Deploying VMware Identity Manager in the DMZ

DEC 2017

VMware AirWatch 9.2

VMware Identity Manager 3.1

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Deploying VMware Identity Manager in the DMZ

Deploying VMware Identity Manager in the DMZ provides information about how to deploy VMware Identity Manager in the DMZ instead of the internal network. For information about deploying VMware Identity Manager in the internal network, see *Installing and Configuring VMware Identity Manager*.

Intended Audience

The information is written for experienced Windows and Linux system administrators who are familiar with VMware technologies, particularly vCenter™, ESX™, and vSphere®, and with networking concepts, Active Directory, and databases.

Knowledge of other technologies, such as RSA Adaptive Authentication, RSA SecurID, and RADIUS is also helpful if you plan to implement those features.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

1 Deployment Models

Two main types of deployment models are available for deploying VMware Identity Manager in the DMZ, one that integrates with a VMware AirWatch® deployment, and one that does not require AirWatch and uses the VMware Identity Manager connector.

You can also combine deployment models if you require functionality that is not supported in one of the models.

- Deployment Model using AirWatch Cloud Connector

  If you have an existing AirWatch deployment, you can integrate VMware Identity Manager with it quickly. In this model, user and group sync from your enterprise directory and user authentication are handled by AirWatch. You deploy VMware Identity Manager in the DMZ.

  Note that integrating VMware Identity Manager with resources such as Horizon 7 and Citrix-published resources is not supported in this model. Only integration with Web applications and native mobile applications is supported.

  See On Premises Deployment Model Using AirWatch Cloud Connector.

- Deployment Model using VMware Identity Manager Connector in outbound-only connection mode

  In scenarios that do not require an AirWatch deployment, you can install the VMware Identity Manager server virtual appliance in the DMZ and a VMware Identity Manager connector virtual appliance in the enterprise network. The connector connects the server with on-premises services such as Active Directory. The connector is installed in outbound-only connection mode and does not require inbound firewall port 443 to be opened. In this model, user and group sync from your enterprise directory and user authentication are handled by the VMware Identity Manager connector.

  See On Premises Deployment Model Using VMware Identity Manager Connector in Outbound-Only Connection Mode.

  - Adding Kerberos authentication support to your VMware Identity Manager Connector deployment

    You can add Kerberos authentication for internal users (which requires inbound connection mode) to your deployment based on outbound-only connection mode connectors.

    See Adding Kerberos Authentication Support to Your Deployment.

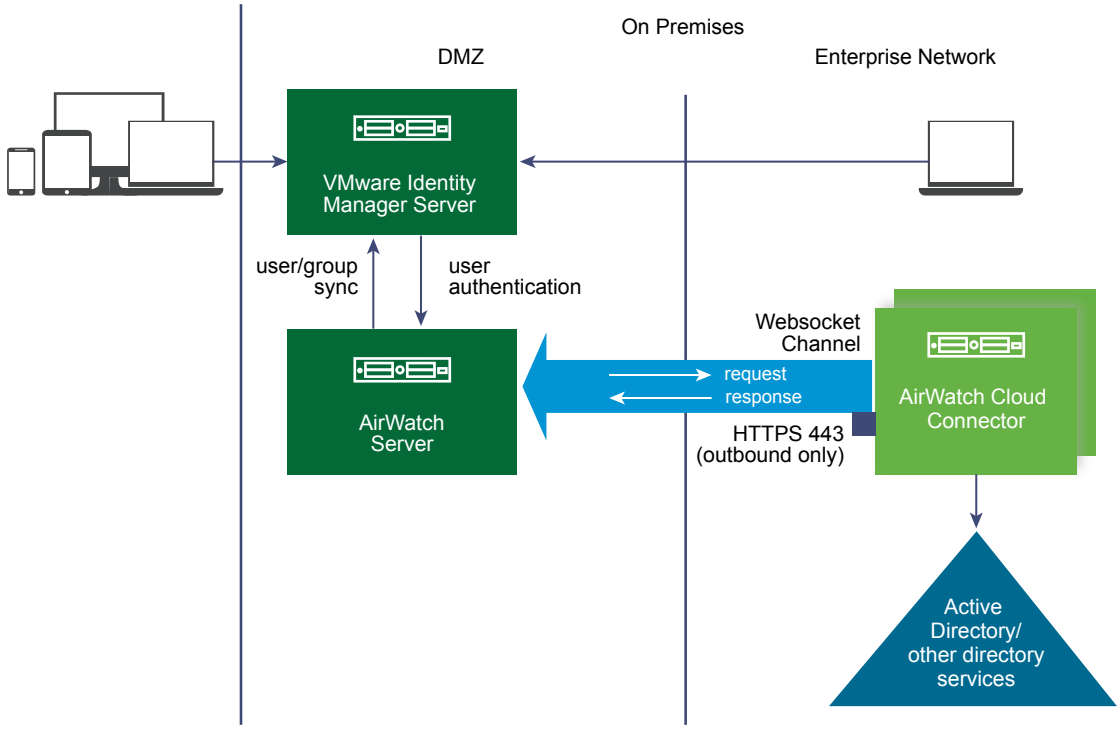
This section includes the following topics:

On Premises Deployment Model Using AirWatch Cloud Connector

If you have an existing AirWatch deployment, you can integrate VMware Identity Manager with it. You deploy the VMware Identity Manager virtual appliance in the DMZ. In this model, user and group sync from your enterprise directory, and user authentication, are handled by AirWatch.

Note that integrating VMware Identity Manager with resources such as Horizon 7 or Citrix-published resources is not supported in this model. Only integration with Web applications and native mobile applications is supported.

Figure 1-1. Deployment with AirWatch Cloud Connector



Note If you plan to configure Android SSO, enable SSL pass-through on port 5262 at the load balancer in front of VMware Identity Manager.

Note If you plan to configure certificate authentication on the embedded connector, enable SSL pass-through on the load balancer for the port configured as the certificate authentication SSL pass-through port. The default port is 7443.

Prerequisites

You must have the following components:

- An AirWatch server deployment
- An AirWatch Cloud Connector instance deployed on premises and integrated with your enterprise directory

Port Requirements

The following ports are required to be opened at the load balancer or firewall for the VMware Identity Manager server:

- Inbound 443 (HTTPS)
- Inbound 88 (TCP/UDP) - iOS SSO only
- Inbound 5262 (HTTPS) - Android SSO only
- Inbound *CertAuthSSLPassthroughPort* (HTTPS) - Certificate authentication configured on embedded VMware Identity Manager connector only. The default port is 7443.

For AirWatch deployment requirements, see the AirWatch documentation.

Supported Authentication Methods

This deployment model supports the following authentication methods. These methods are available through the VMware Identity Manager Built-in identity provider.

- Password (AirWatch Connector)
- Mobile SSO (for iOS)
- Mobile SSO (for Android)
- Device Compliance (with AirWatch)
- Certificate - uses the embedded VMware Identity Manager connector
- VMware Verify

In addition, inbound SAML through a third-party identity provider is also available.

Supported Directory Integrations

You integrate your enterprise directory with AirWatch. See the AirWatch documentation for the types of directories supported.

Supported Resources

You can integrate the following types of resources with VMware Identity Manager in this deployment model:

- Web applications
- Native mobile applications

You cannot integrate the following resources with VMware Identity Manager in this deployment model:

- Horizon 7, Horizon 6, or View desktop and application pools
- Citrix-published resources
- ThinApp packaged applications
- VMware Horizon® Cloud Service™ applications and desktops

Additional Information

- Chapter 2 Deploying VMware Identity Manager in the DMZ
- Integrating AirWatch with VMware Identity Manager in the *VMware Identity Manager Administration Guide*
- AirWatch documentation

On Premises Deployment Model Using VMware Identity Manager Connector in Outbound-Only Connection Mode

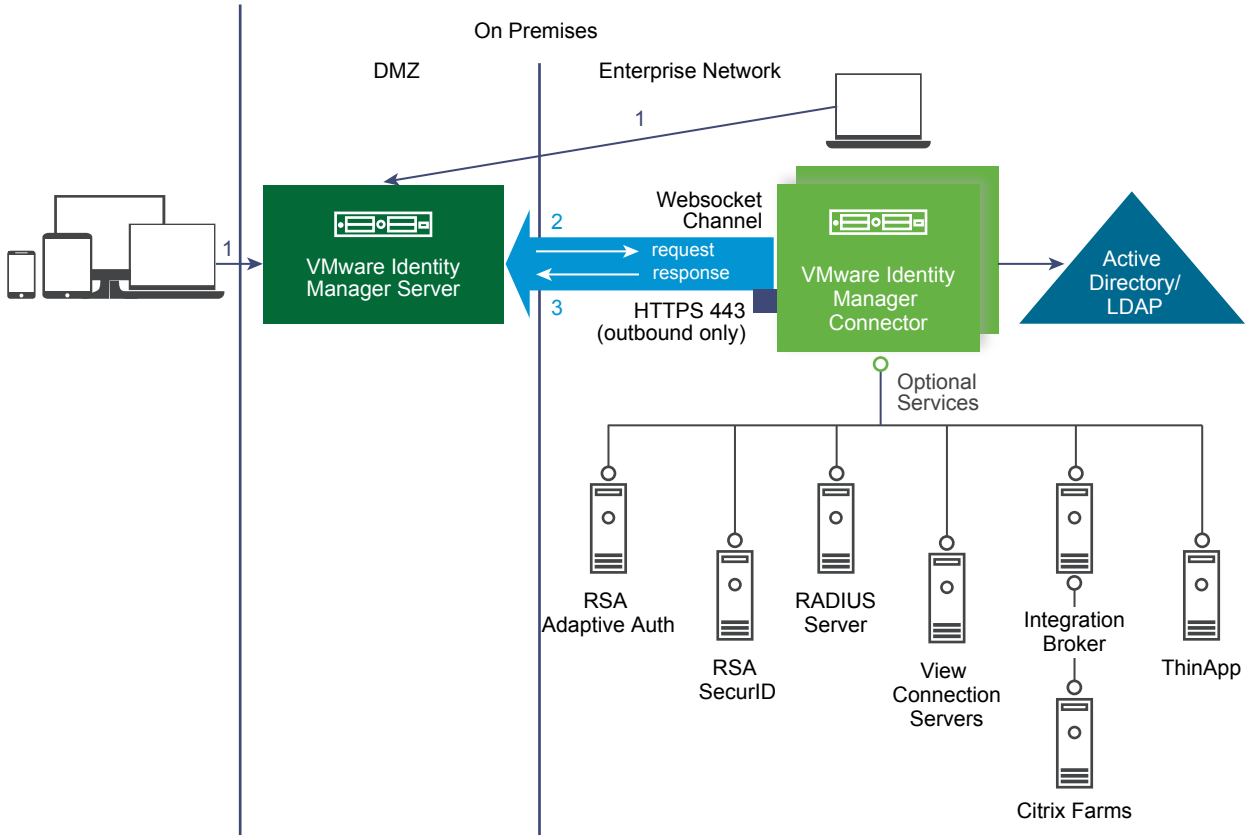
In this model, you install the VMware Identity Manager virtual appliance in the DMZ. You also install a standalone VMware Identity Manager connector virtual appliance in outbound-only connection mode in the enterprise network. This model does not include any AirWatch components.

User and group sync from your enterprise directory and user authentication are handled by the standalone VMware Identity Manager connector. The connector can also sync resources, such as Horizon 7 desktops and applications, to the VMware Identity Manager service.

Note Some authentication methods do not require the connector and are managed directly by the service.

Important Use the standalone connector instead of the connector that is integrated with the VMware Identity Manager appliance to sync users and groups and for user authentication.

Figure 1-2. Using VMware Identity Manager Connector in Outbound Mode



Note If you plan to configure Android SSO, enable SSL pass-through on port 5262 at the load balancer in front of VMware Identity Manager.

Note If you plan to configure certificate authentication on the embedded connector, enable SSL pass-through on the load balancer for the port configured as the certificate authentication SSL pass-through port. The default port is 7443.

Port Requirements

The following ports are required to be opened at the load balancer or firewall for the VMware Identity Manager server:

- Inbound 443 (HTTPS)
- Inbound 88 (TCP/UDP) - iOS SSO only
- Inbound 5262 (HTTPS) - Android SSO only
- Inbound *CertAuthSSLPassthroughPort* (HTTPS) - Certificate authentication configured on embedded connector only. The default port is 7443.

VMware Identity Manager connector is installed in outbound-only connection mode and does not require inbound port 443 to be opened. The connector communicates with the VMware Identity Manager service through a Websocket-based communication channel.

For the complete list of ports used, see Chapter 2 Deploying VMware Identity Manager in the DMZ and Chapter 3 Deploying VMware Identity Manager Connector in the Enterprise Network.

Supported Authentication Methods

This deployment model supports all authentication methods. Some of these authentication methods do not require the connector and are managed directly by the service through the Built-in identity provider.

- Password - uses the connector
- RSA Adaptive Authentication - uses the connector
- RSA SecurID - uses the connector
- RADIUS - uses the connector
- Certificate - uses the embedded connector
- VMware Verify - through the Built-in identity provider
- Mobile SSO (iOS) - through the Built-in identity provider
- Mobile SSO (Android) - through the Built-in identity provider
- Inbound SAML through a third-party identity provider

Note For information on using Kerberos, see Adding Kerberos Authentication Support to Your Deployment.

Supported Directory Integrations

You can integrate the following types of enterprise directories with the VMware Identity Manager service in this deployment model:

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication
- LDAP Directory

  If you plan to integrate an LDAP directory, see the limitations in "Integrating with LDAP Directories" in *Installing and Configuring VMware Identity Manager*.

Alternatively, you can use the following methods to create users in the VMware Identity Manager service:

- Create local users directly in the VMware Identity Manager service.
- Use Just-in-Time provisioning to create users in the VMware Identity Manager service dynamically at login, using SAML assertions sent by a third-party identity provider.

Supported Resources

You can integrate the following types of resources with the VMware Identity Manager service in this deployment model:

- Web applications
- Horizon 7, Horizon 6, or View desktop and application pools
- Citrix-published resources
- ThinApp packaged applications
- Horizon Cloud applications and desktops

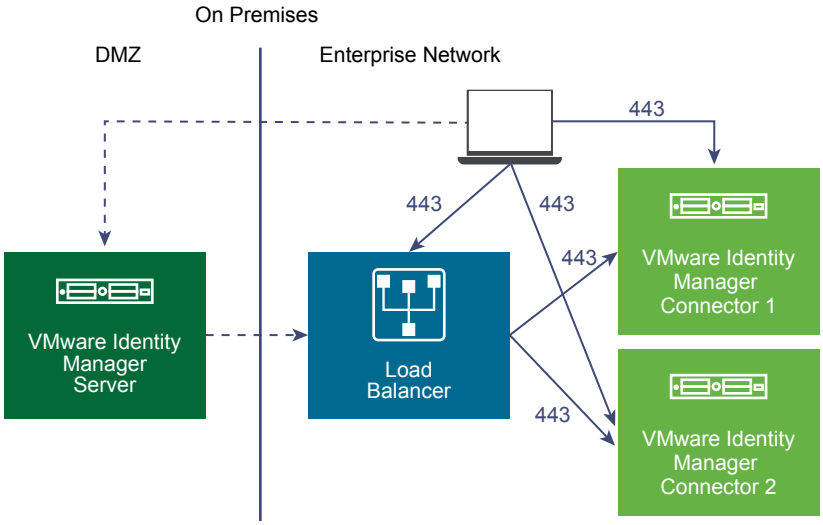
Additional Information

- Chapter 2 Deploying VMware Identity Manager in the DMZ and Chapter 3 Deploying VMware Identity Manager Connector in the Enterprise Network
- Directories
  - "Integrating with Your Enterprise Directory" in *Installing and Configuring VMware Identity Manager*
  - "Using Local Directories" in *Installing and Configuring VMware Identity Manager*
  - "Just-in Time User Provisioning" in *VMware Identity Manager Administration*.
- "Configuring User Authentication in VMware Identity Manager" in *VMware Identity Manager Administration*
- *Setting up Resources in VMware Identity Manager*

Adding Kerberos Authentication Support to Your Deployment

You can add Kerberos authentication for internal users, which requires inbound connection mode, to your deployment based on VMware Identity Manager outbound-only connection mode connectors. The same connectors can be configured to use Kerberos authentication for users coming from the internal network and another authentication method for users coming from outside. This can be achieved by defining authentication policies based on network ranges.

Figure 1-3. Adding Kerberos Authentication



Note that the process to configure high availability of Kerberos authentication is different.

For more information, see Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment.

Adding Certificate Authentication Method to your Deployment

To add certificate authentication to your deployment, you can configure certificate authentication on the connector that is embedded in the VMware Identity Manager service.

See Configuring Certificate Authentication for a DMZ Deployment Scenario for information.

Deploying VMware Identity Manager in the DMZ

2

You can deploy the VMware Identity Manager virtual appliance in the DMZ if you do not want to deploy it in the enterprise network. When you deploy the VMware Identity Manager appliance in the DMZ, you also deploy a standalone VMware Identity Manager connector in outbound-only connection mode in the enterprise network.

System and Network Configuration Requirements

System and network configuration requirements for deploying VMware Identity Manager in the DMZ are similar to the requirements for deploying VMware Identity Manager in the enterprise network, described in System and Network Configuration Requirements and Preparing to Deploy VMware Identity Manager in *Installing and Configuring VMware Identity Manager*, except for the differences listed here.

- You do not need to open an inbound firewall port to any appliance in the enterprise network.

  The VMware Identity Manager virtual appliance is deployed in the DMZ. The VMware Identity Manager connector is deployed in the enterprise network in outbound-only connection mode and communicates with the service through a Websocket-based communication channel.
- You do not need to deploy a reverse proxy or load balancer to allow external access to VMware Identity Manager.
- A load balancer is needed only if you configure high availability and redundancy for the VMware Identity Manager virtual appliance.
- If you set up certificate authentication on the embedded connector, you need to enable SSL pass-through on the load balancer for the port configured as the SSL pass-through port for certificate authentication. The default port is 7443.
- The following ports are used. Your deployment might require only a subset of these.

Port	Source	Target	Description
443	Load Balancer	VMware Identity Manager virtual appliance	HTTPS
443, 8443	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	HTTPS/HTTP For all VMware Identity Manager instances in a cluster and across clusters in different data centers

Port	Source	Target	Description
443	Browsers	VMware Identity Manager virtual appliance	HTTPS
88	Browsers	VMware Identity Manager virtual appliance	TCP/UDP iOS SSO only
5262	Browsers	VMware Identity Manager virtual appliance	TCP/UDP Android SSO only
443	VMware Identity Manager virtual appliance	vapp-updates.vmware.com	Access to the VMware upgrade server
8443	Browsers	VMware Identity Manager virtual appliance	Administrator Port HTTPS
25	VMware Identity Manager virtual appliance	SMTP server	TCP port to relay outbound mail
53	VMware Identity Manager virtual appliance	DNS server	TCP/UDP Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
TCP: 9300-9400 UDP: 54328	VMware Identity Manager virtual appliance	VMware Identity Manager virtual appliance	Audit needs
1433	VMware Identity Manager virtual appliance	Database	Microsoft SQL
443	VMware Identity Manager virtual appliance	AirWatch REST API	HTTPS For device compliance checking and for the ACC Password authentication method, if used.
SSL pass-through port for certificate authentication	Browsers	VMware Identity Manager virtual appliance	HTTPS For certificate authentication configured on the embedded connector. Default port: 7443
514	VMware Identity Manager virtual appliance	syslog server	UDP For external syslog server, if configured

Deploying the VMware Identity Manager Appliance

For information about deploying and configuring the VMware Identity Manager virtual appliance, see Deploying VMware Identity Manager and Managing Appliance System Configuration Settings in *Installing and Configuring VMware Identity Manager*.

Configuring Failover and Redundancy

For information about configuring failover and redundancy for the VMware Identity Manager virtual appliance, see the following sections in *Installing and Configuring VMware Identity Manager*:

- Configuring Failover and Redundancy in a Single Datacenter
- Deploying VMware Identity Manager in a Secondary Datacenter for Failover and Redundancy

Note The section "Using a Load Balancer or Reverse Proxy to Enable External Access to VMware Identity Manager" is not applicable in scenarios where VMware Identity Manager is deployed in the DMZ.

Deploying VMware Identity Manager Connector in the Enterprise Network

3

When you deploy the VMware Identity Manager virtual appliance in the DMZ, you must also deploy a standalone VMware Identity Manager connector appliance in your enterprise network in outbound-only connection mode.

The connector connects the VMware Identity Manager service to other components within the enterprise network such as Active Directory and Horizon 7.

The connector communicates with the service in outbound-only connection mode through a communication channel.

Note If you have an AirWatch deployment and use the AirWatch Cloud Connector, the VMware Identity Manager connector is not required unless you need the use cases supported by the VMware Identity Manager connector. See On Premises Deployment Model Using AirWatch Cloud Connector.

System and Network Configuration Requirements

See System and Network Configuration Requirements.

Deploying and Configuring VMware Identity Manager Connector

For information on deploying and configuring the VMware Identity Manager connector in outbound-only connection mode, see the following topics.

- Deploying the VMware Identity Manager Connector
- Configuring High Availability for the VMware Identity Manager Connector
- Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment

Failover and Redundancy

For information on configuring the connector for failover and redundancy, see the following topics.

- Configuring High Availability for the VMware Identity Manager Connector
- Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment

This section includes the following topics:

Deploying the VMware Identity Manager Connector

To deploy the VMware Identity Manager connector, you install the connector virtual appliance in vCenter Server, power it on, and activate it using an activation code that you generate in the VMware Identity Manager administration console. You also configure appliance settings such as setting passwords.

After you install and configure the connector, you go to the VMware Identity Manager administration console to set up the connection to your enterprise directory, enable authentication adapters on the connector, and enable outbound mode for the connector.

System and Network Configuration Requirements

Consider your entire deployment, including the resources you plan to integrate, when you make decisions about hardware, resources, and network requirements.

Supported vSphere and ESX Versions

You install the virtual appliance in vCenter Server. The following versions of vSphere and ESX server are supported:

- 5.0 U2 and later
- 5.1 and later
- 5.5 and later
- 6.0 and later

VMware vSphere® Client™ or VMware vSphere® Web Client is required to deploy the OVA file and access the deployed virtual appliance remotely. The vSphere Client is available on the vSphere product download page on my.vmware.com.

VMware Identity Manager Connector Virtual Appliance Requirements

Ensure that you meet the requirements for the number of servers and the resources allocated to each server.

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,1000
Number of connector servers	1 server	2 load-balanced servers	2 load-balanced servers	2 load-balanced servers	2 load-balanced servers
CPU (per server)	2 CPU	4 CPU	4 CPU	4 CPU	4 CPU

Number of Users	Up to 1,000	1,000-10,000	10,000-25,000	25,000-50,000	50,000-100,1000
RAM (per server)	6 GB	6 GB	8 GB	16 GB	16 GB
Disk space (per server)	60 GB	60 GB	60 GB	60 GB	60 GB

Network Configuration Requirements

Component	Minimum Requirement
DNS record and static IP address	The requirements for the connector are the same as the requirements for the VMware Identity Manager virtual appliance. See Create DNS Records and IP Addresses in *Installing and Configuring VMware Identity Manager*.
Firewall port	Ensure that the outbound firewall port 443 is open from the connector instance to your VMware Identity Manager URL.

Port Requirements

Ports used in the connector server configuration are described below. Your deployment might include only a subset of these.

Port	Source	Target	Description
443	Connector virtual appliance	VMware Identity Manager service	HTTPS
443	Connector virtual appliance	vapp-updates.vmware.com	Access to the upgrade server
8443	Browsers	Connector virtual appliance	Administrator Port HTTPS
389, 636, 3268, 3269	Connector virtual appliance	Active Directory	Default values are shown. These ports are configurable.
5500	Connector virtual appliance	RSA SecurID system	Default value is shown. This port is configurable
53	Connector virtual appliance	DNS server	TCP/UDP Every virtual appliance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22
88, 464, 135, 445	Connector virtual appliance	Domain controller	TCP/UDP
389, 443	Connector virtual appliance	View Connection Server	Access to View Connection Server instances for Horizon/View integrations
445	Connector virtual appliance	VMware ThinApp repository	Access to ThinApp repository

Port	Source	Target	Description
80, 443	Connector virtual appliance	Integration Broker server	TCP Connection to the Integration Broker server. Port option depends on whether a certificate is installed on the Integration Broker server.
514	Connector virtual appliance	syslog server	UDP For external syslog server, if configured

Supported Directories

You integrate your enterprise directory with VMware Identity Manager and sync users and groups from your enterprise directory to the service. You can integrate the following types of directories.

- 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.

  VMware Identity Manager supports Active Directory on Windows 2008, 2008 R2, 2012, and 2012 R2, with a Domain functional level and Forest functional level of Windows 2003 and later.

- An LDAP directory

Your directory must be accessible to the connector virtual appliance.

Note You can also create local directories in the VMware Identity Manager service.

Deployment Checklists

The requirements for the connector are similar to the requirements for the VMware Identity Manager virtual appliance. See Deployment Checklists in *Installing and Configuring VMware Identity Manager*.

Generate Activation Code for Connector

Before you install the VMware Identity Manager connector, log in to the VMware Identity Manager administration console and generate an activation code for the connector. This activation code is used to establish communication between the service and the connector.

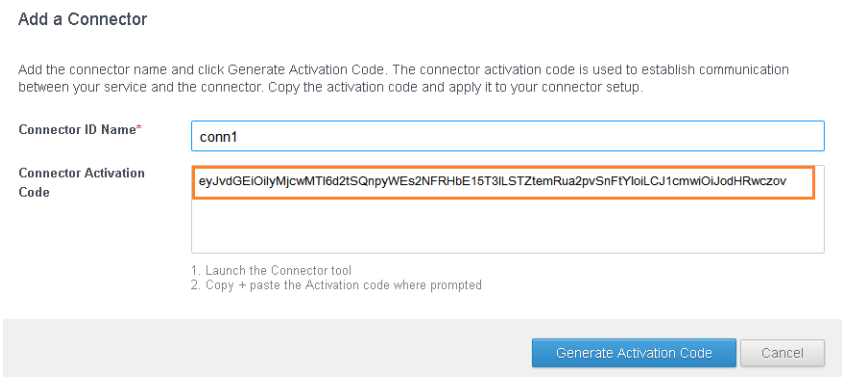
Procedure

1. Log in to the administration console.
2. Click the **Identity & Access Management** tab.
3. Click **Setup**.
4. On the Connectors page, click **Add Connector**.
5. Enter a name for the connector.

6 Click **Generate Activation Code.**

The activation code displays on the page.

7 Copy the activation code and save it.



You need the activation code later when you deploy the connector.

You can now install the connector virtual appliance.

Install and Configure the Connector Virtual Appliance

To deploy the connector, you install the connector virtual appliance in vCenter Server using the vSphere Client or vSphere Web Client, power it on, and activate it using the activation code that you generated in the VMware Identity Manager administration console.

Prerequisites

- Download the connector OVA file from the VMware Identity Manager product page on my.vmware.com.
- Ensure you have vSphere Client or vSphere Web Client.
- If using the vSphere Web Client, use either Firefox or Chrome browsers. Do not use Internet Explorer to deploy the OVA file.
- Identify the DNS records and host name to use for your appliance.

Procedure

1 In the vSphere Client or the vSphere Web Client, select **File > Deploy OVF Template**.

2 Follow the wizard to deploy the template.

Page	Description
Source	Browse to the OVA package location, or enter a specific URL.
OVA Template Details	Verify that you selected the correct version.
License	Read the End User License Agreement and click **Accept**.
Name and Location	Enter a name for the virtual appliance. The name must be unique within the inventory folder and can contain up to 80 characters. Names are case sensitive. Select a location for the virtual appliance.

Page	Description
Host / Cluster	Select the host or cluster to run the deployed template.
Resource Pool	Select the resource pool.
Storage	Select the location to store the virtual machine files.
Disk Format	Select the disk format for the files. For production environments, select a **Thick Provision** format. Use the **Thin Provision** format for evaluation and testing.
Network Mapping	Map the networks in your environment to the networks in the OVF template.
Properties	a In the **Timezone setting** field, select the correct time zone. b The Customer Experience Improvement Program checkbox is selected by default. VMware collects anonymous data about your deployment in order to improve response to user requirements. Deselect the checkbox if you do not want the data collected. c In the Host Name text box, enter the host name to use. If this is blank, reverse DNS is used to look up the host name. d To configure the static IP address for connector, enter the address for each of the following: Default Gateway, DNS, IP Address, and Netmask. **Important** If any of the four address fields, including Host Name, are left blank, DHCP is used. To configure DHCP, leave the address fields blank.
Ready to Complete	Review your selections and click **Finish**.

Depending on your network speed, the deployment can take several minutes. You can view the progress in the progress dialog box.

3 When the deployment is complete, select the connector appliance, right-click, and select **Power > Power on**.

The connector appliance is initialized. You can go to the **Console** tab to see the details. When the virtual appliance initialization is complete, the console screen displays the connector version and URLs to log in to the connector Setup wizard.

4 To run the Setup wizard, point your browser to the connector URL displayed in the Console tab.

5 On the Welcome Page, click **Continue**.

6 Create strong passwords for the following connector virtual appliance administrator accounts.

Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Option	Description
Appliance Administrator	Create the appliance administrator password. The user name is **admin** and cannot be changed. You use this account and password to log in to the connector services to manage certificates, appliance passwords and syslog configuration. **Important** The **admin** user password must be at least 6 characters in length.
Root Account	A default VMware root password was used to install the connector appliance. Create a new root password.
sshuser Account	Create the password to use for remote access to the connector appliance.

7 Click **Continue**.

8 On the Activate Connector page, paste the activation code and click **Continue**.

The activation code is verified and the communication between the VMware Identity Manager service and your connector instance is established.

The connector setup is complete.

What to do next

Click the link on the Setup is Complete page to go to the administration console. Then set up the directory connection.

Set up a Directory

After you deploy the connector virtual appliance, set up a directory in the VMware Identity Manager administration console. You can sync users and groups from your enterprise directory to the VMware Identity Manager service.

VMware Identity Manager supports integrating the following types of directories.

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication
- LDAP directory

See Integrating with Your Enterprise Directory for more information.

Note You can also create local directories in the VMware Identity Manager service. See Using Local Directories.

Procedure

1 Click the link on the Setup is Complete page, which is displayed after you activate the connector.

The **Identity & Access Management > Directories** tab is displayed.

2 Click **Add Directory** and select the type of directory you want to add.

3 Follow the wizard to enter the directory configuration information, select groups and users to sync, and sync users to the VMware Identity Manager service.

See Integrating with Your Enterprise Directory for information on how to set up a directory.

What to do next

Click the **Users & Groups** tab and verify that users have been synced.

Enable Authentication Adapters on the Connector

Several authentication adapters are available for the connector in outbound mode, including PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter, and RadiusAuthAdapter. Configure and enable the adapters that you intend to use.

Procedure

1. In the VMware Identity Manager administration console, click the **Identity & Access Management** tab.
2. Click **Setup**, then click the **Connectors** tab.

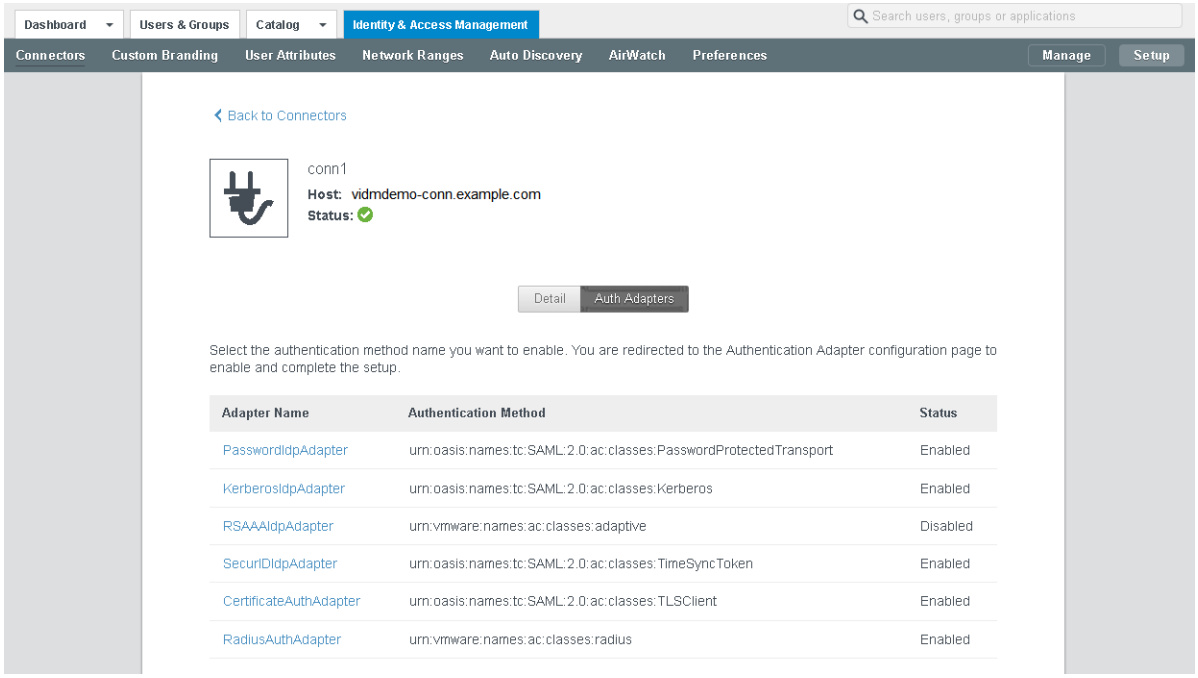
   The connector you deployed is listed.
3. Click the link in the **Worker** column.
4. Click the **Auth Adapters** tab.

   All available authentication adapters for the connector are listed.

   If you have already set up a directory, the PasswordIdpAdapter is already configured and enabled, with the configuration information you specified while creating the directory.
5. Configure and enable the authentication adapters you want to use by clicking on the link for each and entering the configuration information. You must enable at least one authentication adapter.

   For information on configuring specific authentication adapters, see the *VMware Identity Manager Administration Guide*.

   For example:



Enable Outbound Mode for the Connector

To enable outbound-only connection mode for the connector, associate the connector with the Built-in identity provider.

The Built-in identity provider is available by default in the VMware Identity Manager service and provides additional built-in authentication methods such as VMware Verify. For information about the Built-in identity provider, see the *VMware Identity Manager Administration Guide*.

Note The connector can be used in both outbound and regular mode simultaneously. Even if you enable outbound mode, you can still configure Kerberos authentication for internal users using authentication methods and policies.

Procedure

1 In the administration console **Identity & Access Management** tab, click **Manage**.

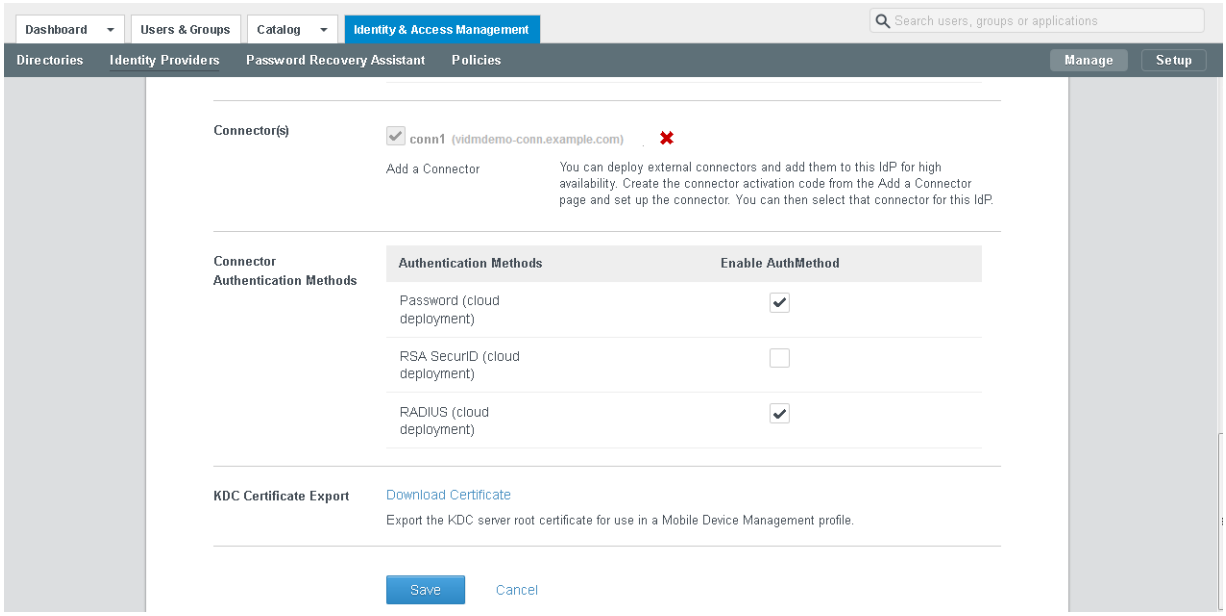
2 Click the **Identity Providers** tab.

3 Click the **Built-in** link.

4 Enter the following information.

Option	Description
Users	Select the directory or domains that will use the Built-in identity provider.
Network	Select the network ranges that will use the Built-in identity provider.
Connector(s)	Select the connector that you set up. **Note** Later, when you add additional connectors for high availability, select and add all of them here to associate them with the Built-in identity provider. VMware Identity Manager automatically distributes traffic among all the connectors associated with the Built-in identity provider. A load balancer is not required.
Connector Authentication Methods	The deployment methods that you enabled for the connector are listed. Select the authentication methods that you want to use. The PasswordIdpAdapter, which was automatically configured and enabled when you created a directory, is displayed on this page as **Password (cloud deployed)**, which denotes that it is used with the connector in outbound mode.

For example:



5 Click **Save** to save the Built-in identity provider configuration.

6 Edit policies to use the authentication methods that you enabled.

   a In the **Identity & Access Management** tab, click **Manage**.

   b Click the **Policies** tab and click the policy you want to edit.

   c Under **Policy Rules**, for the rule you want to edit, click the link in the **Authentication Method** column.

   d In the Edit Policy Rule page, select the authentication method that you want to use for this rule.

   e Click **OK**.

   f Click **Save**.

   For more information about configuring policies, see the *VMware Identity Manager Administration Guide*.

The outbound mode of the connector is now enabled. When a user logs in using one of the authentication methods that you enabled for the connector in the Built-in identity provider page, an HTTP redirect to the connector is not required.

Configuring High Availability for the VMware Identity Manager Connector

You can set up the VMware Identity Manager connector for high availability and failover by adding multiple connector virtual appliances in a cluster. If one of the virtual appliances becomes unavailable for any reason, other connectors will still be available.

To create the cluster, you install new connector virtual appliances and configure them in exactly the same way as you set up the first connector.

You then associate all the connector instances with the Built-in identity provider. The VMware Identity Manager service automatically distributes traffic among all the connectors associated with the Built-in identity provider. A load balancer is not required. If one of the connectors becomes unavailable because of a network issue, the service does not direct traffic to it. When connectivity is restored, the service resumes sending traffic to the connector.

After you set up the connector cluster, the authentication methods that you enabled on the connector are highly available. If one of the connector instances is unavailable, authentication is still available. For directory sync, however, in the event of a connector instance failure, you will need to manually select another connector instance as the sync connector. Directory sync can only be enabled on one connector at a time.

Note This section does not apply to high availability of Kerberos authentication. See Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment.

Install Additional Connector Instances

After you install and configure the first connector instance, you can add additional connectors for high availability. Install new connector virtual appliances and configure them in exactly the same way as the first connector instance.

Prerequisites

You have installed and configured the first connector instance, as described in Deploying the VMware Identity Manager Connector.

Procedure

1 Install and configure a new connector instance by following these instructions.

- Generate Activation Code for Connector
- Install and Configure the Connector Virtual Appliance

2 Associate the new connector with the `WorkspaceIDP` of the first connector instance.

a In the administration console, select the **Identity & Access Management** tab, then select the **Identity Providers** tab.

b In the Identity Providers page, find the `WorkspaceIDP` of the first connector instance and click the link.

c In the **Connector(s)** field, select the new connector.

d Enter the Bind DN password and click **Add Connector**.

e Click **Save**.

3 If you had joined an Active Directory domain in the first connector instance, then you must join the domain in the new connector instance too.

   a In the **Identity & Access Management** tab, click **Setup**.

      The new connector instance is listed in the Connectors page.

   b Click **Join Domain** next to the new connector and specify the domain information.

Note For directories of type Integrated Windows Authentication (IWA), you must perform the following actions.

   a Join the new connector instance to the domain to which the IWA directory in the original connector instance was joined.

      1 Select the **Identity & Access Management** tab, then click **Setup**.

         The new connector instance is listed in the Connectors page.

      2 Click **Join Domain** and specify the domain information.

   b Save the IWA directory configuration.

      1 Select the **Identity & Access Management** tab.

      2 In the Directories page, click the IWA directory link.

      3 Click **Save** to save the directory configuration.

4 Configure and enable authentication adapters on the new connector.

Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be enabled on all the connectors.

   a In the **Identity & Access Management** tab, click **Setup**, then click the **Connectors** tab.

   b Click the link in the **Worker** column of the new connector.

   c Click the **Auth Adapters** tab.

      All available authentication adapters for the connector are listed.

      The PasswordIdpAdapter is already configured and enabled because you associated the new connector with the directory associated with the first connector.

   d Configure and enable the other authentication adapters in the same way as the first connector. Ensure that the configuration information is identical.

      For information on configuring authentication adapters, see the *VMware Identity Manager Administration Guide*.

What to do next

Add New Connector to Built-in Identity Provider

Add New Connector to Built-in Identity Provider

After you deploy and configure the new connector instance, add it to the Built-in identity provider and enable the same authentication methods that are enabled on the first connector. VMware Identity Manager automatically distributes traffic among all the connectors associated with the Built-in identity provider.

Procedure

1. In the administration console **Identity & Access Management** tab, click **Manage**.
2. Click the **Identity Providers** tab.
3. Click the **Built-in** link.
4. In the **Connector(s)** field, select the new connector from the drop-down list and click **Add Connector**.
5. In the **Connector Authentication Methods** section, enable the same authentication methods that you selected for the first connector.

   The Password (cloud deployment) authentication method is automatically configured and enabled. You must enable the other authentication methods.

   Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be enabled on all the connectors.

   For information on configuring specific authentication adapters, see the *VMware Identity Manager Administration Guide*.
6. Click **Save** to save the Built-in identity provider configuration.

Enabling Directory Sync on Another Connector in the Event of a Failure

In the event of a connector instance failure, authentication is handled automatically by another connector instance. However, for directory sync, you must modify the directory settings in the VMware Identity Manager service to use another connector instance instead of the original connector instance. Directory sync can only be enabled on one connector at a time.

Procedure

1. Log in to the VMware Identity Manager administration console.
2. Click the **Identity & Access Management** tab, then click **Directories**.
3. Click the directory that was associated with the original connector instance.

Tip You can view this information in the **Setup > Connectors** page.

4 In the **Directory Sync and Authentication** section of the directory page, in the **Sync Connector** drop-down list, select another connector instance.

5 In the **Bind DN Password** text box, enter your Active Directory bind account password.

6 Click **Save**.

Adding Kerberos Authentication Support to Your VMware Identity Manager Connector Deployment

You can add Kerberos authentication for internal users, which requires inbound connection mode, to your deployment based on outbound-only connection mode connectors. The same connectors can be configured to use Kerberos authentication for users coming from the internal network and another authentication method for users coming from outside. This can be achieved by defining authentication policies based on network ranges.

Note To set up high availability for Kerberos authentication, a load balancer is required.

Configuring and Enabling the Kerberos Authentication Adapter

Configure and enable the KerberosIdpAdapter on the VMware Identity Manager connector. If you have deployed a cluster for high availability, configure and enable the adapter on all the connectors in your cluster.

Important Authentication adapters on all the connectors in your cluster must be configured identically. The same authentication methods must be configured on all the connectors.

For more information about configuring Kerberos authentication, see the *VMware Identity Manager Administration Guide*.

Prerequisites

The connector must be joined to the Active Directory domain.

Procedure

1 In the VMware Identity Manager administration console, click the **Identity & Access Management** tab.

2 Click **Setup**, then click the **Connectors** tab.

All the connectors that you have deployed are listed.

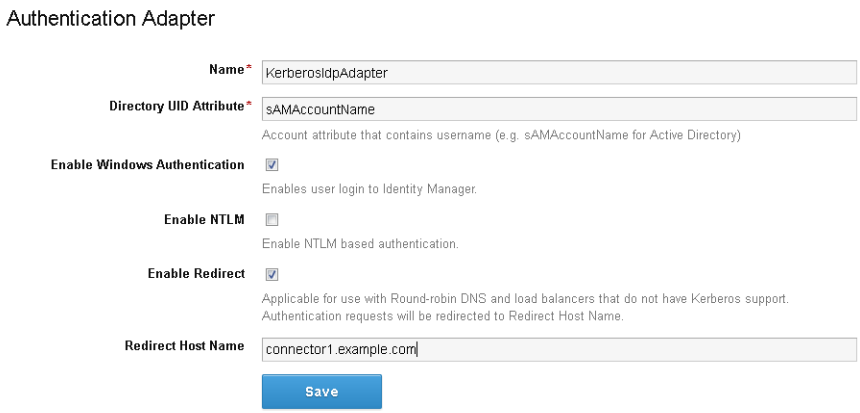
3 Click the link in the **Worker** column of one of the connectors.

4 Click the **Auth Adapters** tab.

5 Click the KerberosIdpAdapter link, and configure and enable the adapter.

Option	Description
Name	The default name of the adapter is KerberosIdpAdapter. You can change this name.
Directory UID Attribute	The account attribute that contains username.
Enable Windows Authentication	Select this option.
Enable NTLM	You do not need to select this option unless your Active Directory infrastructure relies on NTLM authentication.
Enable Redirect	If you have multiple connectors in a cluster and plan to set up Kerberos high availability by using a load balancer, select this option and specify a value for **Redirect Host Name**. If your deployment has only one connector, you do not need to use the **Enable Redirect** and **Redirect Host Name** options.
Redirect Host Name	A value is required if the **Enable Redirect** option is selected. Enter the connector's own host name. For example, if the connector's host name is connector1.example.com, enter **`connector1.example.com`** in the text box.

For example:



For more information on configuring the KerberosIdPAdapter, see the *VMware Identity Manager Administration Guide*.

6 If you have deployed a cluster, configure the KerberosIdPAdapter on all the connectors in your cluster.

Ensure that you configure the adapter identically on all the connectors, except for the Redirect Host Name value, which should be specific to each connector.

What to do next

Set up high availability for Kerberos authentication, if necessary. Kerberos authentication is not highly available without a load balancer.

Configuring High Availability for Kerberos Authentication

To configure high availability for Kerberos authentication, install a load balancer in your internal network inside the firewall and add the connector appliances to it.

You must also configure certain settings on the load balancer, establish SSL trust between the load balancer and the connector, and change the connector authentication URL to use the load balancer host name.

Configure Load Balancer Settings

You must configure certain settings on the load balancer, such as enabling X-Forwarded-For headers, setting the load balancer timeout correctly, and enabling sticky sessions.

Configure these settings.

- X-Forwarded-For Headers

  You must enable X-Forwarded-For headers on your load balancer. This determines the authentication method. See the documentation provided by your load balancer vendor for more information.

- Load Balancer Timeout

  For the connector to function correctly, you might need to increase the load balancer request timeout from the default. The value is set in minutes. If the timeout setting is too low, you might see the following error.

  ```
  502 error: The service is currently unavailable
  ```

- Enable Sticky Sessions

  You must enable the sticky session setting on the load balancer if your deployment has multiple connector appliances. The load balancer will then bind a user's session to a specific connector instance.

Apply VMware Identity Manager Connector Root Certificate to the Load Balancer

When the VMware Identity Managerconnector virtual appliance is configured with a load balancer, you must establish SSL trust between the load balancer and the connector. The connector root certificate must be copied to the load balancer.

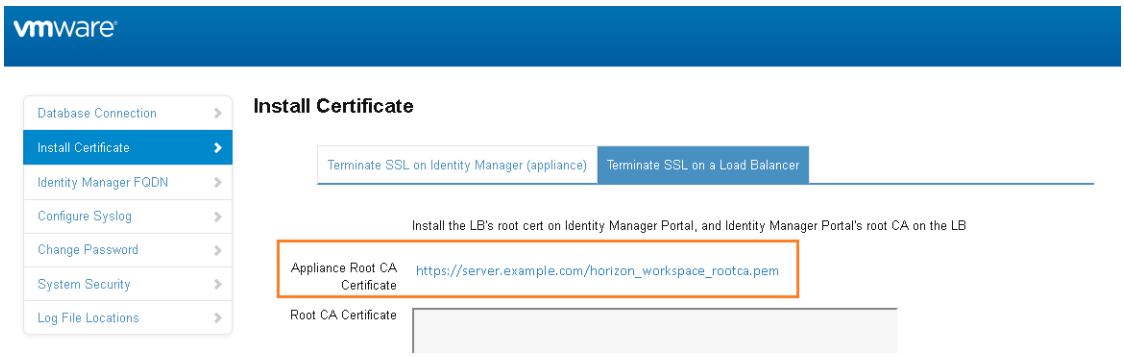
The connector certificate can be downloaded from the connector appliance admin pages at https://*myconnector*.*mycompany*:8443/cfg/ssl.

When the connector domain name points to the load balancer, the SSL certificate can only be applied to the load balancer.

Since the load balancer communicates with the connector virtual appliance, you must copy the connector root CA certificate to the load balancer as a trusted root certificate.

Procedure

1. Log in to the connector appliance admin pages, https://*myconnector.mycompany*:8443/cfg/ssl, as the admin user.
2. Select **Install Certificate**.
3. Select the **Terminate SSL on a Load Balancer** tab and in the **Appliance Root CA Certificate** field, click the link `https://hostname/horizon_workspace_rootca.pem`.



4. Copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE---- and paste the root certificate into the correct location on each of your load balancers. Refer to the load balancer documentation.

What to do next

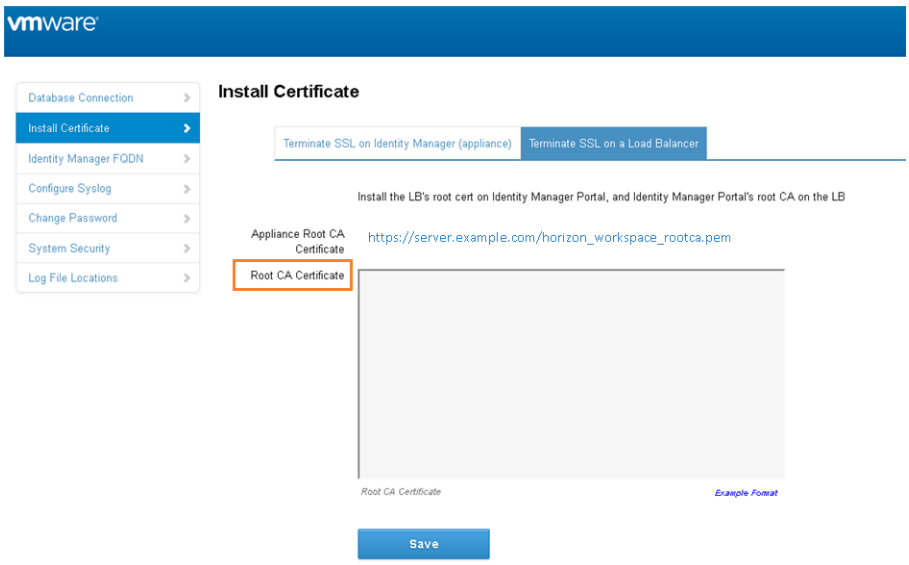
Copy and paste the load balancer root certificate to the VMware Identity Manager connector appliance.

Apply Load Balancer Root Certificate to the VMware Identity Manager Connector

When the VMware Identity Manager connector virtual appliance is configured with a load balancer, you must establish trust between the load balancer and the connector. In addition to copying the connector root certificate to the load balancer, you must copy the load balancer root certificate to the connector.

Procedure

1. Obtain the load balancer root certificate.
2. Go to the connector appliance administration page at https://*myconnector.mycompany*:8443/cfg/ssl and log in as the admin user.
3. In the **Install Certificate** page, select the **Terminate SSL on a Load Balancer** tab.
4. Paste the text of the load balancer certificate into the **Root CA Certificate** field.



5 Click **Save**.

Change Connector IdP Host Name to the Load Balancer Host Name

After you add the connector virtual appliances to the load balancer, you must change the IdP host name on the Workspace IdP of each connector to the load balancer host name.

Prerequisites

The connector virtual appliance must be configured behind a load balancer. Make sure that the load balancer port is 443. Do not use 8443 as this port number is the administrative port and is unique to each virtual appliance.

Procedure

1 Log in to the VMware Identity Manager administration console.

2 Click the **Identity & Access Management** tab.

3 Click the **Identity Providers** tab.

4 In the Identity Providers page, click the Workspace IdP link for your connector instance.

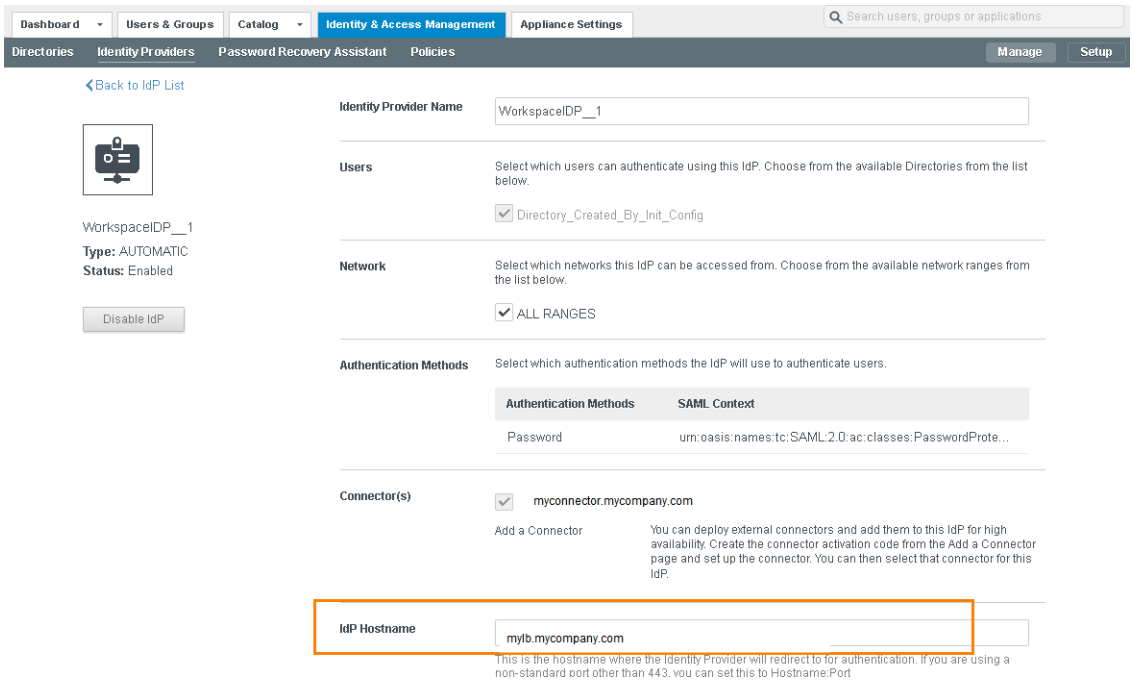
5 In the **IdP Hostname** text box, change the host name from the connector host name to the load balancer host name.

For example, if your connector host name is `myconnector` and your load balancer hostname is `mylb`, change the URL

```
myconnector.mycompany.com:port
```

to the following:

```
mylb.mycompany.com:port
```



Configuring Certificate Authentication for a DMZ Deployment Scenario

Enabling certificate authentication for a VMware Identity Manager on-premises deployment requires setting SSL pass-through at the load balancer. In a DMZ deployment scenario, where the VMware Identity Manager service is deployed in the DMZ and the VMware Identity Manager connector is deployed in the internal network, if you do not want to allow inbound access to the connector, you can enable certificate authentication on the connector that is embedded in the VMware Identity Manager service.

In this scenario, use the embedded connector for certificate authentication only. Use the external connector for all other authentication methods.

To use the embedded connector for certificate authentication, you create a new Workspace identity provider for your directory, associate it with the embedded connector, and enable the Certificate Authentication adapter on the embedded connector. You can then configure your policies to use the certificate authentication method. Policies can also be set per app.

You also need to configure an SSL pass-through port for certificate authentication so that the SSL handshake is between the end user and the embedded connector. You set the port and upload the SSL certificate for it on the Appliance Settings pages and enable SSL pass-through for the port on the load balancer.

Other traffic continues to use port 443.

Note This feature does not support local directories. Also, this feature is applicable only for on-premises DMZ deployments and does not apply to any other installation scenarios.

Deployment Requirements

- On the load balancer in front of the VMware Identity Manager service appliance, enable SSL pass-through on the port you configure as the SSL pass-through port for certificate authentication. The default port is 7443.

  The port must be in the range 1024-65535 and cannot be 8443, which is the admin port.
- Verify that the port is open on the load balancer or firewall.

Prerequisites

For the SSL pass-through port on the VMware Identity Manager server, obtain a signed SSL certificate from a public Certificate Authority. The hostname on the certificate must match the load balancer host name. The certificate must also be trusted by the end user.

Procedure

1 Set the SSL pass-through port for certificate authentication.

   a In the administration console, click the **Appliance Settings** tab.

   b Click **Manage Configuration** and enter the admin user password.

   c In the left pane, click **Install SSL Certificates** and select the **Passthrough Certificate** tab.

   d Enter the required information.

Option	Description
Port	Enter the port you want to use as the SSL pass-through port for certificate authentication. The default port is 7443. The port must be in the range 1024-65535 and cannot be 8443, which is the admin port. **Note** The port is available only if a certificate is added.
SSL Certificate Chain	Copy and paste the SSL certificate. Include the entire certificate chain, in the following order: Server certificate Intermediate certificate Root certificate For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----. Certificates must be in the PEM format.
Private Key	Copy and paste the private key.

   e Click **Add**.

   The server is restarted.

2 Create a new Workspace identity provider.

a Click the **Identity & Access Management** tab, then click the **Identity Providers** tab.

b Click **Add Identity Provider** and select **Create Workspace IDP**.

c Enter the information for the new identity provider.

Option	Description
Identity Provider Name	Enter a name for the identity provider.
Users	Select the directory for which you want to enable certificate authentication. **Note** This feature does not support local directories.
Connector(s)	1 From the **Add a Connector** drop-down menu, select the embedded connector. The embedded connector has the same hostname as the service. 2 Deselect the **Bind to AD** check box. 3 Click **Add Connector**. **Important** Do not select the **Bind to AD** option.
Network	Select the network ranges from which the identity provider can be accessed.

d Click **Add**.

3 Set the port for the embedded connector.

a Click the **Identity & Access Management** tab and click **Setup**.

b In the Connectors page, click the new Workspace identity provider you created for the embedded connector.

c In the **IdP Hostname** text box, change the value from ***`hostname`*** to ***`hostname:port`***, where *port* is the custom port you configured for certificate authentication in step 1.

d Click **Save**.

4 Enable the CertificateAuthAdapter on the embedded connector.

a Click **Setup**.

b In the Connectors page, find the embedded connector.

The embedded connector has the same hostname as the service.

c In the embedded connector row, click the link in the **Worker** column.

Each worker is associated with a directory. If multiple workers are listed, click the worker link for the directory for which you want to enable certificate authentication.

d Click the **Auth Adapters** tab.

e Click **CertificateAuthAdapter**.

f Configure and enable the adapter. See *VMware Identity Manager Administration* for information.

g Click **Save**.

5 Verify that the Identity Providers page displays the Certificate Authentication method.

   a Click **Manage**, then click the **Identity Providers** tab.

   b Verify that **Certificate Authentication** appears in the **Authentication Methods** column for the new identity provider that you created.

6 Configure policies to use the certificate authentication method according to your needs.

   a Click **Manage**, then click the **Identity Providers** tab.

   b Click the policy to edit.

   c Configure policy rules to use the certificate authentication method as needed.

   See *VMware Identity Manager Administration* for more information about creating policies.