Integration Broker instance or load balancer.</li> <li>■ <b>Use SSL:</b> To connect to the Integration Broker over SSL, enable <b>Use SSL</b> and copy and paste the SSL certificate of the Integration Broker server into the <b>SSL Certificate</b> box. Enter all the lines including ---BEGIN CERTIFICATE---- and -----END CERTIFICATE----.</li> </ul> <p>The certificate will be used when resources in this virtual apps collection are synced to VMware Identity Manager.</p>
<b>Launch Integration Broker</b>	<p>Enter the connection information for the Integration Broker instance that you want to use to process launch requests for this collection. You must connect to the SSL Integration Broker over SSL. The SSL Integration Broker can be the same as the SSO Integration Broker.</p> <ul style="list-style-type: none"> <li>■ <b>Host:</b> Enter the fully qualified domain name of the Integration Broker instance. For example, ibserver.example.com.</li> </ul> <p>If you have configured a load balancer in front of multiple Integration Broker instances dedicated to launch, enter the fully qualified domain name of the load balancer.</p> <hr/> <p><b>Note</b> Do not use the IP address.</p> <ul style="list-style-type: none"> <li>■ <b>Port:</b> Enter the port number of the Integration Broker instance or load balancer.</li> <li>■ <b>SSL Certificate:</b> Copy and paste the SSL certificate of the Integration Broker server into the <b>SSL Certificate</b> box. Enter all the lines including ---BEGIN CERTIFICATE---- and -----END CERTIFICATE----.</li> </ul> <p>The certificate will be used during the launch of resources from this virtual apps collection.</p>

## 6 Click **Next**.

- 7 In the Server Farm page, click **Add Server Farm** and enter your Citrix server farm information.

Option	Description
<b>Version</b>	Select the version of your Citrix XenApp or XenDesktop deployment: 6.0, 6.5, or 7.x.
<b>Server</b>	<p>Click <b>Add Server</b> 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 <b>Add Server</b> and add the server.</p> <p>Arrange the servers in failover order. VMware Identity Manager follows this order for SSO and under failover conditions. To rearrange the list, click and drag the rows to the desired position. To delete a server from the list, click the <b>x</b> icon at the right of the row.</p> <hr/> <p><b>Note</b> The XML brokers must have PowerShell Remoting enabled.</p>
<b>Launch Preference</b>	Select how you want VMware Identity Manager to process launch requests for Citrix resources. If you have Citrix StoreFront deployed, select <b>StoreFront</b> , otherwise select <b>Web Interface SDK</b> . You need to select and enter information for only one of the options.

Option	Description
<b>StoreFront</b>	<p>Select this option if you want Citrix resources to be launched using the Citrix StoreFront REST API. When this option is selected, the Integration Broker uses the Citrix StoreFront REST API to communicate with the StoreFront server and retrieve the ICA file.</p> <ul style="list-style-type: none"> <li>■ <b>StoreFront Server URL</b></li> </ul> <p>Enter the StoreFront server URL in the following format:</p> <p><b><i>transportType://storefrontServerFQDN/Citrix/storenameWeb</i></b></p> <p>For example, <b>http://xen76.example.com/Citrix/mystoreWeb</b>.</p> <hr/> <p><b>Note</b> This is the StoreFront server Website URL.</p> <hr/> <p><b>Important</b> Later, after creating the virtual apps collection, when you configure internal network ranges for XenApp ensure that you enter the same URL in the <b>Client Access URL Host</b> field.</p> <hr/> <p><b>Note</b> After creating and syncing the virtual apps collection, if you choose not to use the <b>StoreFront</b> option, ensure that you update the Client Access URL for network ranges as well.</p>
<b>Web Interface SDK</b>	<p>Select this option if you want Citrix resources to be launched using the Citrix Web Interface SDK. When this option is selected, the Integration Broker uses the Citrix Web Interface SDK to communicate with Citrix components and retrieve the ICA file.</p> <ul style="list-style-type: none"> <li>■ <b>Transport type</b></li> </ul> <p>Select the transport type used in your Citrix server configuration: HTTP, HTTPS, or SSL RELAY. This must match your Citrix server configuration.</p> <ul style="list-style-type: none"> <li>■ <b>Port</b></li> </ul> <p>Enter the port used in your Citrix server configuration. This must match your Citrix server configuration.</p> <ul style="list-style-type: none"> <li>■ <b>SSL Relay Port</b></li> </ul> <p>Enter the SSL Relay port used in your Citrix server configuration. This option appears only if you select SSL RELAY as the transport type.</p> <ul style="list-style-type: none"> <li>■ <b>STA Server</b></li> </ul> <p>If your Citrix deployment includes a NetScaler Gateway server, specify the Secure Ticket Authority (STA) server associated with it. The STA server is used to control access for a NetScaler Gateway server.</p> <ol style="list-style-type: none"> <li>1 Click <b>Add STA Server</b> and enter the STA server URL in the following format: <i>transporttype://server:port</i></li> </ol> <p>For example: <b>http://staserver.example.com:80</b></p> <p>Only alphanumeric characters, period (.), and hyphen (-), are allowed in the URL.</p> <ol style="list-style-type: none"> <li>2 To add multiple STA servers, click <b>Add STA server</b> and add the servers.</li> <li>3 Arrange the STA servers in failover order. To move a row, click the handle on the left of the row and drag to the desired location. To delete a server from the list, click the <b>x</b> icon at the right of the row.</li> </ol>

## 8 Click **Next**.

9 In the Configuration page, enter the following information.

Option	Description
<b>Sync Frequency</b>	<p>Select how often you want to sync the resources in the collection from the Citrix server farm to VMware Identity Manager.</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 <b>Manual</b>, you must click <b>Sync</b> on the Virtual Apps Collections page after you create the collection and whenever there is a change in your Citrix resources or entitlements.</p>
<b>Sync Duplicate Apps</b>	<p>Set to <b>No</b> if you want to prevent duplicate applications from being synced from multiple servers.</p> <p>When VMware Identity Manager is deployed in multiple data centers, the same resources are set up in the multiple data centers. Setting this option to <b>No</b> prevents duplication of the applications and desktops in your VMware Identity Manager catalog.</p>
<b>Sync Categories from Server Farms</b>	<p>Enable this option if you want to sync categories from the Citrix servers to VMware Identity Manager.</p>
<b>Activation Policy</b>	<p>Select how you want to make resources in this collection available to users in the Workspace ONE portal and app. If you intend to set up an approval flow, select <b>User-Activated</b>, otherwise select <b>Automatic</b>.</p> <p>With both the <b>User-Activated</b> and <b>Automatic</b> options, the resources are added to the Catalog page. Users can use the resources from the Catalog page or move them to the Bookmarks 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 <b>Users &amp; Groups</b> tab.</p>

10 Click **Next**.

11 In the Summary page, review your selections, then click **Save & Configure Network Range**.

The collection is created but the resources in the collection are not yet synced. The Network Ranges page appears.

**What to do next**

- Configure network ranges for resource launch. See [Configuring Citrix Resource Launch in VMware Identity Manager](#).
- To sync the resources and entitlements in the collection from the Citrix servers to VMware Identity Manager, select the collection in the Virtual Apps Collections page and click **Sync**.

**Note** VMware Identity Manager does not support the Citrix anonymous user group feature.



# Configuring Citrix Resource Launch in VMware Identity Manager

After configuring the Citrix Published Applications page, 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 Resource Launch for Internal Networks

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.

When a user launches an application or desktop from the Workspace ONE catalog, 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 Resource Launch for External Networks with NetScaler Gateway](#).

---

### Prerequisites

A Super Admin role is required to edit and save the Network Ranges page.

### Procedure

- 1 Log in to the VMware Identity Manager console.
- 2 Select the **Catalog > Virtual Apps Collections** tab.
- 3 Click the Citrix collection for which you want to set network ranges.
- 4 Click **Edit Network Range**.
- 5 In the Network Ranges page, 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 click **Create Network Range** to 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 **XenApp 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
<b>Client Access FQDN</b>	<p>If the <b>StoreFront</b> option is selected as the launch preference in the Citrix virtual apps collection, enter the same URL that you entered in the <b>StoreFront URL</b> text box.</p> <p>Otherwise, enter the XenApp server host name. For example, <b>xenapphost.example.com</b>. If there is a load balancer in front of the XenApp servers, use the following format:</p> <p><b><i>loadbalancerURL/citrix/storeweb</i></b></p>
<b>Port</b>	<p>The server port. For example, 443.</p> <p>If you entered a load balancer URL in the <b>Client Access FQDN</b> text box, use port 443.</p>
<b>NetScaler</b>	Set this option to <b>No</b> .

XenApp Farm UUID	XenApp Farm Server	Client Access FQDN	Port	NetScaler
acfa4389-feba-4651-945f-7d6a3bbee008	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.
- g Click **Finish** in the Network Ranges page.

## Configuring Resource Launch for External Networks with NetScaler Gateway

VMware Identity Manager 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 Identity Manager with the appropriate settings so that when users launch Citrix resources, the traffic is routed through the NetScaler Gateway appliance to the XenApp server. In the VMware Identity Manager console, for each XenApp farm, specify the Secure Ticket Authority (STA) server associated with the NetScaler Gateway appliance. The STA server is used to generate and validate STA tickets during the application launch process.

You can also 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 Identity Manager also supports Citrix Secure Gateway. The configuration steps in this section are applicable to both NetScaler Gateway and Citrix Secure Gateway.

**Note** To configure NetScaler Gateway in VMware Identity Manager, you must use Integration Broker 2.4 or later.

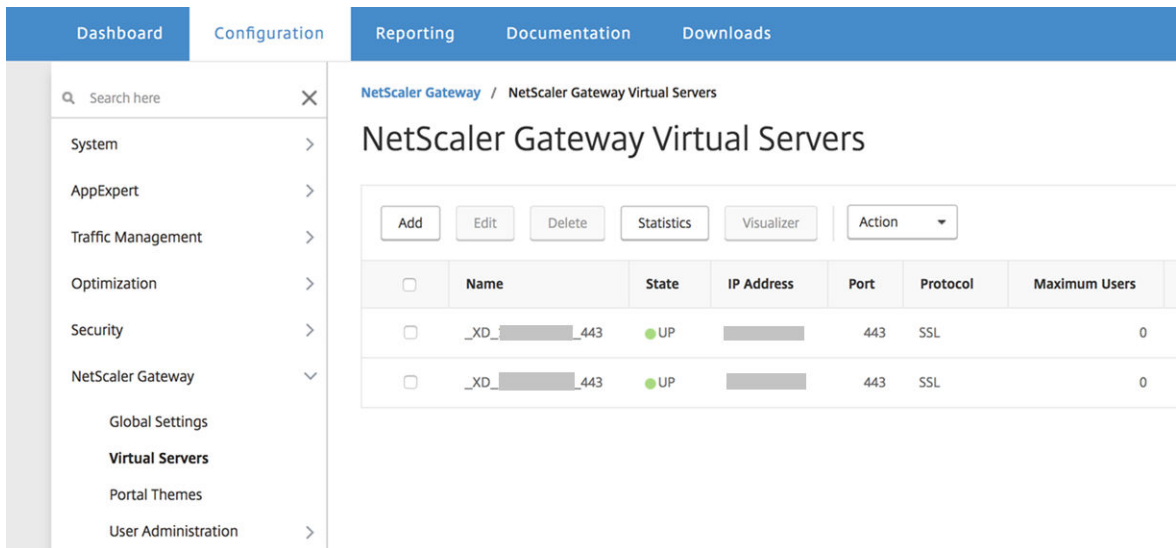
## Obtain the STA Server URL for the NetScaler Gateway

Before you configure NetScaler Gateway settings in VMware Identity Manager, obtain the URL of the Secure Ticket Authority (STA) server associated with the NetScaler Gateway appliance.

This procedure depicts the steps for NetScaler 11.

### Procedure

- 1 In the NetScaler management interface, navigate to **Configuration > NetScaler Gateway > Virtual Servers**.



- 2 Double-click the virtual server.
- 3 In the window that appears, under **Published Applications**, click **STA Server**.

**Profiles**

Net Profile -  
 TCP Profile **nstcp\_default\_XA\_XD\_profile**  
 HTTP Profile **nshhttp\_default\_strict\_validation**

---

**Published Applications**

**No** Next HOP Server

**1** STA Server

**No** Url

4 Make a note of the Secure Ticket Authority Server URL.

**VPN Virtual Server STA Server Binding**

	Secure Ticket Authority Server	Secure Ticket Authority Server Address Type	State
<input type="checkbox"/>			
<input type="checkbox"/>	http://mit.example.com	IPV4	● UP

## Configure NetScaler Gateway in VMware Identity Manager

To configure NetScaler Gateway in VMware Identity Manager, specify a Secure Ticket Authority (STA) server for each XenApp farm in your Citrix deployment. The STA server is used to generate and validate STA tickets during the application or desktop launch process.

When a user launches a Citrix application or desktop, VMware Identity Manager obtains a ticket from the STA server. The ticket is presented to NetScaler Gateway, along with other information, and NetScaler Gateway validates the ticket with the STA server before establishing a secure connection to the XenApp farm.

---

**Note** The information in this topic also applies to Citrix Secure Gateway.

---

### Prerequisites

- Obtain the STA server information for each XenApp farm. See [Obtain the STA Server URL for the NetScaler Gateway](#).

### Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Click the collection for which you want to specify an STA server, then click **Edit**.
- 3 In the Edit Citrix XenApp Collection wizard, click **Server Farm** in the left pane.

- 4 Click the server farm to edit.
- 5 Scroll down to the **STA Server** section and click **Add STA Server**.
- 6 Enter the STA server URL in the following format:

*transporttype://server:port*

For example: **http://staserver.example.com:80**

Only alphanumeric characters, period (.), and hyphen (-), are allowed in the URL.

- 7 Add additional STA servers, if necessary, by clicking **Add STA Server**.  
Your deployment may include a second STA server for failover purposes, for example.
- 8 If you added multiple STA servers, arrange them in failover order by clicking the handle at the left of each row and dragging the row to the desired position.
- 9 Click **Save**.
- 10 If there are multiple XenApp farms in your deployment, repeat these steps to specify an STA server for each farm.

#### What to do next

Configure policies for specific network IP ranges that specify that launch traffic should be routed through NetScaler Gateway to the XenApp server.

### Configure Network Range for NetScaler Gateway

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 is typically used to provide external access to Citrix-published resources.

When a user launches an application or desktop from the Workspace ONE 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 Resource Launch for Internal Networks](#).

---

**Note** The information in this topic also applies to Citrix Secure Gateway. If you are using Citrix Secure Gateway instead of NetScaler Gateway, enter the Secure Gateway host name and port, and select the NetScaler check box.

---

#### Prerequisites

- You have configured NetScaler Gateway in the Citrix virtual apps collection, as described in [Configure NetScaler Gateway in VMware Identity Manager](#).
- A Super Admin role is required to perform this procedure.

**Procedure**

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps Collections** tab.
- 2 Click the Citrix collection for which you want to set network ranges.
- 3 Click **Edit Network Range**.
- 4 In the Network Ranges page, click the network range to configure for Netscaler Gateway.
  - a Click the network range to edit or click **Create Network Range** to create a new network range, if required.
  - b If you are creating a new network range, enter a name, optional description, and the IP address range.
  - c Scroll to the **XenApp 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
<b>Client Access FQDN</b>	The NetScaler Gateway appliance host name. For example: <b>netscalerhost.example.com</b>
<b>Port</b>	The NetScaler Gateway appliance port. For example: <b>443</b>
<b>NetScaler</b>	Set this option to <b>Yes</b> .

XenApp Farm UUID	XenApp Farm Server	Client Access FQDN	Port	NetScaler
acfa4389-feba-4651-945f-7d6a3bbee008	xenapptest.example.com	netscalerhost.example.com	443	Yes <input checked="" type="checkbox"/>

- e Click **Save**.
- f Repeat these steps to edit the other network ranges, if required.
- g Click **Finish** in the Network Ranges page.

## Configuring VMware Identity Manager Settings for Citrix Integration

You can configure several settings in VMware Identity Manager for the Citrix integration.

### Managing Categories for Citrix-Published Resources

You can use the VMware Identity Manager console and your Citrix deployment to manage Citrix-published resource categories.

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 VMware Identity Manager, existing category names for Citrix-published applications and desktops are carried over to VMware Identity Manager.

After the integration, you can continue to create categories in your Citrix deployment. If you enabled the **Sync categories from server farms** for the collection, the new categories are carried over to VMware Identity Manager during the next sync. See [Configuring Citrix Server Farms in VMware Identity Manager](#) .

You can also create categories directly in VMware Identity Manager. You create, assign, and view categories from the **Catalog > Virtual Apps** page in the VMware Identity Manager console.

When you create a category in VMware Identity Manager, the category does not appear in your Citrix deployment.

When you create a category in your Citrix deployment, the category appears in VMware Identity Manager at the next sync. When you update a category name in your Citrix deployment, the updated category name appears in VMware Identity Manager while the original category name remains. If you want to remove the original category name from VMware Identity Manager, you must remove it manually.

## Configuring Delivery Settings (ICA Properties) for Citrix-Published Resources

You can edit the delivery settings for Citrix-published resources in the VMware Identity Manager console. These settings define how the configured Citrix deployment delivers Citrix-published resources to users.

To configure delivery settings, you edit Independent Computing Architecture (ICA) properties. ICA is a Citrix proprietary protocol. A wide range of ICA properties are available, controlling areas such as security, display, and compression. For more information about configuring ICA properties, see the Citrix documentation.

VMware Identity Manager includes default delivery settings. These settings are global, that is, they apply to all Citrix-published resources in the VMware Identity Manager service. You can edit the default settings and add new ones.

### Editing ICA Properties for all Citrix-Published Resources

You can edit the delivery settings (ICA properties) for all Citrix-published applications and desktops in your VMware Identity Manager deployment. These settings are only applicable for collections that have the Web Interface SDK option selected.

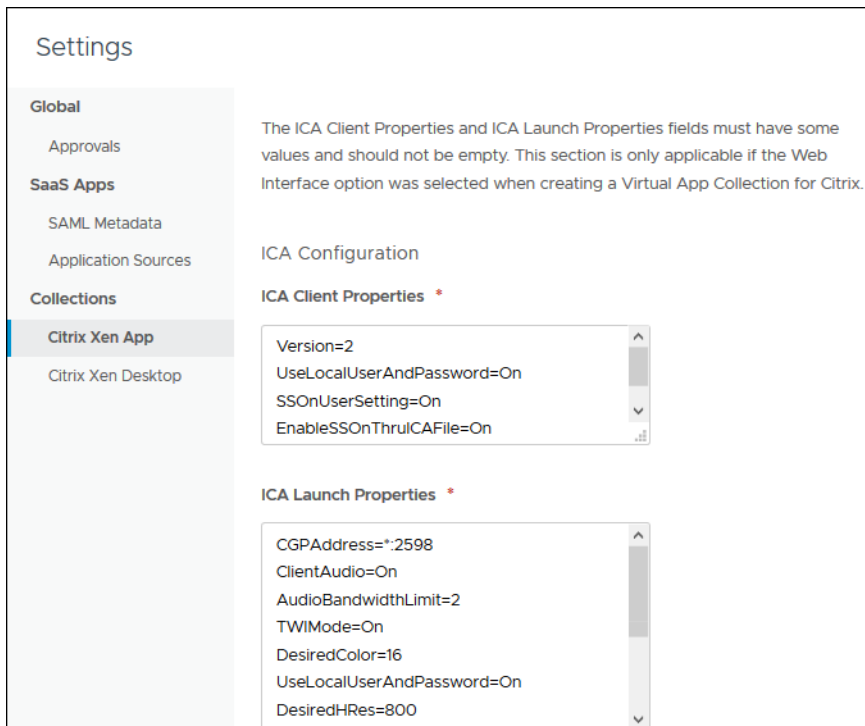
The ICA properties fields are populated with default values until you edit them.

#### Procedure

- 1 In the VMware Identity Manager console, select the **Catalog > Virtual Apps** tab, then click **Settings**.

- 2 In the left pane, click **Citrix XenApp** or **Citrix XenDesktop**, based on your deployment.
- 3 Edit the ICA properties according to Citrix guidelines.
  - To edit properties for launch traffic that goes directly to the XenApp or XenDesktop server, edit the **ICA Configuration** section.
  - To edit properties for launch traffic that is routed through NetScaler Gateway, edit the **NetScaler ICA Configuration** section.

For example:



- 4 Click **Save**.

## Results

Unless individual resources have their own resource delivery settings, your Citrix deployment applies the global ICA properties when it delivers Citrix-published resources available through VMware Identity Manager to users.

## Setting Access Policies for Specific Applications and Desktops

The default access policy set applies to all applications and desktops in your 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.

For detailed information on access policies and how they are applied, see the *VMware Identity Manager Administration Guide*.



## Procedure

- 1 To select an access policy for a specific application from the application configuration page, follow these steps.
  - a In the VMware Identity Manager 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 VMware Identity Manager 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 the VMware Identity Manager 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 VMware Identity Manager. You cannot edit the assignments from VMware Identity Manager.

### Prerequisites

To see the latest updates, manually sync resources and entitlements from the Citrix server farms to VMware Identity Manager from the **Catalog > Virtual Apps Collections** page.

### Procedure

- 1 Log in to the VMware Identity Manager 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
<b>List users and groups assigned to a specific Citrix-published application or desktop</b>	<ol style="list-style-type: none"> <li>Click the <b>Catalog &gt; Virtual Apps</b> tab.</li> <li>(Optional) Click the icon in the <b>Type</b> column heading and select <b>Citrix Published Application</b> and <b>Citrix Published Delivery Group</b> to view all Citrix-published resources. You can also search for an application or desktop by name.</li> <li>Click the desktop or application.</li> <li>Click <b>View Assignments</b>.</li> </ol> <p>All users and groups to whom the application is assigned are listed.</p>
<b>List Citrix-published application and desktop assignments for a specific user or group</b>	<ol style="list-style-type: none"> <li>Click the <b>Users &amp; Groups</b> tab.</li> <li>Click the <b>Users</b> tab or the <b>Groups</b> tab.</li> <li>Click the name of an individual user or group.</li> <li>Click the <b>Apps</b> tab.</li> </ol> <p>Citrix-published application and desktop assignments for the user or group are listed.</p>

## Launching Citrix-Published Resources in Different Browsers

When users launch a Citrix-published desktop or application from the Workspace ONE portal, an ICA file is downloaded and passed to the Citrix Receiver. Citrix Receiver is a native OS application which launches 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 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.

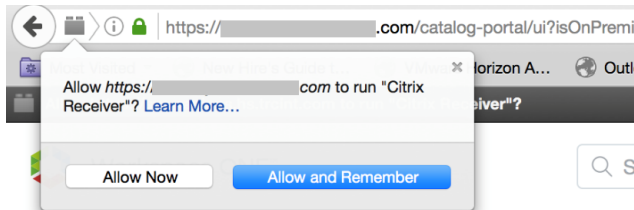
Platform	Browser	How the application or desktop is launched	Action Required
Windows	Firefox	Launches the application or desktop directly	None
	Chrome	Launches the application or desktop directly.	None
	Internet Explorer	Downloads the ICA file with a .ica extension. After the file type is associated with the Citrix Receiver, launches the application or desktop automatically.	In the browser, associate the .ica file type with the Citrix Receiver.

Platform	Browser	How the application or desktop is launched	Action Required
	Edge	Launches the application or desktop directly.	None
		<b>Note</b> With Citrix 4.5 Receiver and XenDesktop, there are known issues with delivery group launch.	
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 Receiver, launches the application or desktop automatically.	In the browser, associate the .ica file type with the Citrix Receiver.
Android	Chrome	Downloads the ICA file	Click the ICA file to launch the desktop or application.
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.

## Allowing Citrix Receiver Plugin on Firefox

On Firefox, when users launch a Citrix-published application, they are prompted to allow the Citrix Receiver plugin.

Allow <https://IdentityManagerHostname> to run Citrix Receiver?



Users must click **Allow Now** or **Allow and Remember** to launch the application.

## Upgrade Impact on Citrix-Published Resources Integration

No additional setup is required after a VMware Identity Manager upgrade or a Citrix product upgrade to maintain the integration between VMware Identity Manager and Citrix-published resources.

To upgrade Integration Broker, you must uninstall the older version and then install the new version.

To reinstall Citrix Receiver, see the Citrix documentation.

# Providing Access to Third-Party Managed Applications in Workspace ONE

## 9

You can add third-party identity providers as an application source in the Workspace ONE catalog to simplify the deployment of large numbers of applications from these third-party identity providers to Workspace ONE. 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 Workspace ONE portal from their desktop and mobile devices.

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 VMware Identity Manager 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 the Workspace ONE catalog.

- 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 Catalog](#)
- [Entitle Users to the Application Source](#)
- [Add Applications Managed by the Application Source](#)

## Add an Application Source to Workspace ONE Catalog

Configure the application source in the Catalog > Settings page to integrate third-party applications with the Workspace ONE catalog. After the application source is configured, you can add applications from the source to the Workspace ONE catalog.

The common configuration settings are set at the application source level. Applications from the application source that you add to the Workspace ONE 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 Identity Manager 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
<b>URL/XML</b>	Select URL/XML to use auto-discovery URL or meta-data XML or Manual <ul style="list-style-type: none"> <li>■ Auto-discovery (meta-data) URL. If the XML metadata is accessible on the Internet, provide the URL.</li> <li>■ 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.</li> <li>■ Manual configuration. If the XML metadata is not available to you, manually configure the XML in the text boxes that are displayed.</li> </ul>
<b>Relay State URL</b>	Enter a custom landing page that users are sent to by Workspace ONE after authenticating to the single sign-on URL.
<b>Advanced Configuration Options</b>	
<b>Sign Response</b>	Enabled. The entire response is signed.
<b>Sign Assertion</b>	Enable to sign the assertion.
<b>Encrypt Assertion</b>	If enabled, the SAML assertion is encrypted. For encryption to work, the ability to read encrypted SAML assertions must be supported.
<b>Include Assertion Signature</b>	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.
<b>Signature Algorithm</b>	Select SHA256 with RSA as the secure encrypted hash algorithm to use for the signature.
<b>Digest Algorithm</b>	Select SHA256.

Option	Description
<b>Application Login URL</b>	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.
<b>Enable Authentication Failure Notification</b>	If enabled, a SAML failure response is sent to the service provider when a login attempt fails.
<b>Proxy Count</b>	Set the proxy count to limit the number of proxy layers between the service provider and the authenticating identity provider.
<b>API Access</b>	Allow API access to this application.

- Click **Next**.
- 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

Set the entitlements for the application source to All Users. You can manage the entitlements from the specific application configuration pages.

### Procedure

- In the VMware Identity Manager console, in the **Catalog > Web Apps** page, select the application source from the list.
- Click **Assign**.
- Type **ALL USERS** in the search box to find and select the ALL USERS group.
- 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

After the identity provider is configured as an application source, web applications that use the SAML 2.0 authentication profile can be added to the Workspace ONE catalog.

### Prerequisites

Third-party identity provider configured as an application source in the Catalog > Settings page.

### Procedure

- 1 Log in to the VMware Identity Manager administration 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
<b>Name</b>	Enter the name of the application.
<b>Description</b>	(Optional) Add a description of the application.
<b>Icon</b>	<p>(Optional) To add an icon that displays in the users Workspace ONE application page, click <b>Choose File</b> to upload an icon.</p> <p>PNG, JPG, and ICON file formats, up to 4 MB, are supported. Uploaded icons are resized to 80px X 80px.</p> <p>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.</p>

- 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 the VMware Identity Manager Administration guide, Managing Access Policies section.

### Results

The application is added to the Workspace ONE catalog and users can access the application from their Workspace ONE 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 VMware Identity Manager Resource Configuration

# 10

You can troubleshoot issues that you or users experience after you configure VMware Identity Manager resources.

This chapter includes the following topics:

- [Troubleshooting Launch Errors](#)
- [Troubleshooting ThinApp Integration](#)
- [Troubleshooting Horizon Integration](#)
- [Troubleshooting Citrix-Published Resources Integration](#)

## Troubleshooting Launch Errors

You can troubleshoot Horizon, Horizon Cloud, and Citrix resource launch failures by viewing error messages about the root cause and suggested solutions in the VMware Identity Manager console.

### Procedure

- 1 In the VMware Identity Manager 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

Use this information to troubleshoot the ThinApp configuration in VMware Identity Manager.

### 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 VMware Identity Manager Desktop application even when the application is already installed and running.



## Problem

After installing the VMware Identity Manager 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 VMware Identity Manager Desktop application must be installed on the system, and prevents the ThinApp package from starting. This message might appear even when the VMware Identity Manager Desktop application process is running on the Windows system. The VMware Identity Manager Desktop application might report that all files are up to date.

## Cause

This problem can occur for multiple reasons.

Cause	Description
<p>The VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 disabled 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 disabled for the browser in which the user is trying to launch the ThinApp package.</p>	<p>In the Workspace ONE portal, ThinApp packages are represented using a link with a <code>horizon://</code> protocol. When the VMware Identity Manager 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 Workspace ONE portal, this <code>HorizonThinAppLauncher.exe</code> application is launched.</p> <p>If the user has disabled the use of all protocol handlers in the browser, or disabled the use of the handler for the <code>horizon://</code> protocol, ThinApp packages will not launch using their icons in the Workspace ONE 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 disabled 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 <b>No</b> or a similar choice to prevent the launch, and also selected <b>Remember my selection</b> 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 Workspace ONE portal.</p>

## Solution

- 1 Verify the user has logged in to the VMware Identity Manager Desktop application with the user's VMware Identity Manager user account.

The user signs into the client using the VMware Identity Manager 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>&lt;html&gt; &lt;script type="text/vbscript"&gt; On Error Resume Next  dim objName objName = "HorizonAgentFinder.HorizonFinder" dim obj Set obj = CreateObject(objName)  document.write(objName &amp; " is ") if IsEmpty(obj) then     document.write("not installed") else     document.write("installed") end if &lt;/script&gt; &lt;/html&gt;</pre>
Firefox	<p>Open Firefox's Add-ons Manager by clicking <b>Tools &gt; Add-ons</b>. On the Plugins page, verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate.</p>
Chrome	<p>Open Chrome's content settings by opening the Settings page and clicking <b>Show advanced settings &gt; Content settings</b>. Click <b>Disable individual plug-ins</b> to display the list of plugins. Verify the VMware Horizon Agent Finder browser plugin is listed and set it to always activate.</p>
Safari for Windows	<p>Open Safari's list of installed plugins by clicking <b>Help &gt; Installed Plug-ins</b>. Verify the VMware Horizon Agent Finder browser plugin is listed. Verify that plugin 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 VMware Identity Manager 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 VMware Identity Manager 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 VMware Identity Manager 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 disabled the horizon:// protocol for the browser, or if all protocol handlers are disabled 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 Horizon Integration

Use this information to troubleshoot the Horizon 7 or Horizon 6 configuration in VMware Identity Manager.

### Users Unable to Launch Horizon Applications or Desktops

Users are unable to launch Horizon 7 or Horizon 6 applications or desktops from the VMware Identity Manager user portal.

#### Problem

Users are unable to launch Horizon 7 or Horizon 6 applications or desktops from the VMware Identity Manager user portal and the following error appears in the user interface:

Error launching resource. Please contact your IT Administrator.

#### Cause

This error might occur if the SAML metadata on the Horizon Connection Server instances expired after the last sync.

## Solution

- 1 In the VMware Identity Manager console, click the **Catalog > Virtual Apps Collections** tab.
- 2 Select the Horizon virtual apps collection and click **Sync** to sync Horizon resources to VMware Identity Manager again.

## Troubleshooting Citrix-Published Resources Integration

Use this information to troubleshoot the Citrix-published resources configuration in VMware Identity Manager.

See also *Troubleshooting Citrix-Published Resources Configuration in VMware Identity Manager*.

### Citrix-Published Resources Are Not Available in VMware Identity Manager

A communication issue between Integration Broker and PowerShell SDK might prevent Citrix-Published Applications and Desktops from appearing in the VMware Identity Manager catalog.

You can specify URLs in a browser to troubleshoot where an Integration Broker configuration issue exists. This troubleshooting method can help you identify if the problem is a configuration issue in the following areas.

- The Citrix server farm
- Citrix-published resources
- Resource entitlements

If a Web page does not display the expected output, it displays an error and adds information to the Integration Broker logs. Review the Integration Broker logs to continue the troubleshooting process.

#### Problem

After you integrate Citrix with VMware Identity Manager, Citrix-published resources do not appear in the VMware Identity Manager catalog.

#### Cause

A configuration issue might exist with the Integration Broker setup that prevents proper communication with PowerShell SDK.

## Solution

- 1 Use a browser to check the Citrix server farm information.
  - a In a browser, enter a URL such as one of the following, replacing the placeholders with the appropriate information.
    - Citrix Server Farm 7.x  
`https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenAppServerHostname&xenappversion=Version7x`
    - Citrix Server Farm 6.5  
`https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenAppServerHostname&xenappversion=Version65orLater`
    - Citrix Server Farm 5.5 or 6.0  
`https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=XenAppServerHostname&xenappversion=Legacy`
  - b Review the content of the Web page and, if necessary, review the Integration Broker logs.

If Integration Broker is properly configured, the page displays Citrix server farm information, such as the following.

```
"[{"FarmName\\":\\"test data\\",\\"ServerVersion\\":\\" 6.0.6410\\",\\"AdministratorType\\":\\"Full\\",\\"SessionCount\\":\\"2\\",\\"MachineName\\":\\"test data\\"}]"
```

If the Web page does not display the server farm information, log information is sent to the Integration broker. To further troubleshoot the issue, review the logs on the Integration Broker host at `%programdata%/VMware/ HorizonIntegrationBroker`.

**2** Use a browser to list all Citrix-published resources in the server farm.

- a In a browser, enter a URL such as one of the following, replacing the placeholders with the appropriate information.

■ Citrix Server Farm 7.x

To list all applications:

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?  
computerName=XenAppServerHostname&xenappversion=Version7x
```

To list all delivery groups:

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/deliveryGroups?  
computerName=XenAppServerHostname&xenappversion=Version7x
```

■ Citrix Server Farm 6.5

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?  
computerName=XenAppServerHostname&xenappversion=Version65orLater
```

■ Citrix Server Farm 5.5 or 6.0

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/applications?  
computerName=XenAppServerHostname&xenappversion=Legacy
```

- b Review the content of the Web page and, if necessary, review the Integration Broker logs.

If Integration Broker is properly configured, the page displays a list of all the resources in the Citrix server farm.

If the Web page does not display a list of resources, log information is sent to the Integration broker. To further troubleshoot the issue, review the logs on the Integration Broker host at %programdata%/VMware/HorizonIntegrationBroker.

### 3 Use a browser to check the entitlements for a single Citrix-published resource.

- a In a browser, enter a URL such as one of the following, replacing the placeholders with the appropriate information.

Replace the *ApplicationName* place holder with the name of the application you are specifying.

- Citrix Server Farm 7.x

To check an application:

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?
computerName=XenAppServerHostname&xenappversion=Version7x&appName=Applic
ationName
```

To check a delivery group:

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/deliveryGroup/
entitlements?
computerName=XenAppServerHostname&xenappversion=Version7x&deliveryGroupN
ame=deliveryGroupName
```

- Citrix Server Farm 6.5

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?
computerName=XenAppServerHostname&xenappversion=Version65orLater&appNa
me=ApplicationName
```

- Citrix Server Farm 5.5 or 6.0

```
https://IBhostname/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?
computerName=XenAppServerHostname&xenappversion=Legacy&appName=Applic
ationName
```

- b Review the content of the Web page and, if necessary, review the Integration Broker logs.

If Integration Broker is properly configured, the page displays a list of all the entitlements for the application or delivery group you specified.

If the Web page does not display a list of entitlements, log information is sent to the Integration broker. To further troubleshoot the issue, review the logs on the Integration Broker host at %programdata%/VMware/HorizonIntegrationBroker.

## Unable to Launch Citrix Published Applications or Desktops

Administrators or users cannot launch any Citrix published applications or desktops to which they are entitled.

### Problem

Citrix published applications, desktops, and user entitlements sync to VMware Identity Manager but administrators or users cannot launch the applications or desktops to which they are entitled.

## Solution

To troubleshoot this issue, log in to the Windows Server on which the Integration Broker is installed and verify that you can run the application or desktop directly using the Citrix interface.

If you are unable to run the application or desktop directly from the Integration Broker server, check the firewall settings on the Integration Broker server and verify that ports required for the XenApp servers are not blocked.

## Users Accessing Citrix-Published Resources Receive an Encryption Error

The ICA properties in VMware Identity Manager must include the encryption property set to the same encryption level as configured on the XenApp servers in the farm, otherwise users cannot access their Citrix-published applications or desktops.

### Problem

When a user connects to a Citrix-published resource from VMware Identity Manager, the following error message is displayed.

You do not have the proper encryption level to access this Session

### Cause

VMware Identity Manager does not set encryption levels. If the encryption level on the XenApp server is set higher than the default setting used in the Citrix Receiver, users see this error.

You must set a higher encryption level in VMware Identity Manager.

### Solution

- 1 Log in to the VMware Identity Manager console.
- 2 Click the **Catalog > Virtual Apps** tab, then click **Settings**.
- 3 In the left pane, click **Citrix XenApp** or **Citrix XenDesktop**, based on your deployment.



- 4 Make the following changes in both the **ICA Configuration** and **Netscaler ICA Configuration** sections.
  - a In the **ICA Client Properties** text box, set the encryption level with the following property:  
**EncryptionLevelSession=EncRC5-128**  
This example sets the encryption level to 128 but you must modify it to the level configured on the XenApp servers.
  - b In the **ICA Launch Properties** text box, set the encryption level by entering or editing the following property:  
**[EncRC5-128]**  
**DriverNameWin16=fdc128w.dll**  
**DriverNameWin32=fdc128n.dll**  
This example sets the encryption level to 128 but you must modify it to the level configured on the XenApp servers.

## When Users Launch a Citrix-Published Resource, the Browser Displays 500 Internal Server Error

A mismatch between the configurations of the Citrix server farm and VMware Identity Manager might cause the launch of Citrix-published resources to fail.

### Problem

Launching a Citrix-published resource fails as the browser displays 500 Internal Server Error.

### Cause

A 500 error occurs when the Citrix server farm information provided in the VMware Identity Manager console does not match the Citrix server configuration.

### Solution

- 1 Note the settings of the transport type, port number, and SSL relay port number of each server farm integrated with your VMware Identity Manager deployment.
- 2 Log in to the VMware Identity Manager console.
- 3 Select the **Catalog > Virtual Apps Collections** tab.
- 4 Click the Citrix virtual apps collection, then click **Edit**.
- 5 In the Edit Citrix XenApp Collection wizard, click **Server Farm** in the left pane, then click the server farm to edit.
- 6 Under **Launch Preference, Web Interface SDK**, change the **Transport Type, Port, and SSL Relay Port** settings to match the settings in your Citrix server configuration.
- 7 Click **Save**.
- 8 Repeat these steps to modify the settings for each server farm.

## Memory Issue Prevents Proper Configuration of Integration Broker

When you integrate VMware Identity Manager with Citrix server farm versions 6.0 and earlier, insufficient memory allotted to PowerShell SDK results in an error.

You can increase the memory allotted to the PowerShell SDK.

### Problem

When you issue the `Invoke-Command` command to verify PowerShell remoting, an error related to insufficient memory appears. You are instructed to issue the `Invoke-Command` command when preparing the integration broker server for Windows.

### Cause

On the Windows system where PowerShell remoting is executed, the memory allotted to PowerShell SDK might be insufficient for the number of Citrix-published resources.

### Solution

- 1 When the error appears, issue the command to increase the allotted memory. For example,

```
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="1024"}'
```

- 2 Reissue the `Invoke-Command` command and complete the task.

## 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 Identity Manager 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 for the Integration Broker.

### Problem

If SSL is enabled for the Integration Broker, 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.

## Launch of Citrix-published Resources Fails if XML Port is Set Incorrectly

Launch of Citrix-published resources from a Citrix 7.x or 6.x server farm fails if the XML Port is set incorrectly in VMware Identity Manager.

### Problem

Launch of Citrix-published resources from a Citrix 7.x or 6.x server farm fails if the XML Port is set incorrectly in VMware Identity Manager.

### Solution

Ensure that the XML port is set correctly.

In a XenApp 6.x or earlier environment, ask the Citrix administrator to run CTXXMLS.EXE to verify the port or browse to the following location within the registry on the XenApp Management server:

```
HKLM/SYSTEM/CurrentControlSet/Services/CtxHttp | TcpPort=
```

Verify the port number. By default the port is set to 80, but it is commonly changed to 8080 or 88. Ensure that the correct port is set in the VMware Identity Manager Citrix configuration in the **Catalog > Manage Desktop Applications > Citrix Published Application** page.

For XenDesktop 7.x, see <https://support.citrix.com/article/CTX127945> for information on verifying the XML port.

## Citrix Resource Sync Fails if Limited Visibility Group Does Not Contain Any Users or Groups

Citrix resource sync fails if the Limited Visibility Group setting is selected and if it does not contain any AD users or groups.

### Problem

In XenDesktop and XenApp 7.9 and later, if the Limited Visibility Group setting is selected and if it does not contain any users or groups, sync to VMware Identity Manager fails.

### Cause

If set, the Limited Visibility Group must contain users or groups.

### Solution

- 1 Find the actual name of the application by running the following PowerShell command:

```
asnp citrix*
```

```
Get-brokerapplication-browsername nameOfCitrixPublishedResource
```

In the application detail that is displayed, look for the name of the application.

- 2 In Citrix Studio, find the application with that name, edit the Limited Visibility property, and add users and groups to the list.

## 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 VMware Identity Manager 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 stops the sync to VMware Identity Manager from working.

You can use the following API to check the issue:

```
http://CitrixBrokerFQDN:80/IB/API/RestServiceImpl.svc/hznxenapp/admin/entitlements?  
computerName=IBFQDN&xenappversion=VersionNumber&appName=applicationName
```

The resulting file contains empty resources. Example output:

```
"[{"IncludedUsers\":"DomainName\\\\"USERNAME:User  
$S-1-5-21-1097426297-1557994628-1672037986-53944:Group\"}]"
```

### 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 VMware Identity Manager

Citrix entitlements do not appear in VMware Identity Manager.

### Problem

Entitlements to an application or delivery group are set on the Citrix server but they do not appear in VMware Identity Manager.

### Cause

Users and groups that are entitled to the application or delivery group may not be synced to VMware Identity Manager.

### Solution

Ensure that the users and groups are synced to VMware Identity Manager.

- 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 VMware Identity Manager 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 VMware Identity Manager before you sync Citrix resources. If they do not exist, the sync will run but the entitlements will not be updated.

---

- 5 If the users and groups do not exist in VMware Identity Manager, perform these actions.
  - a Check where the users and groups exist in Active Directory (using Active Directory Users and Computers Snappin).
  - b In the VMware Identity Manager 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 VMware Identity Manager console, sync Citrix resources again.

When sync completes, the entitlements appear in VMware Identity Manager.

## Exception During Sync if Application Pool Identity is not Configured

An exception occurs during the sync of Citrix resources to VMware Identity Manager because of a common error in the Integration Broker setup, where the Identity setting has been configured for the wrong application pool.

### Problem

During sync, the following exception occurs in the Integration Broker log.

```
IntegrationBrokerLogger Error 1002 2017-04-04 19:10:38,936 (16)
HznXenIntegrationBroker.ApplicationExceptionHandler - Connecting to
remote server failed with the following error message : The client cannot connect to
the destination specified in the request. Verify that the service on the destination
is running and is accepting requests. Consult the logs and documentation for the WS-
Management service running on the destination, most commonly IIS or WinRM. If the
destination is the WinRM service, run the following command on the destination to
analyze and configure the WinRM service: "winrm quickconfig". For more information,
see the about_Remote_Troubleshooting Help topic. at
System.Management.Automation.Runspaces.AsyncResult.EndInvoke()
```

### Cause

This error occurs if the Identity setting is not configured correctly or if it is configured for the wrong application pool.

### Solution

Configure the Identity setting in the application pool that is attached to the Integration Broker. This may be different from the Default Application Pool.

To verify the correct application pool:

- 1 In IIS Manager, click **Application Pools** in the left pane.
- 2 Right-click the application pool and select **View Applications**.
- 3 Verify that the Integration Broker appears in the list of applications.

To configure the Identity setting for the application pool, follow the instructions in [Configure IIS Manager Settings for the Integration Broker Component of VMware Identity Manager](#).

## ICA File is not Created During Citrix Resource Launch

During launch of Citrix resources, the ICA file is not created and an exception occurs.

### Problem

When users try to launch a Citrix resource, the ICA file is not created and an exception such as the following appears in the Integration Broker log.

```
IntegrationBrokerLogger Information 1004 2017-05-02 11:50:42,093 (8)
HznXenIntegrationBroker.API.RestServiceImpl - Get ICA file contents for
AppNameCitrix.MPS.App.XA65Test.Airwatch Notepad Test, Farm Name: XA65Test, Server
Name: serverName, Username: user1 IntegrationBrokerLogger Error 1002 2017-05-02
11:50:42,093 (8) HznXenIntegrationBroker.ApplicationExceptionHandler -
WebPNBuilder implementation class WebPNImpl!
com.citrix.wing.webpnimpl.WebPNBuilderImpl not found at
com.citrix.wing.webpn.WebPNBuilder.getInstance() at
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.CreateUserContext(UserPrincip
al userPrincipal, String appName, Configuration configuration) at
```

```
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFileCommon(UserPrincipal userPrincipal, String appName, Configuration configuration) at  
HznXenIntegrationBroker.XenAppSDK.Impl.XenAppSDKClient.GenerateICAFile(UserPrincipal userPrincipal, String farmName, String serverName, String serverPort, String  
appName, XMLServiceTransportProtocol xmlserviceTransportProtocol, Int32 sslRelayPort)
```

#### **Solution**

Re-install Microsoft Visual J# 2.0 in the Integration Broker server.

## **Restarting Integration Broker**

If the Integration Broker fails to respond, restart IIS on the Windows server.

#### **Problem**

The Integration Broker fails to respond and needs to be restarted.

#### **Solution**

- 1** Open the Command Prompt window as administrator.
- 2** Type `iisreset`.