

VMWARE HORIZON CLOUD WITH VMWARE IDENTITY MANAGER QUICK START GUIDE

Table of Contents

Introduction to Horizon Cloud with VMware Identity Manager.3

Benefits of Integration.3

 Single Sign-On 3

 Two-Factor Authentication 3

 True SSO Support 3

Getting Started 4

 Prerequisites 4

 VMware Identity Manager Tenant 4

 VMware Identity Manager Windows Connector Server. 4

 Active Directory Requirements. 5

 Service Accounts 6

 Networking Port Requirements for VMware Identity Manager
Connector and Horizon Cloud. 6

 Network Configuration Requirements 7

 VMware Identity Manager Connector Installer for Windows 7

Architecture 8

 VMware Identity Manager Connectors Deployed in Horizon Cloud 8

 VMware Identity Manager Connectors Deployed On Premises 9

Quick Start Steps10

 Install VMware Identity Manager Connector for Windows. 10

 Activate VMware Identity Manager Connector17

 Set Up a Directory17

 Enable Outbound Mode for the VMware Identity Manager Connector 18

 Create Virtual Apps Collection for Horizon Cloud 18

 Configure Horizon Cloud Hosted. 18

Appendix A - Enforce SAML-Based Authentication19

Appendix B - Custom ID Mapping 20

About the Author 20

Introduction to Horizon Cloud with VMware Identity Manager

Welcome to the *VMware Horizon® Cloud Service™ with VMware Identity Manager™ Quick Start Guide*. This guide will help you quickly install and configure the VMware Identity Manager Windows Connector that is used with VMware Horizon Cloud with Hosted Infrastructure.

Note: This guide assumes you will be using the Windows version of the VMware Identity Manager Connector. This is the recommended version for Horizon Cloud and is also the only supported version when deploying into your Horizon Cloud Tenant using a utility server. If you are planning to use the Linux Virtual Appliance version of the VMware Identity Manager Connector for your on-premises deployment, please see [Installing and Configuring VMware Identity Manager](#) for step-by-step instructions.

VMware Identity Manager is a component of VMware Workspace ONE™, which provides a simple and secure enterprise platform that allows end users to access their applications, data, and services from any device, anywhere. It provides a single user interface (UI) through the Workspace ONE enterprise catalog, to deliver applications to end users.

Benefits of Integration

The integration of Workspace ONE and Horizon Cloud provides a number of benefits.

Single Sign-On

One of the primary advantages that Workspace ONE and Horizon Cloud provide is secure, single sign-on (SSO) access to both virtual desktops and applications. This provides simplicity and ease of access while maintaining security. Users can use either the Workspace ONE web-based portal from any HTML5 web browser or the Workspace ONE application. When used with an iOS-based device, users can also use touch ID for SSO.

Two-Factor Authentication

Workspace ONE supports multiple multi-factor authentication using RSA, Radius, Certificate, Kerberos, and VMware Verify™ to protect your environment beyond the basic user ID and password. Workspace ONE also provides two-factor authentication (2FA) for Horizon Cloud to secure your digital workspace.

In addition, you can use step-up authentication, which allows for additional multi-factor authentication beyond the initial authentication into Workspace ONE when accessing a desktop or application. This increases security by requiring two-factor authentication to access a specific desktop or application, even if you don't require it to access Workspace ONE.

True SSO Support

Horizon Cloud with True SSO support provides a seamless sign-on experience to desktops and applications when using 2FA with Workspace ONE. With True SSO, a user can log into Workspace ONE using any non-AD method such as RSA SecurID, SmartCard, Certificate, Radius, and any other supported 2FA method, and once authenticated, launch their desktop and application without being prompted for their AD password. True SSO removes the cumbersome login experience of prompting users for their AD password when launching their desktop or applications.

Getting Started

Two service accounts are required for setup of VMware Identity Manager.

To get started, verify that you have the appropriate Windows Server(s) that will run the VMware Identity Manager Connector, either in your Horizon Cloud Tenant as a utility server or on-premises server if using VPN/Direct Connect, and then download the VMware Identity Manager Connector software.

Prerequisites

This section details the prerequisites of the installation.

VMware Identity Manager Tenant

You must have administrative access to the VMware Identity Manager Tenant.

VMware Identity Manager Windows Connector Server

The VMware Identity Manager Windows Connector Server has the following requirements.

- Windows Server 2012 R2 server is available and meets the following specifications. If deploying into Horizon Cloud as a utility server, please note the Horizon Cloud Virtual Machine Model that is required.

NUMBER OF USERS	UP TO 1,000	1,000 TO 10,000	10,000 TO 25,000
vCPU	2	4	4
RAM (GB)	6	6	8
Disk Space (GB)	50	50	50
Horizon Cloud VM Model	Premium	Premium	Premium

Table 1: Windows Server 2012 R2 Specifications

Note: VMware recommends multiple Connector Servers to be deployed for High Availability—see [Configuring High Availability for the VMware Identity Manager Connector](#).

- DNS entry and a static IP for the Windows Server
 - Forward and reverse DNS records
- Ports 80 and 8443 must be available on the Windows Server. If these ports are being used by other services, you will not be able to install the VMware Identity Manager Connector component.
- The Windows Server must be joined to the domain. You must install the VMware Identity Manager Connector component as a domain user that is part of the administrator group on the Windows Server. You then need to run the VMware Identity Manager Connector service as a domain user that is specified during installation, in the following cases.
 - If you plan to connect to Active Directory (Integrated Windows Authentication)
 - If you plan to use Kerberos authentication

- For the installer to be able to browse to and validate domains and users during installation, the following requirements must be met.
 - The target system must be domain joined.
 - The Computer Browser service must be enabled and running.
 - Firewall must be configured with an exception for the Computer Browser service.
 - NetBIOS over TCP/IP must be enabled on the target system.
 - A master browser system should be configured on the network.
 - Broadcast traffic should be enabled on the network.

If you will be installing the VMware Identity Manager Windows Connector in your Horizon Cloud Tenant and do not have a Windows Server 2012 R2 utility server available, contact VMware Support and request for one to be provisioned based on Table 1. For more information on utility servers in Horizon Cloud with Hosted Infrastructure, see Appendix A - Ordering in the [Horizon Cloud Service Description](#).

Active Directory Requirements

VMware Identity Manager Connector supports the following Active Directory on Windows Server versions:

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

Domain function level of Windows 2003 and later is supported.

For Active Directory LDAP and IWA integration with VMware Identity Manager, a Bind DN user account is required in order to connect to Active Directory. This account should have a non-expiring password. See Service Accounts for more information.

Service Accounts

Two service accounts are required for setup of VMware Identity Manager.

The Bind DN user account is used for Active Directory LDAP and IWA integration with VMware Identity Manager. This account should have a non-expiring password.

The VMware Identity Manager Connector Service account is used to run the VMware Identity Manager Connector service on the Windows Server specified during the installation of VMware Identity Manager Connector. This account should be a domain user with a non-expiring password.

Networking Port Requirements for VMware Identity Manager Connector and Horizon Cloud

Table 2 details the port requirements.

SOURCE COMPONENT	DESTINATION COMPONENT	PORT	PROTOCOL	NOTES
VMware Identity Manager Connector	VMware Identity Manager Service	443	HTTPS	Default port. This port is configurable.
Browsers	VMware Identity Manager Connector	8443	HTTPS	Administrative port. Required.
Browsers	VMware Identity Manager Connector	80	HTTP	Required.
VMware Identity Manager Connector	Active Directory	389, 636, 3268, 3269		Default ports. These ports are configurable.
VMware Identity Manager Connector	DNS server	53	TCP/UDP	
VMware Identity Manager Connector	Domain controller	88, 464, 135, 445	TCP/UDP	
VMware Identity Manager Connector	Horizon Cloud Tenant Appliance	443	HTTPS	Required to sync Horizon Cloud Entitlements to VMware Identity Manager.
Horizon Cloud Tenant Appliance	VMware Identity Manager Service	443	HTTPS	Required to create a trust relationship between Tenant Appliance and VMware Identity Manager Service.

Table 2: Networking Port Requirements

Network Configuration Requirements

Ensure that outbound firewall port 443 is open from the VMware Identity Manager Connector Server and the Horizon Cloud Tenant Appliance to your VMware Identity Manager Service URL.

Note: If you are using the VMware-provided Internet connection for outbound Internet traffic, then no firewall changes will need to be made for the VMware Identity Manager Connector Server and the Horizon Cloud Tenant Appliance.

See the VMware Knowledge Base article [VMware Identity Manager Cloud Hosted IP Address Change \(2149884\)](#) for the list of VMware Identity Manager Service IP addresses to which the VMware Identity Manager Connector and the Horizon Cloud Tenant Appliance must have access.

VMware Identity Manager Connector Installer for Windows

Please ensure you have downloaded the VMware Identity Manager Connector Installer for Windows executable, which is part of your Horizon Cloud software entitlement and is accessible from the server that will be used for VMware Identity Manager Connector.

Architecture

VMware Identity Manager Windows Connector can be implemented as a utility server in your Horizon Cloud Tenant or on premises in your data center. Multiple VMware Identity Manager Connector Servers are deployed in both scenarios in order to ensure High Availability of the Connector Service. If one of the connectors becomes unavailable, both authentication and entitlement synchronization remain available.

The VMware Identity Manager Connectors are also configured in Outbound Mode, which requires no inbound Internet access to function. The connector communicates with the VMware Identity Manager Service through a websocket-based communication channel on HTTPS 443. The Horizon Cloud Tenant Appliance also needs outbound access to the VMware Identity Manager Service on HTTPS 443. Split DNS is also used for Horizon Cloud, with the internal Horizon Cloud URL pointing to the Internal Unified Access Gateway load-balanced virtual IP (VIP) address.

VMware Identity Manager Connectors Deployed in Horizon Cloud

This section describes the integration process for a Horizon Cloud deployment of the VMware Identity Manager Connector.

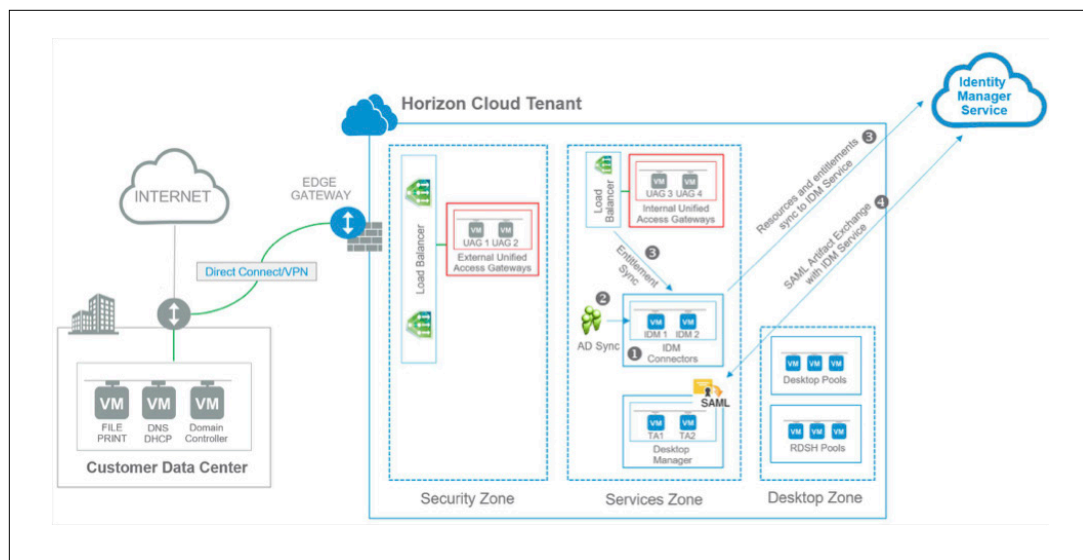


Figure 1: Horizon Cloud Deployment Architecture

1. VMware Identity Manager Connector is installed and configured on utility servers inside Horizon Cloud Tenant.
2. VMware Identity Manager Connector synchronizes Active Directory User and Groups.
3. Horizon Cloud user and group entitlements are synchronized from Horizon Cloud via the Internal Horizon Cloud URL to the VMware Identity Manager Service, through the VMware Identity Manager Connector.
4. Horizon Cloud Tenant Appliances exchange a SAML artifact with VMware Identity Manager Service.

VMware Identity Manager Connectors Deployed On Premises

This section describes the integration process for an on-premises deployment of the VMware Identity Manager Connector.

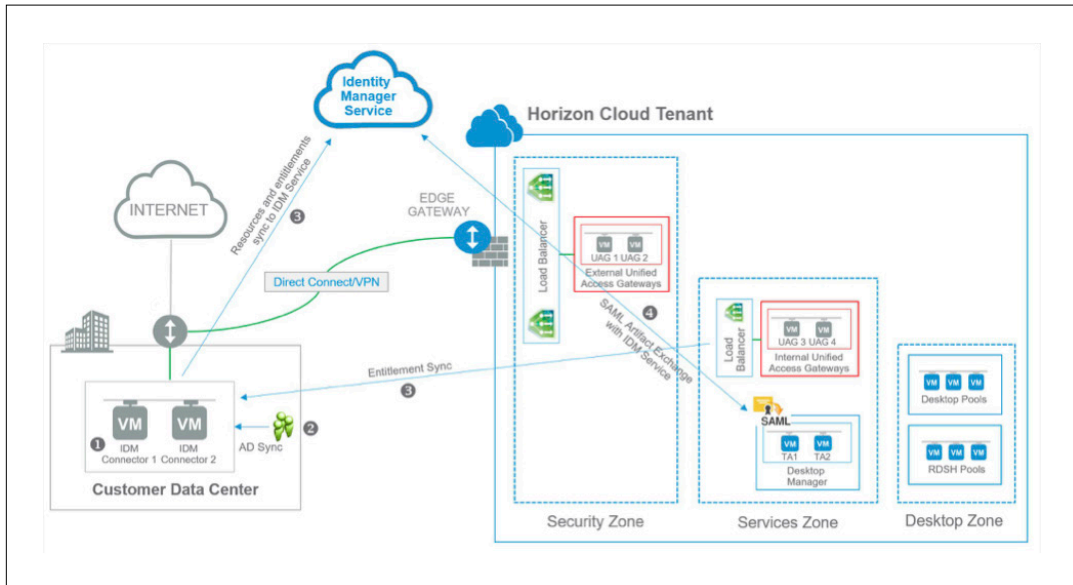


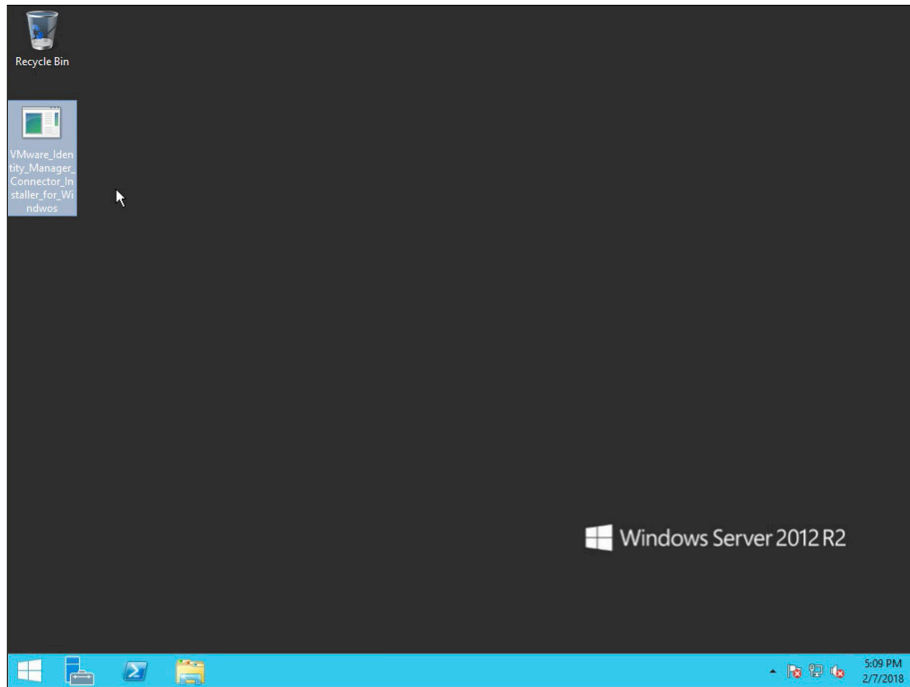
Figure 2: On-Premises Deployment Architecture

1. VMware Identity Manager Connector is installed and configured in an on-premises data center.
2. VMware Identity Manager Connector synchronizes Active Directory User and Groups.
3. Horizon Cloud user and group entitlements are synchronized from Horizon Cloud via the Internal Horizon Cloud URL to the VMware Identity Manager Service, through the VMware Identity Manager Connector.
4. Horizon Cloud Tenant Appliances exchange a SAML artifact with VMware Identity Manager Service.

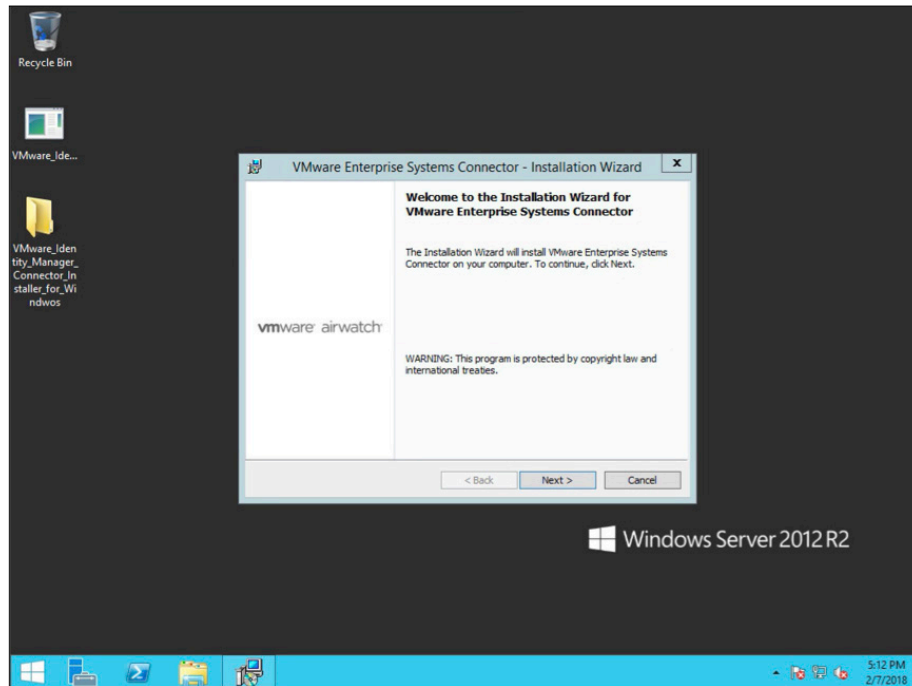
Quick Start Steps

The following tasks will guide you through the installation and configuration of the VMware Identity Manager Connector with Horizon Cloud. Please ensure that you have completed the prerequisites before continuing.

Install VMware Identity Manager Connector for Windows



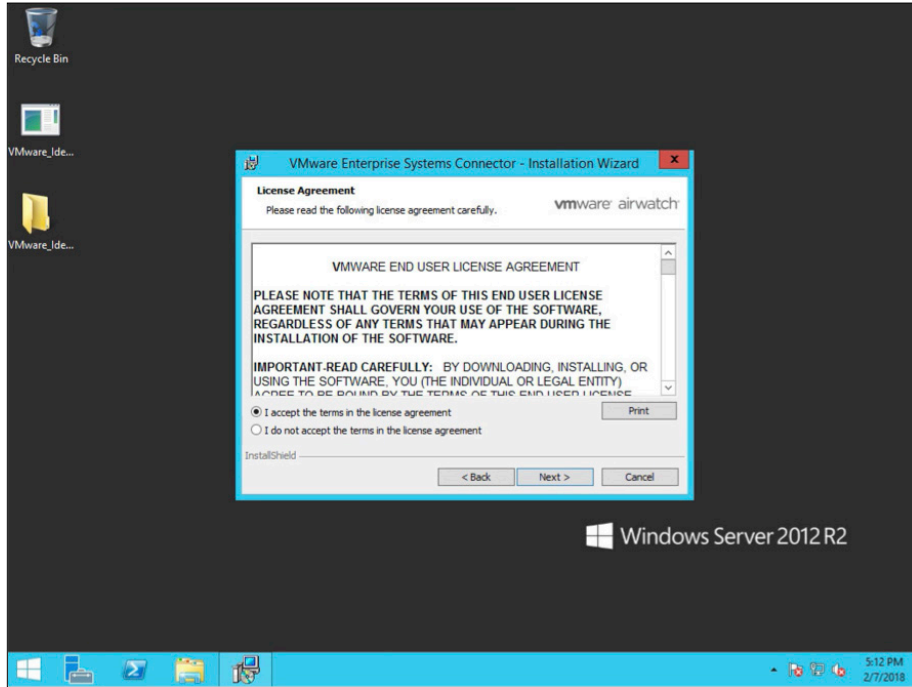
1. Double-click the `VMware_Identity_Manager_Connector_Installer_for_Windows.exe` installer.
Note: Some screens might reference the Enterprise Systems Connector, which the VMware Identity Manager Connector for Windows is part of.



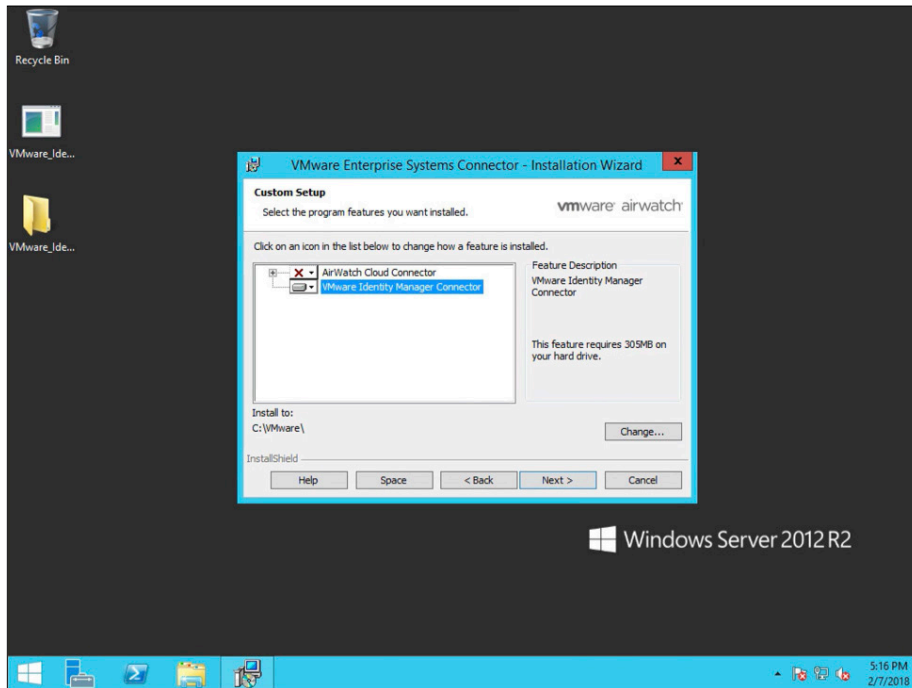
2. On the Welcome screen, click **Next**.

The installer verifies prerequisites on the server. If .NET Framework is not installed, you will be prompted to install it and to restart the server. After restarting, run the installer again to resume the installation process.

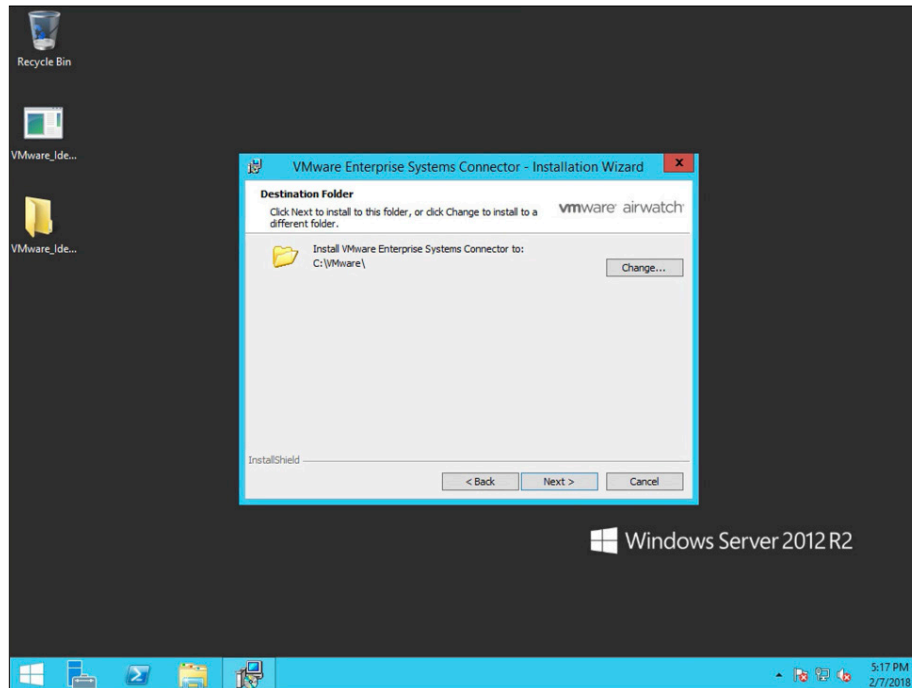
If a previous version of VMware Identity Manager Connector is installed, the installer auto-detects it and offers the option to upgrade to the latest version.



3. Accept the license agreement, then click **Next**.



4. In the Custom Setup page, deselect **AirWatch Cloud Connector** and select **VMware Identity Manager Connector**.

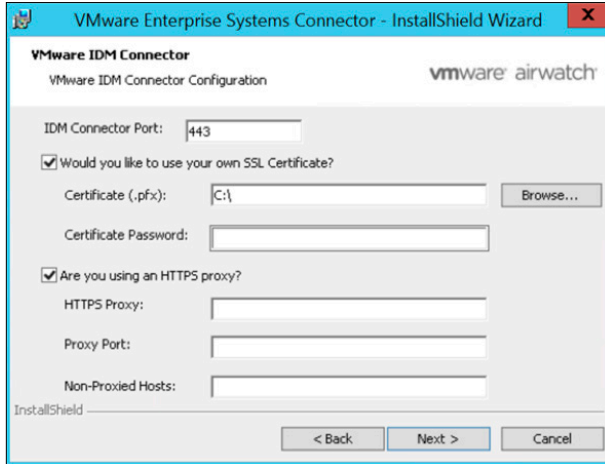


5. Select **Change** to change the installation directory, if required, then click **Next**.

The VMware Identity Manager Connector component requires the Java Runtime Environment (JRE). If the Windows Server does not have JRE installed, or if it has a version earlier than the one packaged with the installer, you are prompted to install it. Note that existing JRE versions are not deleted when the required version is installed.

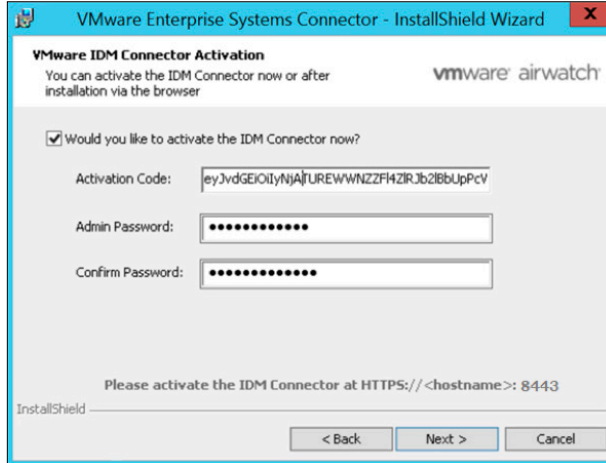
It is recommended to set Java to **never update** in order to ensure that newer versions are not installed.

6. Verify the destination folder, then click **Next**.



7. In the VMware Identity Manager Connector Configuration page, enter the following information then click **Next**.

OPTION	DESCRIPTION
VMware Identity Manager Connector Port	Enter a port number if you want the VMware Identity Manager Connector to run on a port other than 443.
Would you like to use your own SSL Certificate?	<p>By default, a self-signed certificate is generated for the VMware Identity Manager Connector during the installation process. You can install a signed certificate later by logging into the connector admin pages at <code>https://vidmConnectorHostname:8443/cfg/login</code> and navigating to the Install Certificate page.</p> <p>If you already have a certificate and want to install it now, select the check box, then select the certificate and enter the certificate password. The certificate must be in the PFX format.</p> <p>Note: A certificate is not required for VMware Identity Manager Connector when integrating with Horizon Cloud.</p>
Are you using an HTTPS proxy?	<p>Select to configure an HTTPS proxy server for outbound communications, if required.</p> <p>HTTPS Proxy – The proxy server URL. Proxy servers that require authentication are not supported.</p> <p>Proxy Port – The HTTPS proxy server port.</p> <p>Non-Proxied Hosts – Hosts that the VMware Identity Manager Connector can access without going through the proxy server. For example, localhost or hosts on the same subnet.</p>

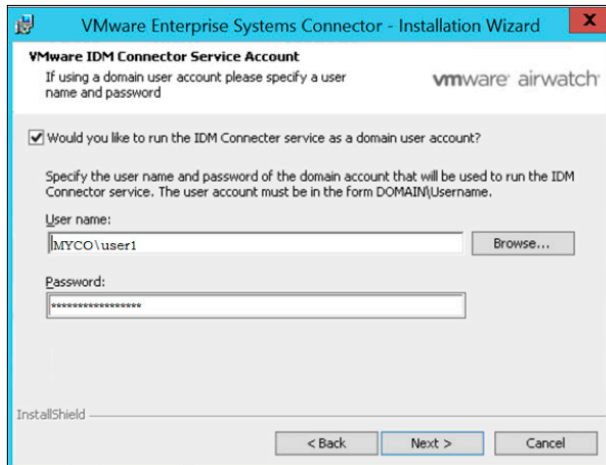


8. In the VMware Identity Manager Connector Activation page, select the check box if you want to activate the connector now.

If you do not activate the VMware Identity Manager Connector now, you can activate it later from `https://vidmConnectorHostname:8443`. For example, `https://myconnector.example.com:8443`.

OPTION	DESCRIPTION
Activation Code	To generate an activation code, log into the VMware Identity Manager Service administration console and copy and paste it here (see screenshot above). See Generate Activation Code for VMware Identity Manager Connector .
Admin Password	Create a password for the connector admin pages. You can access these pages to collect log file bundles and upload certificates.
Confirm Password	Enter the password again.

9. Click **Next**.



10. In the VMware Identity Manager Connector Service Account page, select the check box if you want to run the VMware Identity Manager Connector service as a Windows domain user.
You must run the service as a domain user in the follow cases:
 - If you plan to connect to Active Directory (Integrated Windows Authentication)
 - If you plan to use Kerberos authentication**Note:** To make any selections on this page, you must run the installer as a domain user that is part of the administrator group on the Windows Server. If you are unable to locate admins or users when you click **Browse**, verify that you have met the prerequisites.
11. Click **Next**.
12. Click **Install** to begin the installation.
13. Click **Finish**.

Activate VMware Identity Manager Connector

If you did not activate the VMware Identity Manager Connector during the installation of VMware Identity Manager Connector for Windows, please perform the following steps.

Note: Step 1 should be performed from the VMware Identity Manager administration console. When you first log in to VMware Identity Manager as the administrative user, click the username on the top right and select Administration Console.

1. [Generate Activation Code for VMware Identity Manager Connector](#)
2. [Activate the VMware Identity Manager Connector](#)

Set Up a Directory

After the VMware Identity Manager Connector is deployed and paired to the VMware Identity Manager Service, you can set up a directory in the VMware Identity Manager administration console. You can synchronize users and groups from your enterprise directory to the VMware Identity Manager Service.

In order to integrate with Horizon Cloud, you will need to ensure that the same users and groups that are entitled to applications and desktops in Horizon Cloud are also synchronized from your enterprise directory to the VMware Identity Manager Service.

VMware Identity Manager supports integrating the following types of directories when also integrated with Horizon Cloud:

- Active Directory over LDAP
- Active Directory Integrated Windows Authentication

VMware Identity Manager integrates with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests. See [Active Directory Environments](#) for more information on the requirements for each type of Active Directory configuration.

1. Log in to the VMware Identity Manager administration console.
2. Select the user attributes to sync to the directory.
 - a. Click the **Identity & Access Management** tab, then click **Setup**.
 - b. In the User Attributes tab, select which attributes are required, and add additional attributes if necessary.

If an attribute is marked *required*, only users with that attribute are synced to the service.

Important: Be aware of the following restrictions.

- After the directory is created, you cannot change an attribute from *optional* to *required*. You must make that selection now.
 - The settings in the User Attributes page apply to all directories in the service. When you make an attribute *required*, consider the effect on other directories.
3. Click **Manage, Directories** and then click **Add Directory** and select **Add Active Directory over LDAP/IWA**.
 4. See [Configuring Active Directory Connection to the Service](#) for more information on configuring Active Directory over LDAP or IWA.

Note: Horizon Cloud only supports sAMAccountName as the Directory Search Attribute for both Active Directory over LDAP and IWA. UserPrincipalName is currently not supported.

Enable Outbound Mode for the VMware Identity Manager Connector

Outbound Mode is the recommended configuration when integrating with Horizon Cloud, as it requires no inbound communication to the VMware Identity Manager Connector in order to function.

For more information, see [Enable Outbound Mode for the VMware Identity Manager Connector](#).

Create Virtual Apps Collection for Horizon Cloud

In order to integrate Horizon Cloud, a virtual apps collection must be created. Virtual apps collections contain 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.

1. [Creating Virtual Apps Collections](#)
2. [Configure Horizon Cloud Tenant in VMware Identity Manager](#)

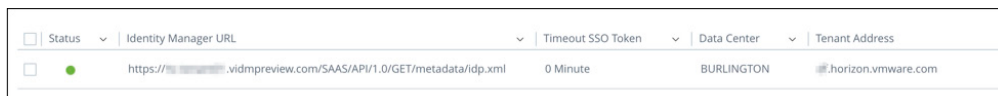
Configure Horizon Cloud Hosted

After you create the virtual apps collection in the VMware Identity Manager administration console, you need to configure SAML authentication in the Horizon Cloud administration console.

1. In the VMware Identity Manager Administration Console, click **Catalog**.
2. Click **Settings**.
3. Click **SAML Metadata**.
4. Click **CopyURL**, located to the right of Identity Provider (IdP) metadata, to copy the URL to your clipboard.
5. Log in to the Horizon Cloud Tenant.
6. Navigate to **Settings > Identity Management**.
7. Click **New**.
8. In the New VMware Identity Manager window, enter the following required information:

SETTING	DESCRIPTION
VMware Identity Manager URL	Enter the VMware Identity Manager IdP metadata URL.
Timeout SSO Token	Optional timeout value in minutes for the SSO token.
Data Center	Horizon Cloud Data Center.
Tenant Address	The Horizon Cloud Tenant Address. Example: <code>mytenant.customer.com</code> .

9. Click **Save**.
10. The Status of the newly created VMware Identity Manager should turn green if successfully paired with Horizon Cloud.

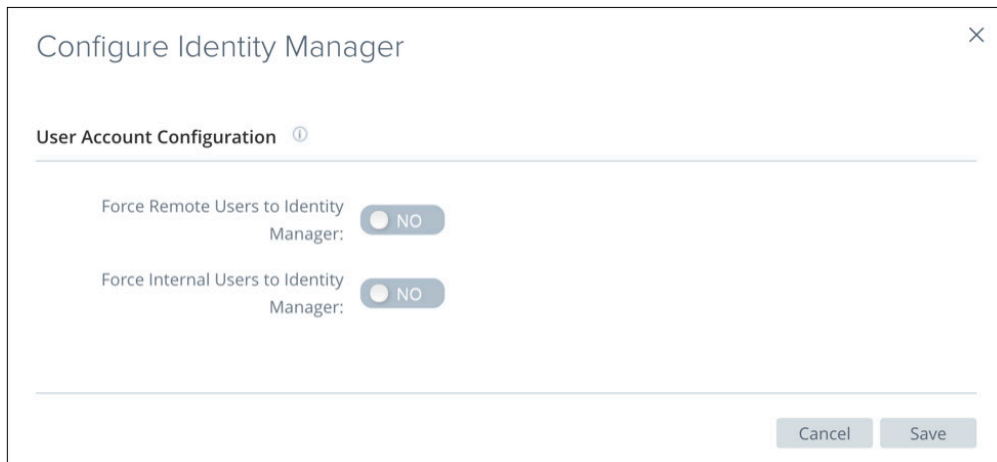


Your integration is now complete. You can view Horizon Cloud desktops and applications in the VMware Identity Manager administration console and end users can launch the desktops and applications to which they are entitled from the Workspace ONE portal or app.

Appendix A – Enforce SAML-Based Authentication

When configuring VMware Identity Manager with Horizon Cloud, you can force users to only authenticate through VMware Identity Manager. This can be set for both Remote and Internal users. After this is set, users will no longer be able to directly connect to the Horizon Cloud Tenant using the Horizon Client or HTML5 web page and must launch their desktops and applications from within VMware Identity Manager.

1. Log in to the Horizon Cloud Tenant.
2. Navigate to **Settings > Identity Management**.
3. Select **Configure**.



Configure Identity Manager

User Account Configuration ⓘ

Force Remote Users to Identity Manager: NO

Force Internal Users to Identity Manager: NO

Cancel Save

4. Enable Force Remote Users to Identity Manager and Force Internal Users to Identity Manager and click **Save**.

Appendix B - Custom ID Mapping

You can use Custom ID Mapping to customize the user ID that is used in the SAML response when users launch Horizon Cloud Desktops and Applications. You can resolve SSO launch failures that are caused by a mismatch of the user ID attribute between VMware Identity Manager and Horizon Cloud.

This setting is particularly useful for when the UPN (username@domain.com) of the user differs from the Active Directory domain that the Horizon Cloud Tenant is bound to. This scenario is common in Office 365 environments.

1. In the VMware Identity Manager Administration Console, click the arrow on the Catalog tab and select **Virtual Apps**.
2. Click **Virtual App Configuration**.
3. Click the name of your virtual apps collection to edit.
4. Under **Custom Id Mapping**, specify the name ID format to use along with the Name ID Value.

OPTION	DESCRIPTION
Name ID Format	Select the name ID format, such as email address or User Principal Name. The default value is Unspecified (username).
Name ID Value	Click Select from suggestions and pick from a predefined list of values or click Custom value and enter the value. The default value is <code>\${user.userName}</code> .

The default settings should be used with Horizon Cloud unless there is a need to customize the user ID that is sent in SAML. Select **Name ID Value Custom** to provide a custom value to be sent.

Custom value examples:

CUSTOM VALUE	OUTPUT
<code>\${user.userName}@\${user.domain}</code>	sAMAccountName@domainName
<code>\${user.userName}@mydomain.com</code>	sAMAccountName@mydomain.com

About the Author

Jerrid Cunniff, Sr. Architect, EUC Cloud Services, VMware, has been with VMware since 2013 and is focused on technical solution development for Cloud-Based Desktops and Applications. In addition, Jerrid works closely with marquee customers and partners to ensure their success with Horizon Cloud.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: 5262-VMW-WP-HORIZONCLOUD_ID_MANAGER_QS_GUIDE-USLET-20180320