VMware Enterprise Systems Connector Installation and Configuration

SEP 2017

VMware AirWatch 9.2

VMware Identity Manager 3.0

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

VMware Enterprise Systems Connector Installation and Configuration

VMware Enterprise Systems Connector Installation and Configuration provides information about setting up the VMware Enterprise Systems Connector™, which provides organizations the ability to integrate VMware AirWatch® and VMware Identity Manager™ with their back-end enterprise systems.

This document provides information about installing both components of the VMware Enterprise Systems Connector, the AirWatch Cloud Connector and the VMware Identity Manager Connector.

This information is applicable for both SaaS and on premises deployment scenarios. Notes in the text indicate any differences between the environments.

Intended Audience

This information is written for experienced Windows system administrators. It is applicable for both SaaS and on premises customers.

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.

VMware Enterprise Systems Connector Overview

1

Before installing the VMware Enterprise Systems Connector, review the information about systems requirements, architecture, and deployment models.

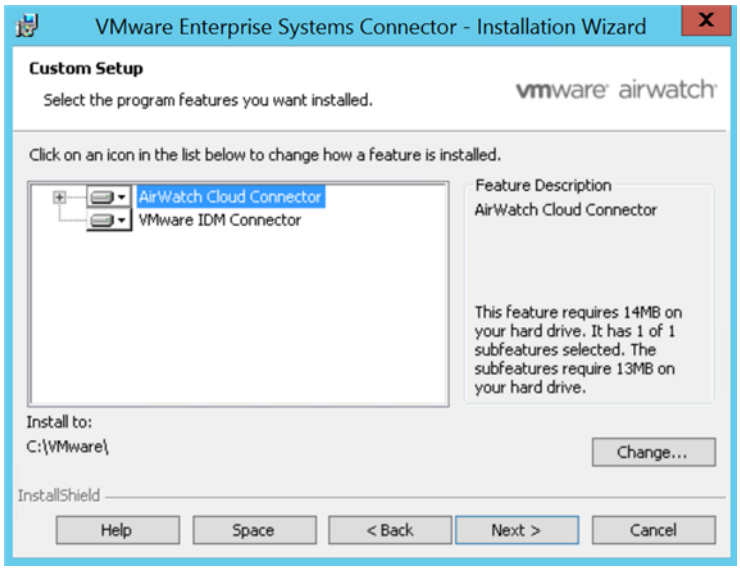
This section includes the following topics:

- About the VMware Enterprise Systems Connector
- Enterprise Systems Connector System Requirements

About the VMware Enterprise Systems Connector

In VMware AirWatch 9.1 and later, the AirWatch Cloud Connector (ACC) is included as a component in a new installer called the VMware Enterprise Systems Connector. This installer serves as the unified connector package for Workspace ONE, AirWatch, and Identity. It is comprised of two components, ACC and the VMware Identity Manager Connector.

During the installation process, you can choose which components to install.



See Determine Which Components to Install for the scenarios where installing both components is recommended.

AirWatch Cloud Connector Component

The AirWatch Cloud Connector (ACC) provides organizations with the ability to integrate AirWatch with their back-end enterprise systems.

The ACC runs in the internal network, acting as a proxy that securely transmits requests from AirWatch to the organization's critical enterprise infrastructure components. This allows organizations to leverage the benefits of AirWatch Mobile Device Management (MDM), running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems. See also Chapter 2 Enterprise Systems Connector Architecture Overview.

The ACC integrates with the following internal components.

- Email Relay (SMTP)
- Directory Services (LDAP/AD)
- Email Management Exchange 2010 (PowerShell)
- BlackBerry Enterprise Server (BES)
- Lotus Domino Web Service (HTTPS)
- Syslog (Event log data)

The following components are only available if you purchased the PKI Integration add-on, which is available separately.

- Microsoft Certificate Services (PKI)
- Simple Certificate Enrollment Protocol (SCEP PKI)
- Third-party Certificate Services (on-premises only)

VMware Identity Manager Connector Component

The VMware Identity Manager Connector provides directory integration, user authentication, and integration with resources such as Horizon View.

Using the VMware Identity Manager Connector component provides the following additional capabilities to your deployment.

- VMware Identity Manager Connector-based authentication methods such as password, RSA Adaptive Authentication, RSA SecurID, and Radius
- Kerberos authentication for internal users
- Integration with the following resources:
  - Horizon View desktop and application pools
  - Citrix-published resources
  - VMware Horizon® Cloud Service™ with Hosted and On-Premises Infrastructure

Getting Started

Note For on-premises deployments, before proceeding with this guide, you should have read and performed the procedures in the *AirWatch Cloud Messaging Service (AWCM) Guide*.

If you are an on-premises customer, ensure that AWCM is installed correctly, running, and communicating with AirWatch without any errors.

Enterprise Systems Connector System Requirements

To deploy Enterprise Systems Connector, ensure your system meets the necessary requirements.

Hardware Requirements

Use the following requirements as a basis for creating your Enterprise Systems Connector server.

If you are installing the ACC component only, use the following requirements.

Table 1-1. ACC Requirements

Number of Users	Up to 10,000	10,000 to 50,000	50,000 to 100,000
CPU Cores	2	2 load-balanced servers with 2 CPU Cores	3 load-balanced servers with 2 CPU Cores
RAM (GB) Per Server	4	4 each	8 each
Disk Space (GB)	50	50 each	50 each

The VMware Identity Manager Connector component has the following additional requirements. If you are installing both the ACC and VMware Identity Manager Connector components, add these requirements to the ACC requirements.

Table 1-2. VMware Identity Manager Connector Requirements

Number of Users	Up to 1000	1000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
CPU	2	2 load-balanced servers, each with 4 CPU	2 load-balanced servers, each with 4 CPU	2 load-balanced servers, each with 4 CPU	2 load-balanced servers, each with 4 CPU
RAM (GB) Per Server	6	6 each	8 each	16 each	16 each
Disk Space (GB)	50	50 each	50 each	50 each	50 each

Note

- For the ACC component, traffic is automatically load-balanced by the AWCM component. It does not require a separate load balancer. Multiple ACC instances in the same organization group that connect to the same AWCM server for high availability can all expect to receive traffic (a live-live configuration). How traffic is routed is determined by AWCM and depends on the current load.
- For the VMware Identity Manager Connector component, see Configuring High Availability for the VMware Identity Manager Connector.
- CPU Cores should each be 2.0 GHz or higher. An Intel processor is required.
- Disk Space requirements include: 1 GB disk space for the Enterprise Systems Connector application, Windows OS, and .NET runtime. Additional disk space is allocated for logging.

Software Requirements

Ensure your Enterprise Systems Connector server meets all the following software requirements.

Status Checklist	Requirement	Notes
	Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2	Required for both components
	Install PowerShell on the server	Required for both components **Note** (AirWatch Cloud Connector component) PowerShell version 3.0+ is required if you are deploying the PowerShell MEM-direct model for email. To check your version, open PowerShell and run the command `$PSVersionTable`. **Note** (VMware Identity Manager Connector component) PowerShell version 4.0 is required if you are installing on Windows Server 2008 R2.
	Install .NET Framework 4.6.2	Required for both components **Note** (AirWatch Cloud Connector component) The AirWatch Cloud Connector auto-update feature will not function correctly until your Enterprise Systems Connector server is updated to .NET Framework 4.6.2. The auto-update feature will not update the .NET Framework automatically. Install .NET Framework 4.6.2 manually on the Enterprise Systems Connector server before performing an upgrade.

General Requirements

Ensure your Enterprise Systems Connector server is set up with the following general requirements to ensure a successful installation.

Status Checklist	Requirement	Notes
	Ensure that you have remote access to the servers that AirWatch is installed on	VMware AirWatch recommends setting up Remote Desktop Connection Manager for multiple server management. You can download the installer from https://www.microsoft.com/en-us/download/details.aspx?id=44989. Typically, installations are performed remotely over a web meeting or screen share that an AirWatch consultant provides. Some customers also provide AirWatch with VPN credentials to directly access the environment as well.
	Installation of Notepad++ (Recommended)	VMware AirWatch recommends setting up Notepad++.
	Services accounts for authentication to backend systems	Validate AD connectivity method using LDP.exe tool (See http://www.computerperformance.co.uk/ScriptsGuy/ldp.zip) LDAP, BES, PowerShell, etc.

Network Requirements

For configuring the ports listed below, all traffic is uni-directional (outbound) from the source component to the destination component.

An outbound proxy or any other connection management software or hardware must not terminate or reject the outbound connection from the Enterprise Systems Connector. The outbound connection required for use by Enterprise Systems Connector must remain open at all times.

Note Any resource such as certificate authorities that you want to reach with the ACC must be on the same domain.

Table 1-3. AirWatch Cloud Connector Component Port Requirements (SaaS)

Status Checklist	Source Component	Destination Component	Protocol	Port	Verification
	Enterprise Systems Connector Server	AirWatch AWCM For example: (https://awcm274.awmdm. com)	HTTPS	443	Verify by entering https://awcmXXX.awmdm.com/awcm/status and ensure there is no certificate trust error. (Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.)
	Enterprise Systems Connector Server	AirWatch Console For example: (https://cn274.awmdm .com)	HTTP or HTTPS	80 or 443	Verify by entering https://cnXXX.awmdm.com and ensure there is no certificate trust error. (Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.) If auto-update is enabled, ACC must be able to query AirWatch Console for updates using port 443.

Table 1-3. AirWatch Cloud Connector Component Port Requirements (SaaS) (Continued)

Status Checklist	Source Component	Destination Component	Protocol	Port	Verification
	Enterprise Systems Connector Server	AirWatch API For example: (https://as274.awmdm.com)	HTTPS	443	Verify by entering https://asXXX.awmdm.com/api/help and ensure you are prompted for credentials. (Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.) ACC to API access is required for the proper functioning of the AirWatch Diagnostics service.
	Enterprise Systems Connector Server	CRL: http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	For various services to function properly
			Optional Integrations		
	Enterprise Systems Connector Server	Internal SMTP	SMTP	25	
	Enterprise Systems Connector Server	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269	
	Enterprise Systems Connector Server	Internal SCEP	HTTP or HTTPS	80 or 443	
	Enterprise Systems Connector Server	Internal ADCS	DCOM	135, 1025-5000, 49152-65535	
	Enterprise Systems Connector Server	Internal BES	HTTP or HTTPS	80 or 443	
	Enterprise Systems Connector Server	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443	

Table 1-4. AirWatch Cloud Connector Component Port Requirements (On Premises)

	Source Component	Destination Component	Protocol	Port	Verification
	Enterprise Systems Connector Server	AirWatch Cloud Messaging Servwer	HTTPS	2001	Telnet from Enterprise Systems Connector to AWCM Server on port or once installed. Verify by entering **`https://<AWCM URL>:2001/awcm/status`**and ensure there is no certificate trust error. If auto-update is enabled, ACC must be able to query AirWatch Console for updates using port 443. If you are using ACC with AWCM and you have multiple AWCM servers and want to load balance them, you need to configure persistence. For more information on setting up AWCM Persistence Rules Using F5, see the following Knowledge Base article: https://support.air-watch.com/articles/115001666028.
	Enterprise Systems Connector Server	AirWatch Console	HTTP or HTTPS	80 or 443	Telnet from Enterprise Systems Connector to Console on port or once installed. Verify by entering **`https://<Console URL>`** and ensure there is no certificate trust error. If auto-update is enabled, ACC must be able to query AirWatch Console for updates using port 443.
	Enterprise Systems Connector Server	API server (or wherever API is installed)	HTTPS	443	Verify by navigating to the URL of your API server. ACC to API access is required for the proper functioning of the AirWatch Diagnostics service.
	Enterprise Systems Connector Server	CRL: http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	For various services to function properly
			Optional Integrations		
	Enterprise Systems Connector Server	Internal SMTP	SMTP	25	
	Enterprise Systems Connector Server	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269	
	Enterprise Systems Connector Server	Internal SCEP	HTTP or HTTPS	80 or 443	

Table 1-4. AirWatch Cloud Connector Component Port Requirements (On Premises) (Continued)

	Source Component	Destination Component	Protocol	Port	Verification
	Enterprise Systems Connector Server	Internal ADCS	DCOM	135, 1025-5000, 49152-65535	
	Enterprise Systems Connector Server	Internal BES	HTTP or HTTPS	80 or 443	
	Enterprise Systems Connector Server	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443	

Table 1-5. VMware Identity Manager Connector Component Port Requirements (SaaS or On Premises)

Status Checklist	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	Every instance must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
	VMware Identity Manager Connector	Domain controller	88, 464, 135, 445	TCP/UDP	
	VMware Identity Manager Connector	RSA SecurID system	5500		Default port. This port is configurable
	VMware Identity Manager Connector	View Connection Server	389, 443		Access to View Connection Server instances for Horizon View integrations

Table 1-5. VMware Identity Manager Connector Component Port Requirements (SaaS or On Premises) (Continued)

Status Checklist	Source Component	Destination Component	Port	Protocol	Notes
	VMware Identity Manager Connector	Integration Broker	80, 443		Access to the Integration Broker for integration with Citrix-published resources. **Important** If you install the Integration Broker on the same Windows server as the Enterprise Systems Connector, you must ensure that in the IIS Server Default Web Site site bindings, the HTTP and HTTPS binding ports do not conflict with the ports used by the VMware Identity Manager Connector component. The VMware Identity Manager Connector always uses port 80. It also uses 443, unless a different port is configured during installation.
	VMware Identity Manager Connector	syslog server	514	UDP	For external syslog server, if configured

(VMware Identity Manager Connector Component) VMware Identity Manager Cloud Hosted IP Addresses

(SaaS customers) See Knowledge Base article 2149884 for the list of VMware Identity Manager service IP addresses to which the VMware Identity Manager Connector must have access.

(VMware Identity Manager Connector Component) DNS Records and IP Addresses Requirements

A DNS entry and a static IP address must be available for the connector. Before you begin your installation, request the DNS record and IP addresses to use and configure the network settings of the Windows server.

Configuring reverse lookup is optional. When you implement reverse lookup, you must define a PTR record on the DNS server so the connector uses the correct network configuration.

You can use the following sample list of DNS records. Replace the sample information with information from your environment. This example shows forward DNS records and IP addresses.

Table 1-6. Examples of Forward DNS Records and IP Addresses

Domain Name	Resource Type	IP Address
myidentitymanager.company.com	A	10.28.128.3

This example shows reverse DNS records and IP addresses.

Table 1-7. Examples of Reverse DNS Records and IP Addresses

IP Address	Resource Type	Host Name
10.28.128.3	PTR	myidentitymanager.company.com

After you complete the DNS configuration, verify that the reverse DNS lookup is properly configured. For example, the virtual appliance command `host IPaddress` must resolve to the DNS name lookup.

Note If you have a load balancer with a Virtual IP address (VIP) in front of the DNS servers, note that VMware Identity Manager does not support using a VIP. You can specify multiple DNS servers separated by a comma.

Note If you are using a Unix or Linux-based DNS server and plan to join the connector to the Active Directory domain, make sure that the appropriate service (SRV) resource records are created for each Active Directory domain controller.

(VMware Identity Manager Connector Component) Supported Active Directory Versions

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

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 is supported.

Enterprise Systems Connector Architecture Overview 2

The Enterprise Systems Connector contains two Windows services that can be installed on a physical or virtual server running Windows 2008 R2, 2012, or 2012 R2. It operates from within your internal network and can be configured behind any existing Web Application Firewalls or load balancers.

By initiating a secure HTTPS connection from Enterprise Systems Connector to messaging services built into AirWatch and VMware Identity Manager, Enterprise Systems Connector can periodically transmit information from your internal resources such as AD, LDAP, etc. to the product without any firewall changes. If you plan on proxying traffic through an outbound proxy, you can use settings in the connector configuration that allow for proxying.

Supported Configurations

Use Enterprise Systems Connector in the following configurations.

- Using HTTPS transport
- Supporting HTTP traffic through an outbound proxy

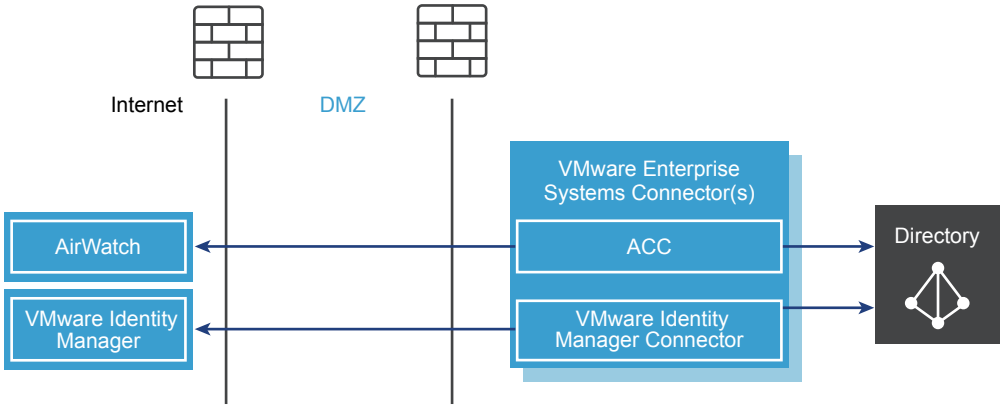
This section includes the following topics:

Enterprise Systems Connector SaaS Deployment Model

In a SaaS deployment model, the Enterprise Systems Connector resides in your internal network and integrates with your internal systems, allowing AirWatch and VMware Identity Manager to leverage them for various functions, such as certificates and directory services.

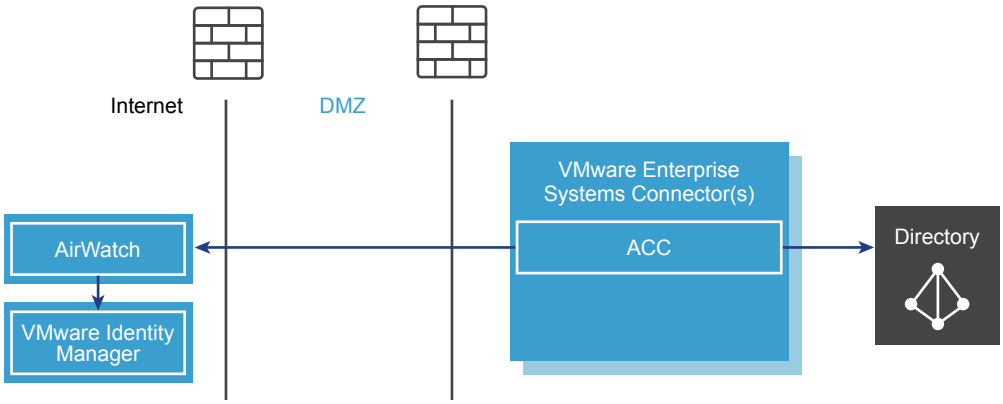
The following diagram shows the full deployment of the Enterprise Systems Connector, with both ACC and VMware Identity Manager Connector components deployed.

Figure 2-1. Enterprise Systems Connector SaaS Deployment



The following diagram shows the deployment of the ACC component only.

Figure 2-2. Enterprise Systems Connector SaaS Deployment (ACC only)

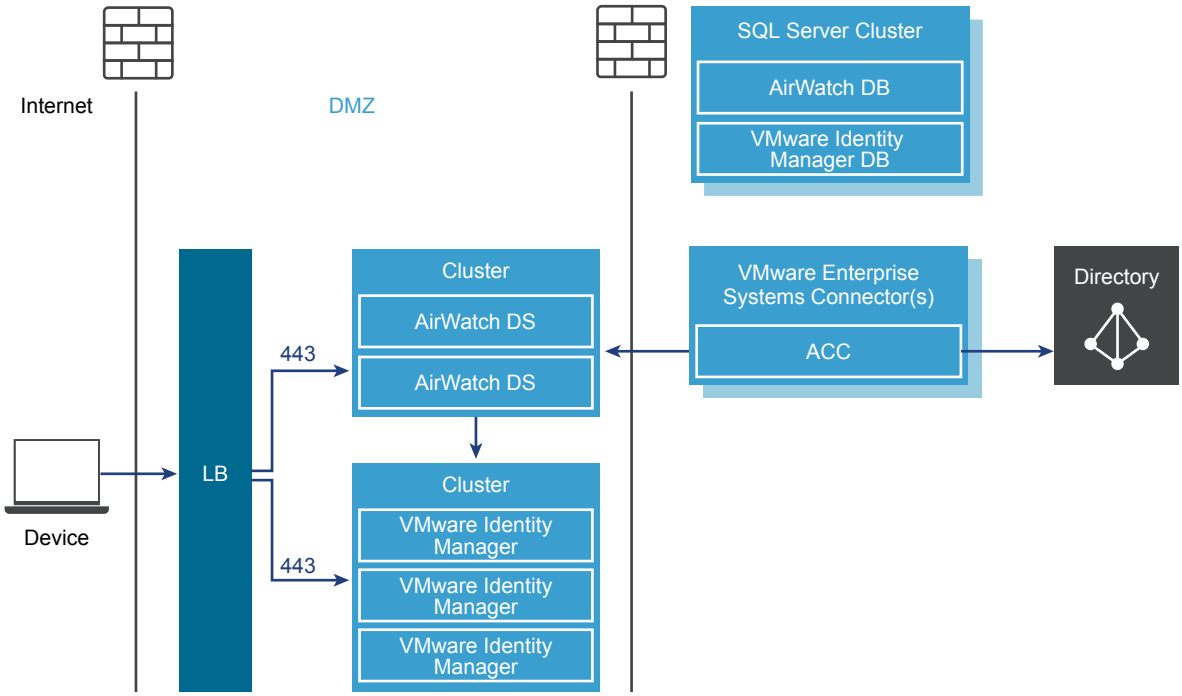


Enterprise Systems Connector On-Premises Deployment Model

In an on-premises deployment model, the Enterprise Systems Connector resides in your internal network and communicates with AWCM and the VMware Identity Manager service. AWCM is typically installed on the AirWatch device services server.

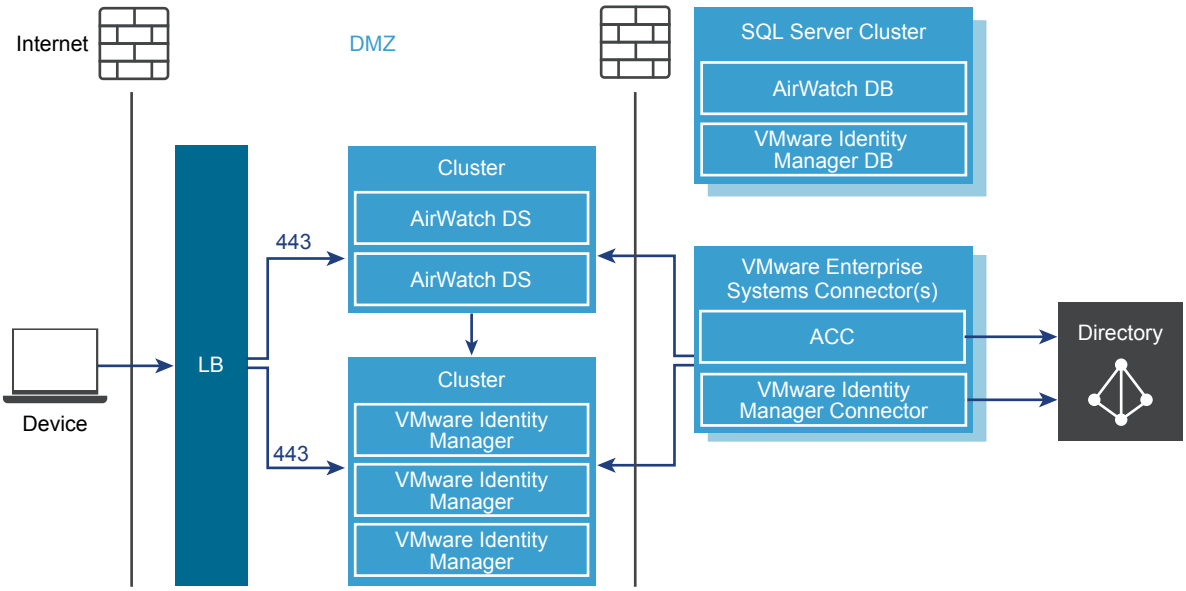
The following diagram shows the deployment of the ACC component with a typical on-premises AirWatch layout.

Figure 2-3. Enterprise Systems Connector On Premises Deployment (ACC only)



The following diagram shows the deployment of both the ACC and VMware Identity Manager Connector components with a typical on-premises AirWatch layout.

Figure 2-4. Enterprise Systems Connector On Premises Deployment (ACC and VMware Identity Manager Connector)



ACC Component Certificate Integration Workflows

Certificates are used to authenticate the communication between the AirWatch Console and AirWatch Cloud Connector (ACC).

How Certificates are Generated

- You enable the ACC and then generate certificates for AirWatch and ACC.
  - Both certificates are unique to the group selected in the AirWatch Console and reside on the AirWatch server.
  - Both certificates are generated from a trusted AirWatch root.
- You install ACC. The ACC certificate that AirWatch generates is automatically bundled and installed with ACC.

How Data is Routed in On-Premises Environments

- AirWatch sends requests to AWCM. Requests are SSL encrypted using HTTPS.
- ACC queries AWCM for AirWatch requests. Requests are SSL encrypted using HTTPS.
- All data is sent through AWCM.

The ACC configuration trusts only messages signed from the AirWatch environment. This trust is unique per group.

Any additional ACC servers set up in the same AirWatch group as part of a highly available (HA) configuration are issued the same unique ACC certificate. For more information about high availability, refer to the VMware AirWatch Recommended Architecture Guide, available on AirWatch Resources.

How Data is Secured in On-Premises Environments

The AirWatch server sends each request as an encrypted and signed message to the AWCM.

- Requests are encrypted using the unique public key of the ACC instance. Only ACC can decrypt the requests.
- Requests are signed using the private key of the AirWatch server instance that is unique for each group. Therefore, ACC trusts the requests only from the configured AirWatch server.
- Responses from ACC to the AirWatch server are encrypted with the same key as the request and signed with the ACC private key

Enterprise Systems Connector Installation Process

3

You must perform several tasks to configure and install the Enterprise Systems Connector in your internal network.

Procedure

1. Determine Which Components to Install - Determine whether to install only the ACC component or both ACC and the VMware Identity Manager Connector.
2. (On-Premises Customers Only) Install Secure Channel Certificate on AWCM - On-premises customers must install a Secure Channel Certificate to establish security between the AWCM and the following components: AirWatch Console, Device Services, API, and the Self-Service Portal.
3. Establish Communications with AWCM - SaaS and on-premises customers should establish communications with AWCM. Performing this action allows you to configure an AirWatch instance to use a particular AWCM server.
4. Obtaining the VMware Enterprise Systems Connector Installer - You can download the Enterprise Systems Connector installer from the Cloud Connector page in the AirWatch console as described in Enable Enterprise Systems Connector from the AirWatch Console. The installer is also available as part of the Workspace ONE Getting Started wizard.
5. Enable Enterprise Systems Connector from the AirWatch Console - Before you install Enterprise Systems Connector, you must first enable it, generate certificates, and select the enterprise services and AirWatch services to be integrated. After completing this step, you can install Enterprise Systems Connector.
6. Run the Enterprise Systems Connector Installer - Run the Enterprise Systems Connector installer on your configured server that meets all the prerequisites.
7. Verify a Successful Enterprise Systems Connector Installation - After you install Enterprise Systems Connector, you can verify a successful installation from within the AirWatch Console.

This section includes the following topics:

- Determine Which Components to Install
- (On-Premises Customers Only) Install Secure Channel Certificate on AWCM
- Establish Communications with AWCM

- Obtaining the VMware Enterprise Systems Connector Installer
- Enable Enterprise Systems Connector from the AirWatch Console
- Run the Enterprise Systems Connector Installer
- Verify a Successful Enterprise Systems Connector Installation

Determine Which Components to Install

Before you begin the installation process, decide whether to install the ACC component only, or install both ACC and VMware Identity Manager Connector, according to your business needs.

Installing both components of the Enterprise Systems Connector is recommended for most Workspace ONE customers. In addition to ACC features, the full installation includes support for the following features.

- Virtual apps and desktops in Workspace ONE
- RSA Secure ID Authentication
- Integrated Windows Authentication
- Multiple, trusted or untrusted Active Directory with VMware Identity Manager
- VMware Identity Manager with multiple directory-organization group configurations in AirWatch
- Platform for identity-centric integration features

If you have already deployed Workspace ONE with ACC only, that model continues to be supported, but if you plan to take advantage of any of these features, installing the full Enterprise Systems Connector is recommended. Migration from ACC-only to the VMware Identity Manager Connector available in the Enterprise Systems Connector is supported. See Chapter 6 Directory Migration from ACC to the VMware Identity Manager Connector.

(On-Premises Customers Only) Install Secure Channel Certificate on AWCM

On-premises customers must install a Secure Channel Certificate to establish security between the AWCM and the following components: AirWatch Console, Device Services, API, and the Self-Service Portal.

Important Perform the following steps on the server running AWCM. Do not download the installation program onto another computer and copy it to the AWCM server. If the download fails on the server running AWCM, then contact AirWatch Support for potential workarounds.

Note If you make any changes to the Secure Channel Certificate in the AWCM keystore after you have downloaded and installed AirWatch Tunnel or Enterprise Systems Connector, then you will need to uninstall, delete all folders, re-download and re-install it.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Advanced > Secure Channel Certificate**.

2 Select **Download AWCM Secure Channel Installer** within the AirWatch Cloud Messaging section to begin the installation of the Secure Channel Certificate install script.

The Secure Channel Installer for Linux is only used for the Cloud Notification Service. AWCM is only supported on Windows servers.

3 Copy the **Secure Channel Certificate** install script to your local AWCM server and right-click to **Run as Administrator** to execute and install.

4 Enter or select **Browse** to find the Truststore path and select **OK**.

5 Select **OK** when a Message dialog box appears informing you that the Certificate was added to keystore.

6 Proceed with the steps for Establishing Communications with AWCM.

7 Proceed with the installation steps for Enterprise Systems Connector.

Establish Communications with AWCM

SaaS and on-premises customers should establish communications with AWCM. Performing this action allows you to configure an AirWatch instance to use a particular AWCM server.

Procedure

1 Navigate to Groups & Settings > All Settings > System > Advanced > Site URLs to view the AirWatch Cloud Messaging section.

Note If you are a SaaS customer and do not see this page in the system settings, then these settings have already been configured for you.

2 Configure the following settings.

Setting	Description
Enable AirWatch Server	Check this box to allow the connection between the AirWatch Console and the AWCM server.
AirWatch Server External URL	This field allows you to enter the servername used by external components and devices (e.g., ACC) to securely (using HTTPS) communicate with AWCM. An example of an ACC URL is: Acme.com. Do not add https:// since this is assumed by the application and automatically added.

Setting	Description
AirWatch External Port	This is the port that is being used by the servername above to communicate with AWCM. For secure external communications, use port 443. If you are bypass offloading SSL, then you want to use an internal non-secure communications port, which is by default 2001 but can be changed to other port numbers.
AWCM Server Internal URL	This URL allows you to reach AWCM from internal components and devices (e.g., Admin Console, Device Services, etc.). Examples of AirWatch URLs are: https://Acme.com:2001/awcm or http://AcmeInternal.Local/awcm. If your AWCM server and AirWatch Console are internal (within the same network), and you want to bypass offloaded SSL, there is no need for a secure connection, so you can use http instead of https. For example, http://AcmeInternal.Local:2001/awcm. This example shows the server resides within the internal network and is communicating on port 2001.

Obtaining the VMware Enterprise Systems Connector Installer

The VMware Enterprise Systems Connector installer is available from multiple locations.

The installer is available from the Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector page in the AirWatch Console, as described in Enable Enterprise Systems Connector from the AirWatch Console. It is also available as part of the Workspace ONE Getting Started wizard. To use the Workspace ONE Getting Started wizard, see the *VMware Workspace ONE Quick Configuration Guide*.

Enable Enterprise Systems Connector from the AirWatch Console

Before you install Enterprise Systems Connector, you must first enable it, generate certificates, and select the enterprise services and AirWatch services to be integrated. After completing this step, you can install Enterprise Systems Connector.

Note Perform the following steps on the server that will run Enterprise Systems Connector. Do not download the installer onto another computer and copy it to the Enterprise Systems Connector server.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**.

2 Configure the following settings on the **General** tab.

Setting	Description
Enable Cloud Connector	Select this checkbox to enable Enterprise Systems Connector and display the General tab.
Enable Auto Update	Select to enable Enterprise Systems Connector to automatically update when a newer version is available. For more information regarding auto-update, refer to VMware Enterprise Systems Connector Auto-Update Option.

3 Configure the following settings on the **Advanced** tab.

Setting	Description
Generate Certificates	Select this button to generate a certificate for the Enterprise Systems Connector and AirWatch server. Certificates are generated for both and displayed under VMware Enterprise Systems Connector and AirWatch certificates. Once certificates are generated, the button changes to **Regenerate Certificates**. For more information about regenerating certificates, see Regenerate Certificates.
Communication with AWCM	Select how the Enterprise Systems Connector communicates with AWCM under Communication with AWCM. ■ **Use External AWCM URL** – This is the default option that will apply to most deployments. ■ **Use Internal AWCM URL** – Use this option if your security settings restrict your Enterprise Systems Connector server from resolving the External AWCM URL. For example, if Enterprise Systems Connector is on your internal network and your AWCM server is in a DMZ. Select the **Enabled** or **Disabled** buttons to enable or disable Enterprise Services. The services you select (enabled) will integrate with Enterprise Systems Connector. ■ SMTP (Email Relay) AirWatch SaaS offers email delivery through its own SMTP, but you can enable Enterprise Systems Connector to use another SMTP server here. Enter SMTP servers settings for email in **Groups & Settings > All Settings > System > Enterprise Integration > Email (SMTP)**. ■ Directory Services (LDAP/AD) ■ Exchange PowerShell (for certain Secure Email Gateways) ■ BES (BlackBerry sync user and mobile device information) ■ Syslog (Client/server protocol used to integrate with the AirWatch event log data)

Setting	Description
Enterprise Services	The following components are only available if you purchased the PKI Integration add-on, which is available separately. ■ Microsoft Certificate Services (PKI) ■ Simple Certificate Enrollment Protocol (SCEP PKI) ■ OpenTrust CMS Mobile (third-party certificate services) ■ Entrust PKI (third-party certificate services) ■ Symantec MPKI (third-party certificate services) Since there is no need to go through Enterprise Systems Connector for cloud certificate services, if you want to integrate with certificate services (like Symantec MPKI) by selecting one of the checkboxes in the screen below, the service you select must be on premises, not in the cloud (SaaS).
AirWatch Services	Select **Enabled** or **Disabled** to enable or disable AirWatch Services. The AirWatch components you select (enabled) will integrate with Enterprise Systems Connector. AirWatch recommends leaving all services enabled. ■ Device Services (Admin Console and all services required for it to operate, including related Windows services) ■ Device Management (Enrollment, App Catalog, and related Windows services) ■ Self-Service Portal (including related Windows services) ■ All Other Components (including related Windows services) **Note** (On-premises customers) If you have not already performed *Enabling AWCM to Communicate with VMware Enterprise Systems Connector*, then you can select **Download AWCM Secure Channel Installer** to be redirected to the download page. **Note** (SaaS customers) You do not need to download the Secure Channel Certificate installer.

4 Select **Save** to keep all these settings.

5 Navigate back to the General tab and select **Download Cloud Connector Installer**.

A Download Cloud Connector Installer page displays.

6 Enter a password for the Enterprise Systems Connector certificate in the fields. The password will be needed later when you run the Enterprise Systems Connector installer and need to enter the certificate password.

7 Select **Download** and save the .exe file on the Enterprise Systems Connector server for use later.

Run the Enterprise Systems Connector Installer

Run the Enterprise Systems Connector installer on a Windows server that meets all the requirements.

The installer includes the AirWatch Cloud Connector and VMware Identity Manager Connector components. You can install one or both components. After the initial installation, you can run the installer again to modify any features or update your installation.

Prerequisites

The following prerequisites apply to the AirWatch Cloud Connector (ACC) component.

- Before beginning, on-premises customers should ensure the server on which Enterprise Systems Connector is being installed can reach AWCM by browsing to `https://{url}:port/awcm/status`, where {url} is the AirWatch environment URL and *port* is the external port you configured for AWCM to communicate. You should see the status of the AWCM with no SSL errors. If there are errors, resolve them before continuing or ACC does not function properly.
- SaaS customers should ensure the server on which you are installing Enterprise Systems Connector can reach AWCM by browsing to https://awcm*XXX*.awmdm.com/awcm/status. Replace *XXX* with the same number as used in your environment URL, for example,'100' for cn100. You should see the status of the AWCM with no SSL errors. If there are errors, resolve them before continuing or the ACC will not function properly.

The following prerequisites apply to the VMware Identity Manager Connector component.

- 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, and you must install the VMware Identity Manager Connector component as a domain user that is part of the administrator group on the Windows server, in the following cases.
  - If you plan to connect to Active Directory (Integrated Windows Authentication)
  - If you plan to use Kerberos authentication
  - If you plan to integrate Horizon View with VMware Identity Manager and want to use the Perform Directory Sync or Configuring 5.x Connection Server options

  In these cases, you must also choose to run the IDM Connector service as a domain user during installation.
- 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.

Procedure

1 Double-click the installer.

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 Enterprise Systems Connector installer again to resume the installation process.

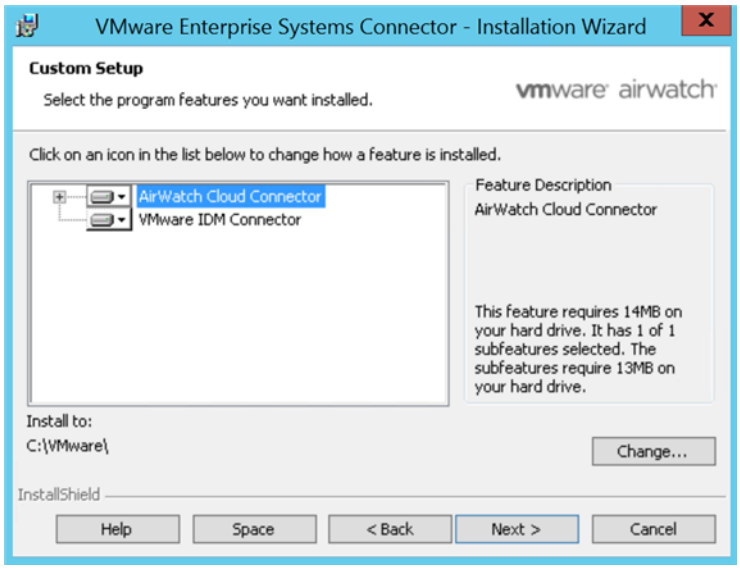
If a previous version of ACC is installed, the installer auto-detects it and offers the option to upgrade to the latest version. For more information on updating ACC, see ACC Updates.

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

4 In the Custom Setup page, select the components to install.

By default, both AirWatch Cloud Connector and VMware Identity Manager Connector are selected. To deselect a component, click the expansion arrow and select **This feature will not be available**.

For more information about the components, see Determine Which Components to Install.

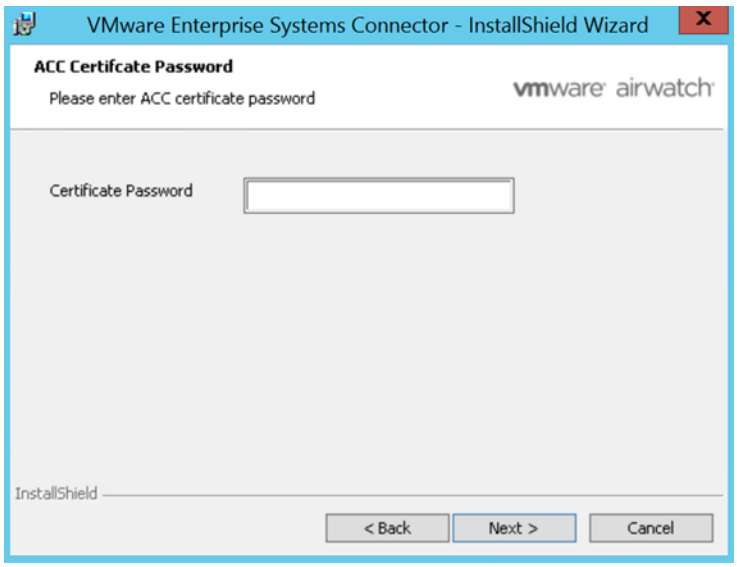


5 Select **Change...** to change the installation directory, if required, then click **Next**.

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 lower 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.

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

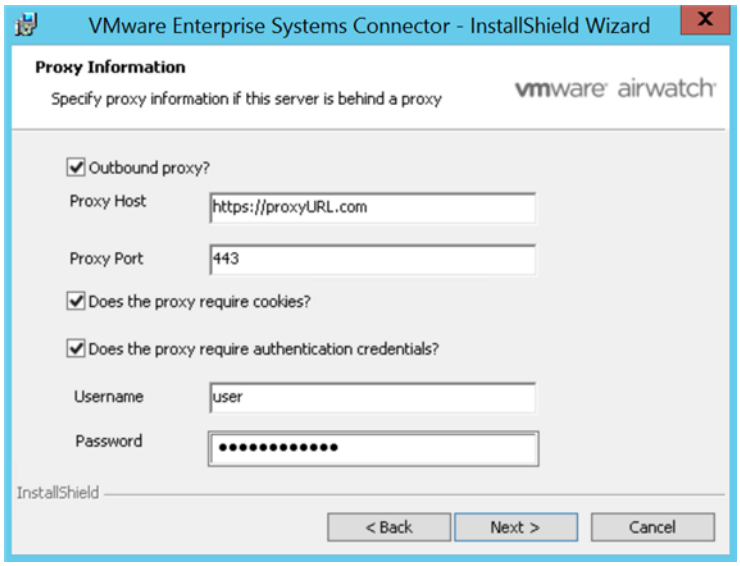
7 Enter the ACC certificate password that you provided on the System Settings page in AirWatch, then click **Next**.



8 If you plan on proxying ACC traffic through an outbound proxy, select the check box and provide proxy server information.

If required, enter the user name and password.

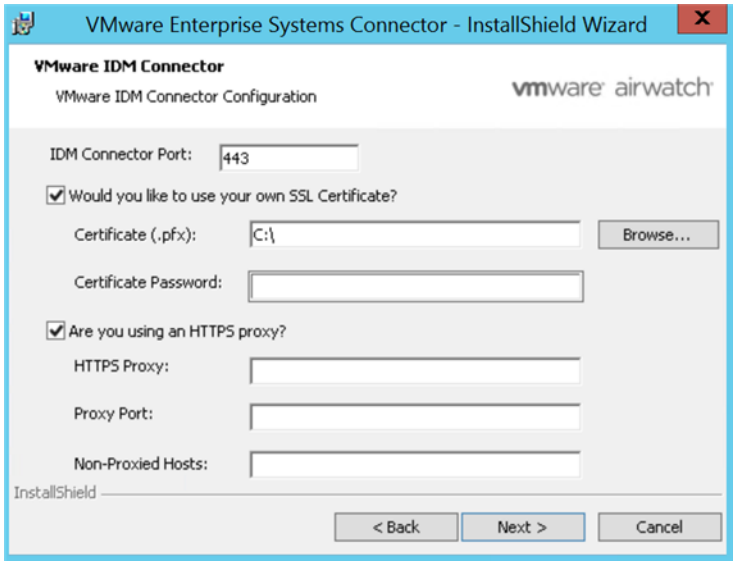
Note The settings on this page apply only to ACC. Proxy server information for the VMware Identity Manager Connector is entered separately later.



9 Click **Next**.

10 (VMware Identity Manager Connector only) In the IDM Connector Configuration page, enter the following information, then click **Next**.

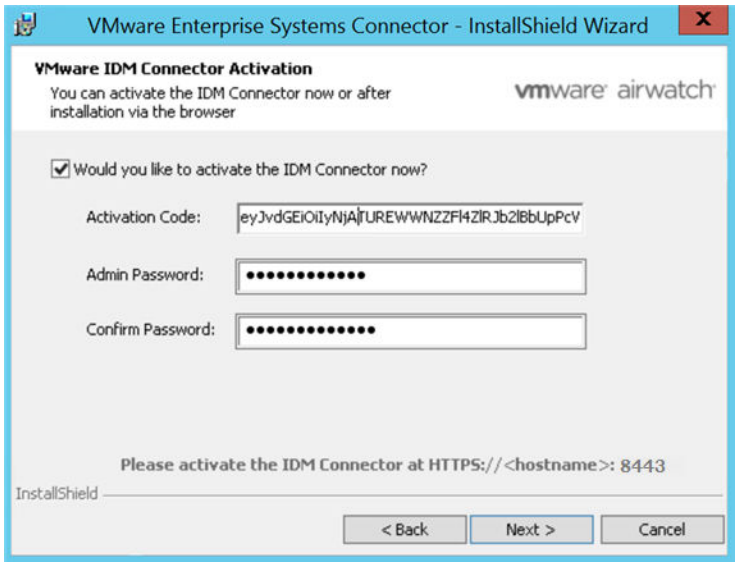
Option	Description
IDM Connector Port	Enter a port number if you want the VMware Identity Manager Connector to run on a port other than 443.
Would you like to use your own SSL certificate?	By default, a self-signed certificate is generated for the VMware Identity Manager Connector during the installation process. You can install a signed certificate later by logging into the connector admin pages at https://*vidmConnectorHostname*:8443/cfg/login and navigating to the Install Certificate page. 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.
Are you using an HTTPS proxy?	Select to configure an HTTPS proxy server for outbound communications, if required. **HTTPS Proxy**: The proxy server URL. Proxy servers that require authentication are not supported. **Proxy Port**: The HTTPS proxy server port. **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.



11 (VMware Identity Manager Connector only) In the VMware IDM Connector Activation page, select the check box if you want to activate the connector now.

Option	Description
Activation Code	If VMware Identity Manager is configured in the AirWatch Organization Group from which you downloaded the installer, this field is pre-populated with the activation code. If the field is not pre-populated, generate an activation code in the VMware Identity Manager administration console and copy and paste it here. See Generate Activation Code for VMware Identity Manager Connector for information.
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.

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.

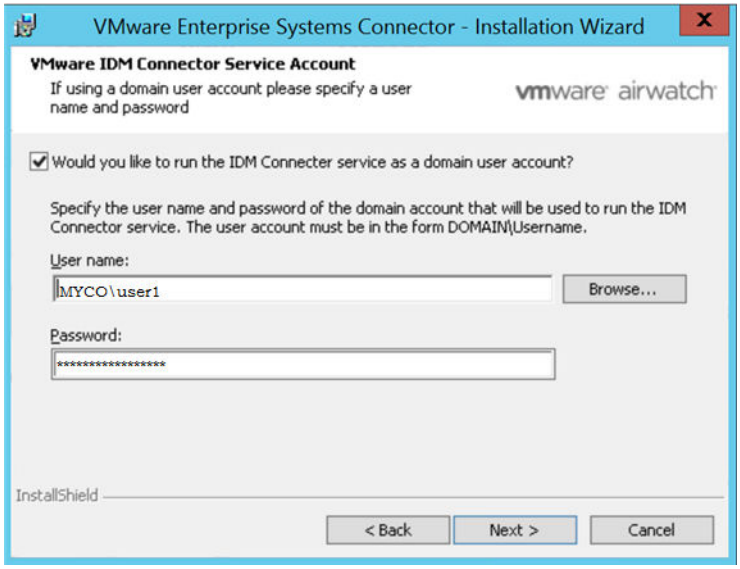


12 Click **Next**.

13 (VMware Identity Manager Connector only) In the IDM Connector Service Account page, select the check box if you want to run the IDM Connector service as a Windows domain user.

You must run the service as a domain user in the following cases.

- If you plan to connect to Active Directory (Integrated Windows Authentication)
- If you plan to use Kerberos authentication
- If you plan to integrate Horizon View with VMware Identity Manager and want to use the Perform Directory Sync or Configuring 5.x Connection Server options



Note To make any selections on this page, you must be running the installer as a domain user that is part of the administrator group on the Windows server.

Note If you are unable to locate domains or users when you click **Browse**, verify that you have met the prerequisites.

14 Click **Next**.

15 Click **Install** to begin the installation.

The installer displays a checkbox for auto-updating ACC. For more information on auto-update, see the ACC Auto-Update Option.

16 Click **Finish**.

Verify a Successful Enterprise Systems Connector Installation

After you install the Enterprise Systems Connector, you can verify a successful installation from within the AirWatch Console.

Note The Test Connection option only applies to the ACC component of the Enterprise Systems Connector. It does not apply to the VMware Identity Manager Connector component.

Procedure

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**.

2 Select **Test Connection** at the bottom of the screen and the following message displays.

3 If migrating, determine which features are new and test the new functionality to verify the migration was successful.

What to do next

Now that you have successfully installed the Enterprise Systems Connector, you can use it to integrate with your directory service infrastructure.

ACC Management

4

This section contains information about updating the ACC component and regenerating certificates.

This section includes the following topics:

ACC Updates

Upgrade the AirWatch Cloud Connector (ACC) from the AirWatch Console to take advantage of the latest bug fixes and enhancements. This process can be automated using the ACC auto-update option, or performed manually for situations where administrative control is a priority.

Note For information about upgrading the VMware Identity Manager Connector component, see Upgrading VMware Identity Manager Connector.

ACC Auto-Update

When you install ACC, by default, the auto-update check box is selected. Auto-update allows ACC to upgrade automatically to the latest version without user intervention by querying AirWatch for newer versions of ACC. AirWatch recommends that you allow auto-update (do not deselect the check box), but AirWatch made this optional for those environments and situations in which manual upgrades are preferred.

Note The auto-update option only applies to the ACC component of the Enterprise Systems Connector. It does not apply to the VMware Identity Manager Connector component.

Benefits to Auto-Update

- No need to determine manually if you need to upgrade and then have to search for the latest ACC version - the software does it for you.
- You always have the latest features, enhancements, and fixes.
- Most importantly, you have the most up-to-date security.

Update Process

ACC auto-update is performed using the Bank1 and Bank2 folders inside the Cloud Connector folder. AirWatch detects which of these folders is empty and streams the appropriate ACC files into it, in addition to emptying the contents of the other folder. For the subsequent update, AirWatch repeats the process except for the alternate folder. This process repeats each time a new version is auto-updated. This process is illustrated in the Update Process Flow figure.

Important Do not delete the Bank1 or Bank2 folders. The Bank1 and Bank2 folders are integral to the ACC auto-update process.

Figure 4-1. Update Process Flow

Auto-Update Security

ACC auto-updates are performed with security in mind. Every update is signed by the AirWatch Console and verified by ACC, so it only updates itself with a trusted upgrade. The upgrade process is also transparent to the AirWatch Admin. When a newer version is available, ACC knows from querying the AirWatch Console on port 443, and then an upgrade occurs.

While ACC is upgrading to the latest version, it is not available, so there is a short loss of service (that is, approx. 1 minute). When multiple ACC servers are installed, to ensure that all ACC services are not down at the same time, AirWatch incorporates a random timer to the upgrade process so ACC outages occur at different times for short periods of time.

If the ACC auto-updates, the version under Add or Remove Programs does not change - the original version is still listed. The version under Add or Remove Programs only changes when you run the full ACC installer. The best way to verify if the auto-update succeeded is to look in the ACC logs for what version is running.

Effects of Disabling Auto-Update

If you choose to disable this feature and ACC is not upgraded, ACC remains operational until any one of the following occurs.

- ACC is powered off and then on (purposely or a power outage).
- ACC must be reinstalled.

- AirWatch Console is upgraded to a later version.
- AirWatch, AWCM, or ACC certificates are regenerated. When certificates are regenerated the latest version of ACC must be installed and rebooted to recognize the new certificates.

Perform a Manual ACC Update

AirWatch does not recommend performing a manual ACC update, but this method is available as an option if it better suits the needs of your environment. For more information on the alternative, see ACC Auto-Update.

Procedure

1. Ensure auto-update is turned off in the AirWatch Console. This will save the latest ACC .zip files onto your ACC server when the console is upgraded and create entries in your ACC log file informing you that ACC needs to be upgraded.
2. Stop the AirWatch Cloud Connector service.
3. Perform one of the following approaches.
    a. The first approach is to manually unzip the ACC .zip files into the Bank folder mentioned in the log file. Either overwrite the existing files in this folder or delete all the files. On restarting the Cloud Connector service, the ACC version will get upgraded.
    b. The second approach is to use either of the Bank folders. In this case, leave either the .config or .config.old file available in the other Bank folder so the stock .config file can be repaired to customized values. Unzip the files and restart the Cloud Connector service, which will run with the newly upgraded version.

Regenerate Certificates

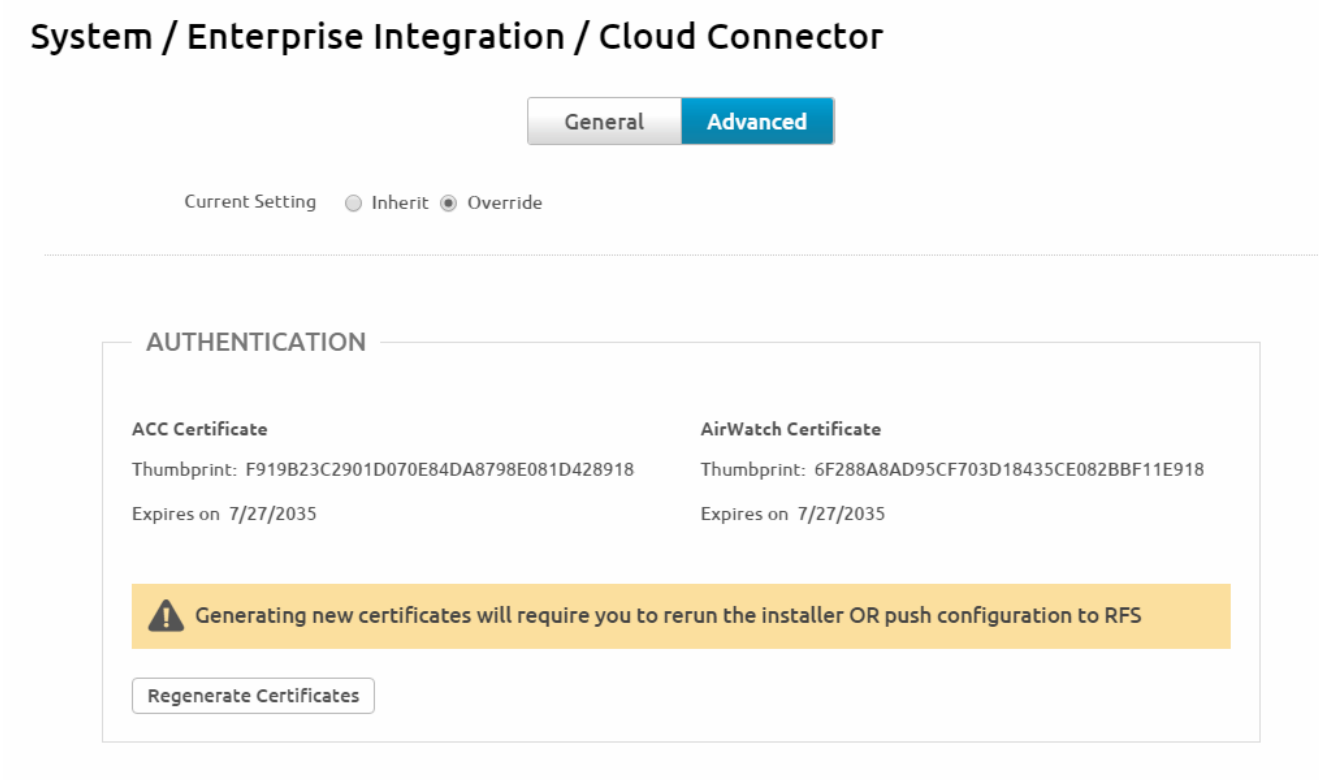
You might find it necessary to regenerate the certificates used for AirWatch and AirWatch Cloud Connector (ACC) servers, for example, if they expire or if your organization requires it on a regularly scheduled basis. The process is simple and is performed from the AirWatch Console, however it does require you to download and run the ACC installer again.

The certificates contain a thumbprint and expiration date. Both can be cleared and regenerated at the same time by selecting the Regenerate Certificates button and following the prompts. If you regenerate certificates, ACC will no longer be able to communicate with AirWatch and you will need to perform the installation procedure again to allow both server to recognize the new certificates.

Procedure

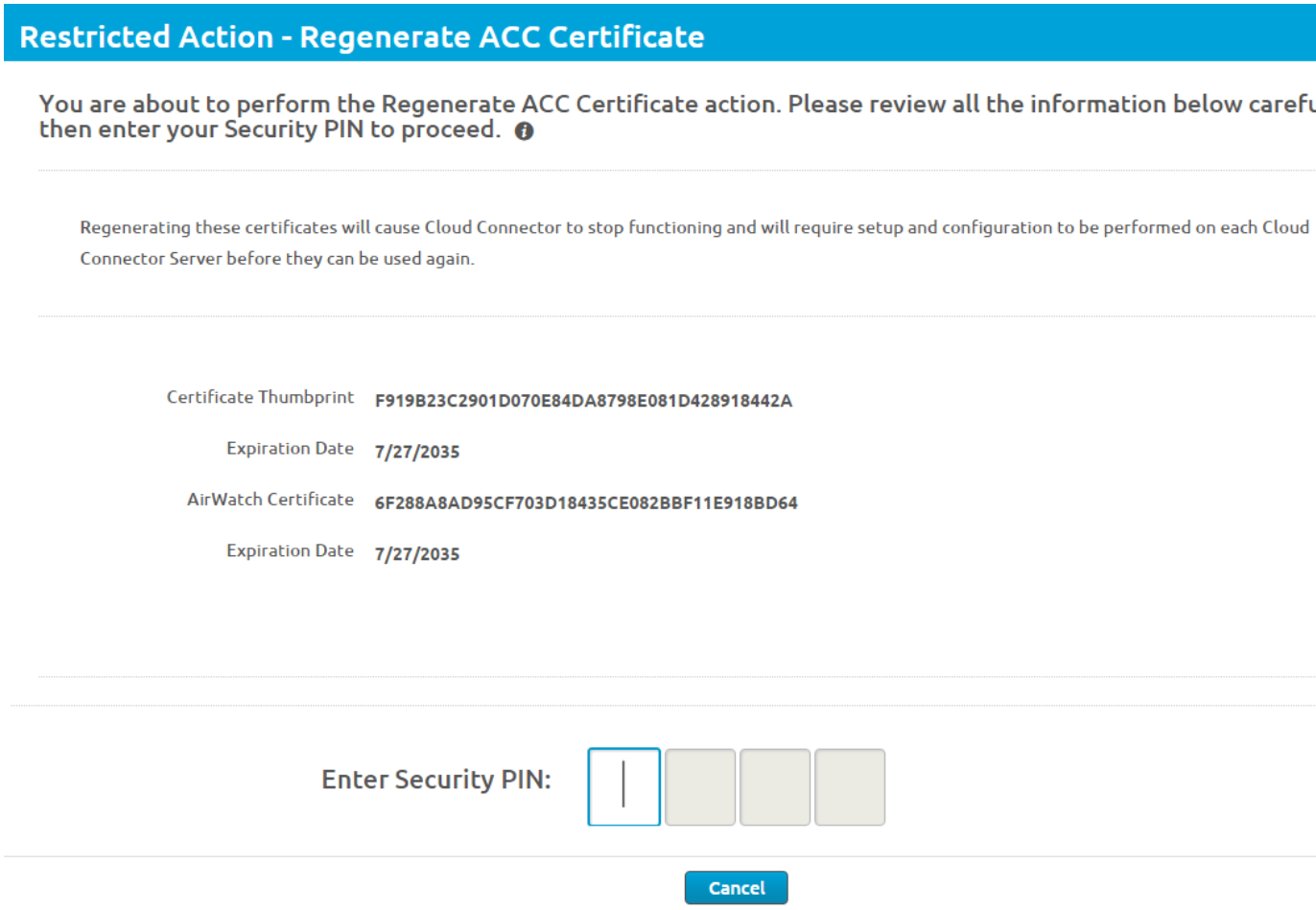
1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Cloud Connector**. Both certificates, their thumbprints, and expiration dates are shown on the Advanced tab.

2 Select **Regenerate Certificates** to generate a new certificate for the ACC and AirWatch servers.



3 If required, enter your security PIN to confirm the action and acknowledge the warning message. Old certificates are deleted and new certificates, thumbprints, and expiration dates are regenerated.

Figure 4-2.



When you enter your PIN to confirm, the ACC no longer can communicate with the AirWatch server. To restore communications between ACC and the AirWatch server, return to Installing ACC and complete all the steps again. This allows both servers to recognize the latest certificate and regain communications.

VMware Identity Manager Connector Configuration

5

This section contains information about configuring the VMware Identity Manager Connector and managing admin settings. It also includes advanced configuration information.

This section includes the following topics:

Configuring the VMware Identity Manager Connector

After you install the VMware Identity Manager Connector component, you need to configure it.

Configuring the VMware Identity Manager Connector involves the following tasks.

1 Generate an activation code and activate the connector, if you did not do so during installation.

2 Set up a directory.

3 Enable authentication adapters on the connector.

4 Enable outbound mode for the connector.

Generate Activation Code for VMware Identity Manager Connector

Log in to the VMware Identity Manager administration console and generate an activation code for the VMware Identity Manager Connector. This activation code is used to establish communication between your tenant and your connector instance.

Note If VMware Identity Manager is configured in the AirWatch Organization Group from which you downloaded the installer, you do not need to generate the activation code. If you are activating the connector from the installer, the activation code is pre-populated in the **Activation Code** field. Continue with the installer.

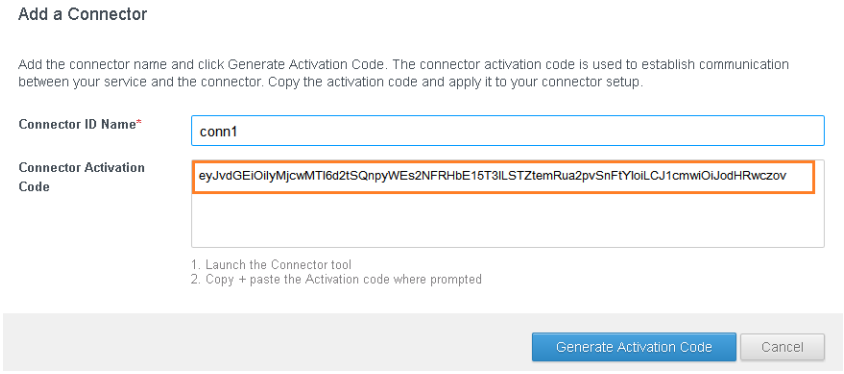
Prerequisites

(SaaS environments) You have your VMware Identity Manager tenant URL, for example, *mycompany.vmwareidentity.com*. When you receive your email confirmation, go to your tenant URL and sign in using the local admin credentials you received. This admin is a local user.

Procedure

1. Log in to the administration console.
2. (SaaS environments) Click **Accept** to accept the Terms and Conditions agreement.
3. Click the **Identity & Access Management** tab.
4. Click **Setup**.
5. On the Connectors page, click **Add Connector**.
6. Enter a name for the connector.
7. Click **Generate Activation Code.**

   The activation code displays on the page.
8. Copy the activation code and save it.



What to do next

If you are activating the VMware Identity Manager connector component while running the Enterprise Systems Connector installer, copy and paste the connector code into the VMware IDM Connector Activation page of the installer.

If you are activating the VMware Identity Manager connector component later, after installation, see Activate the VMware Identity Manager Connector.

Activate the VMware Identity Manager Connector

If you did not activate the VMware Identity Manager Connector from the Enterprise Systems Connector installer during installation, you can activate it later by going to the URL https://*vidmConnectorHostname*:8443.

Prerequisites

You have an activation code for the connector.

Procedure

1. Go to the URL https://*vidmConnectorHostname*:8443.

   Specify *vidmConnectorHostname* as a fully-qualified domain name. For example, https://myconnector.example.com:8443.
2. In the Welcome page, click **Continue**.
3. In the Set Passwords page, create a password for the connector admin pages, then click **Continue**.

   You can access these pages to collect log file bundles and upload certificates.
4. In the Activate Connector page, enter the activation code, then click **Continue**.

   A Setup is Complete message appears when the connector is activated successfully.

Set up a Directory

After you install and activate the VMware Identity Manager Connector, set up a directory in the VMware Identity Manager administration console and establish the connection with your enterprise directory to sync users and groups to the service.

VMware Identity Manager supports integrating the following types of directories.

- Active Directory over LDAP
- Active Directory (Integrated Windows Authentication)
- LDAP directory

See the *Directory Integration with VMware Identity Manager* guide for more information before you set up the directory. High-level tasks are listed here.

Prerequisites

The prerequisites depend on the type of directory you are integrating. See the *Directory Integration with VMware Identity Manager* guide for information.

Procedure

1 Log in to the VMware Identity Manager administration console.

Tip You can also go to the administration console by clicking the **Log in to the administration console** link in the Setup is Complete page that is displayed after you activate the connector.

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.
   - If you plan to sync Citrix-published resources to VMware Identity Manager, you must make **distinguishedName** a required attribute.

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

4 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 "Configuring Active Directory Connection to the Service" in the *Directory Integration with VMware Identity Manager* guide for information.

What to do next

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

Enable Authentication Adapters on the VMware Identity Manager Connector

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

When you created the directory, the Password authentication method was automatically enabled for it. The PasswordIdpAdapter was configured with the information you provided for the directory.

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.

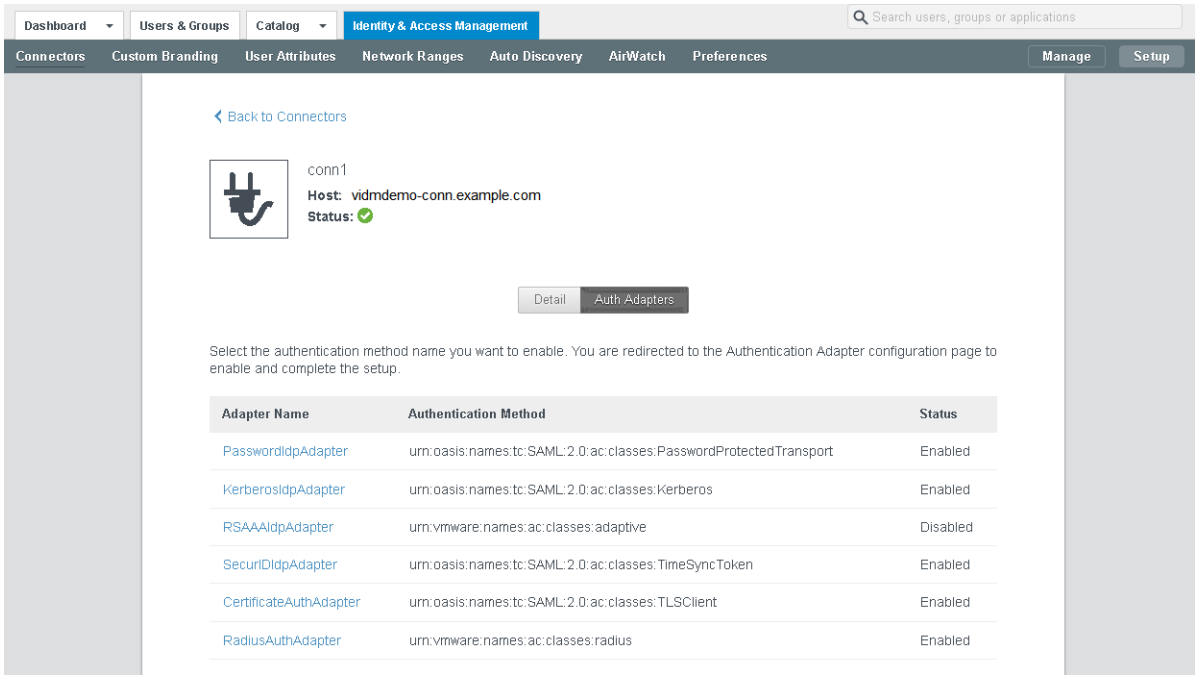
All available authentication adapters for the connector are listed.

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 VMware Identity Manager Connector

To enable outbound-only connection mode for the VMware Identity Manager 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*.

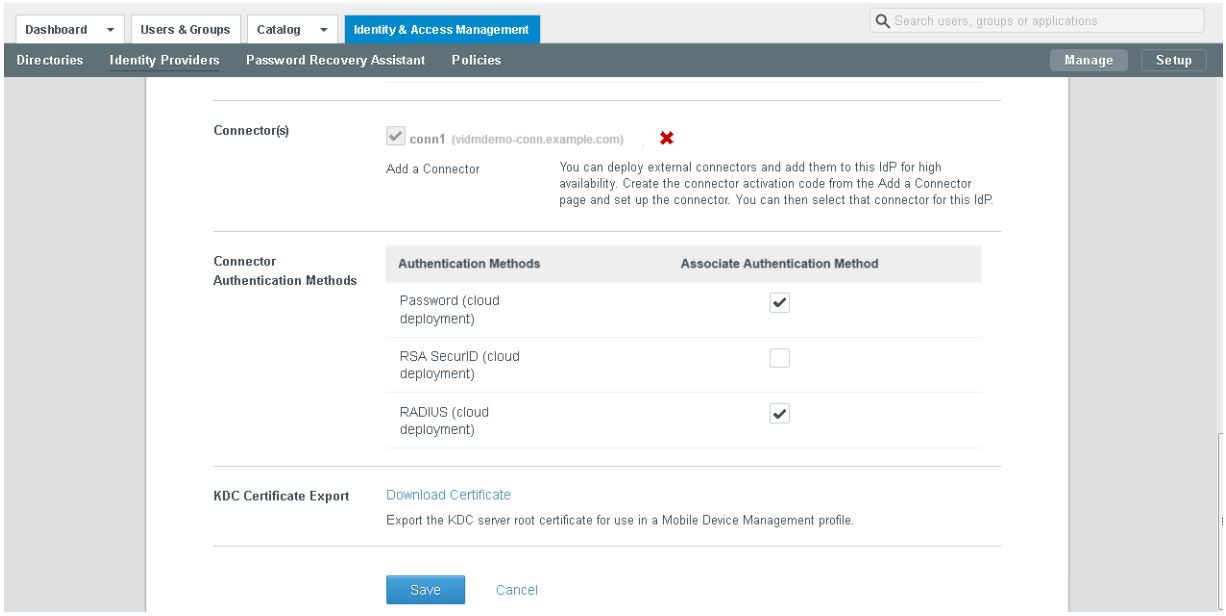
Note The connector can be used in both outbound and regular mode simultaneously. Even if you enable outbound mode, you can still configure Kerberos authentication for internal users using authentication methods and policies.

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.

Managing VMware Identity Manager Connector Admin Settings

After the initial VMware Identity Manager Connector configuration, you can go to the connector admin pages at any time to install certificates, manage passwords, and download log files.

The VMware Identity Manager Connector admin pages are available at https://*connectorFQDN*:8443/cfg/login, for example, https://myconnector.example.com:8443/cfg/login. Log in as the connector admin user with the admin password you created when you installed the connector.

Table 5-1. Connector Settings

Option	Description
Install Certificate	You can install a custom or self-signed certificate for the connector. If the connector is configured with a load balancer, you can install the load balancer's root certificate. The location of the connector root CA certificate is displayed on this page as well, on the **Terminate SSL on a Load Balancer** tab.
Change Password	On this page, you can change the connector admin password.
Log File Locations	You can access the connector log files directly on the host computer or bundle the connector log files into a zip file to download.

Using SSL Certificates

When the VMware Identity Manager Connector is installed, a default SSL server certificate is automatically generated. You can use this self-signed certificate for general testing of your implementation. VMware strongly recommends that you generate and install commercial SSL certificates in your production environment.

A certificate of authority (CA) is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate.

If you deploy the VMware Identity Manager Connector with the self-signed SSL certificate, the root CA certificate must be available as a trusted CA for any client that accesses the connector. The clients can include end user machines, load balancers, proxies, and so on. You can download the connector root CA from *https://connectorFQDN/horizon_workspace_rootca.pem*.

Install a CA-Signed Certificate for the VMware Identity Manager Connector

When the VMware Identity Manager Connector is installed, a default self-signed SSL server certificate is generated. You should generate and install commercial SSL certificates for your production environment.

Note If the connector points to a load balancer, the SSL certificate is applied to the load balancer.

Prerequisites

Generate a Certificate Signing Request (CSR) and obtain a valid, signed certificate from a CA. If your organization provides SSL certificates that are signed by a CA, you can use these certificates. The certificate must be in the PEM format.

Procedure

1. Log in to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Install Certificate**.

3 In the Terminate SSL on Identity Manager Appliance tab, for the **SSL Certificate** option, select **Custom Certificate**.

4 In the **SSL Certificate Chain** text box, paste the host, intermediate, and root certificates, in that order.

The SSL certificate works only if you include the entire certificate chain in the correct order. For each certificate, copy everything between and including the lines -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----

Ensure that the certificate includes the FQDN hostname.

5 Paste the private key in the **Private Key** text box. Copy everything between ----BEGIN RSA PRIVATE KEY and ---END RSA PRIVATE KEY.

6 Click **Save.**

Example: Certificate Examples

Certificate Chain Example
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Private Key Example
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
...
...
...
1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

Managing Your VMware Identity Manager Connector Passwords

When you installed the VMware Identity Manager Connector, you created a password for the admin user. You can change this password from the connector admin pages.

Important Make sure that you create strong passwords. Strong passwords should be at least eight characters long and include uppercase and lowercase characters and at least one digit or special character.

Procedure

1. Log in to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Change Password**.
3. Enter the old and new passwords.

   Important The admin user password must be at least 6 characters in length.
4. Click **Save**.

Viewing Log Files

The VMware Identity Manager Connector log files can help you debug and troubleshoot problems. The log files can be found in the *InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs directory.

The following log files are the most relevant.

Table 5-2. Log Files

Component	Log File Location on Windows	Description
Configurator Logs	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\configurator.log	Requests that the configurator receives from the REST client and the Web interface.
Connector Logs	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\connector.log	A record of each request received from the Web interface. Each log entry also includes the request URL, timestamp, and exceptions. No sync actions are recorded.
Apache Tomcat Logs	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\catalina.log	Apache Tomcat records of messages that are not recorded in other log files.

You can also download a log file bundle from the VMware Identity Manager Connector admin pages.

Download a Log Bundle

You can download a log file bundle for the VMware Identity Manager Connector from the connector admin pages. The log files can help you debug and troubleshoot problems.

To collect logs from each connector instance in your environment, log in to the admin pages for each instance.

Procedure

1. Log in to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login as the admin user.
2. Click **Log File Locations** and click **Prepare log bundle**.

   The information is collected into a zip file for you to download.
3. Download the log bundle.

Enabling Proxy Settings after Installation

If you did not configure HTTPS proxy settings for the VMware Identity Manager Connector component during installation, you can configure them later by editing the `C:\INSTALL_DIR\opt\vmware\horizon\workspace\conf\wrapper.conf` file.

Procedure

1. Log in to the Windows server.
2. Open the following file in a text editor:

   `C:\INSTALL_DIR\opt\vmware\horizon\workspace\conf\wrapper.conf`
3. Add the following entries after the last `wrapper.java.additional` entry:

```
wrapper.java.additional.32="-Dhttps.proxyHost=proxyServer"
wrapper.java.additional.33="-Dhttps.proxyPort=proxyServerPort"
```

where *proxyServer* is the HTTPS proxy server, *proxyServerPort* is the HTTPS proxy server port, and the number corresponds to the number of the `wrapper.java.additional` entry. For example, if the file already has 31 `wrapper.java.additional` entries, use 32 and 33 for the new entries as shown in the example.

4 If you are running the IDM Connector service as a domain user, also add the following lines:

```
wrapper.ntservice.account=DOMAIN/username
wrapper.ntservice.password=******
```

For example:

```
wrapper.ntservice.account=example/userA
wrapper.ntservice.password=******
```

5 From the command line, run the following commands as administrator:

a `C:\INSTALL_DIR\usr\local\horizon\scripts\horizonService.bat reinstall`

The command should return the following output:

```
Derived instance name: workspace
Reinstalling instance at
C:\VMware\IDMConnector\opt\vmware\horizon\workspace
wrapper | Service is running. Stopping it...
wrapper | Waiting to stop...
wrapper | VMware IDM Connector stopped.
wrapper | VMware IDM Connector removed.
wrapper | VMware IDM Connector installed.
```

b `C:\VMware\IDMConnector\usr\local\horizon\scripts\horizonService.bat start`

The command should return the following output:

```
Derived instance name: workspace
Starting instance at C:\VMware\IDMConnector\opt\vmware\horizon\workspace
wrapper | Starting the VMware IDM Connector service...
wrapper | VMware IDM Connector started.
```

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 instances in a cluster. If one of the connector instances becomes unavailable for any reason, other instances will still be available.

To create a cluster, you install new connector instances 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. This is because 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 VMware Identity Manager Connector Instances

After you install and configure the first VMware Identity Manager Connector instance, you can add additional connectors for high availability by installing new connector instances and configuring them in exactly the same way as the first connector instance.

Important The new connector instances must be activated against the same VMware Identity Manager service as the first connector instance.

Prerequisites

You have installed and configured the first connector instance, as described in Run the Enterprise Systems Connector Installer.

Procedure

1 Install and configure a new VMware Identity Manager Connector instance by following these instructions.

- Run the Enterprise Systems Connector Installer
- Configuring the VMware Identity Manager Connector

Important You must activate the new connector instance against the same VMware Identity Manager service as the first connector.

2 Associate the new VMware Identity Manager Connector with the `WorkspaceIDP` of the first connector instance.

a In the VMware Identity Manager 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 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 VMware Identity Manager Connector Instances to Built-in Identity Provider

Add New VMware Identity Manager Connector Instances to Built-in Identity Provider

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

Procedure

1 In the VMware Identity Manager 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 enabled 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.

When you configure the Kerberos authentication adapter, the VMware Identity Manager connector attempts to initialize Kerberos automatically. If the VMware IDM Connector service is not being run with sufficient privileges to initialize Kerberos, an error message appears. In this case, follow the instructions in http://kb.vmware.com/kb/2149753 to run a script to initialize Kerberos.

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

Prerequisites

- The Windows machine on which the VMware Identity Manager connector is installed must be joined to the domain.
- You must have installed the VMware Identity Manager Connector component as a domain user that is part of the administrator group on the Windows machine, and you must be running the VMware IDM Connector service as a Windows domain user.

Procedure

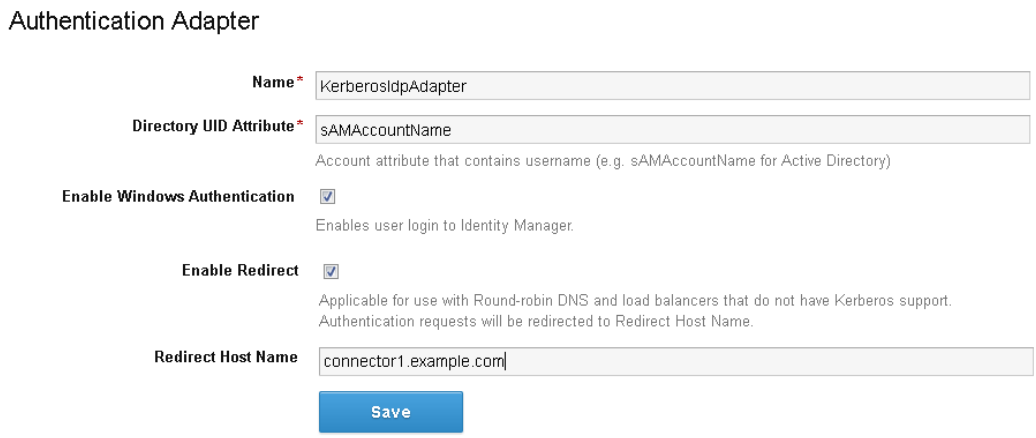
1. In the VMware Identity Manager administration console, click the **Identity & Access Management** tab.
2. Click **Setup**, then click the **Connectors** tab.

   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.

Option	Description
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 Click **Save**.

Note If you get an error stating that Kerberos initialization failed, run the Kerberos initialization script manually by following the instructions in http://kb.vmware.com/kb/2149753, then return to this page and configure the adapter.

7 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.

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 VMware Identity Manager Connector instances to it.

You must also configure certain settings on the load balancer, establish SSL trust between the load balancer and the connector instances, 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 load balancer documentation for more information.

- Load Balancer Timeout

  For the VMware Identity Manager 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 instances. 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 Manager Connector is configured behind 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 as a trusted root certificate.

The VMware Identity Manager Connector certificate can be downloaded from the connector admin pages at https://*connectorFQDN*:8443/cfg/ssl.

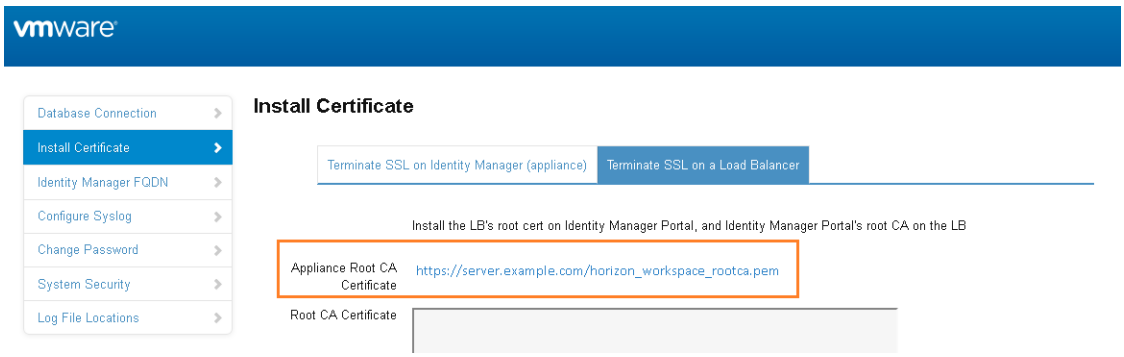
When the connector domain name points to the load balancer, the SSL certificate can only be applied to the load balancer.

Procedure

1 Log in to the connector admin pages, https://*connectorFQDN*:8443/cfg/login, 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.

Apply Load Balancer Root Certificate to the VMware Identity Manager Connector

When the VMware Identity Manager Connector is configured behind 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.

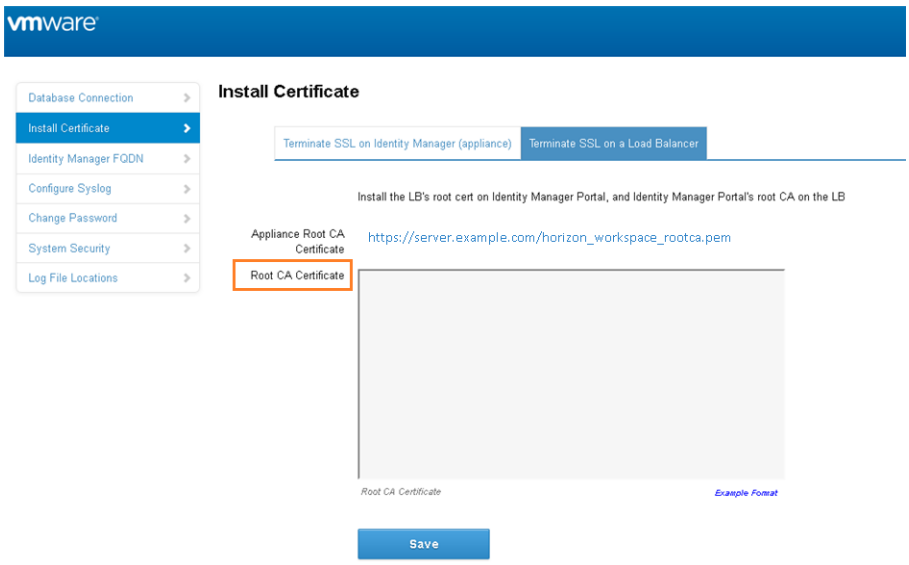
Procedure

1 Obtain the load balancer root certificate.

2 Go to the VMware Identity Manager Connector admin pages at https://*connectorFQDN*:8443/cfg/login 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 VMware Identity Manager Connector instances 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 instances are 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.

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 the connector instance.

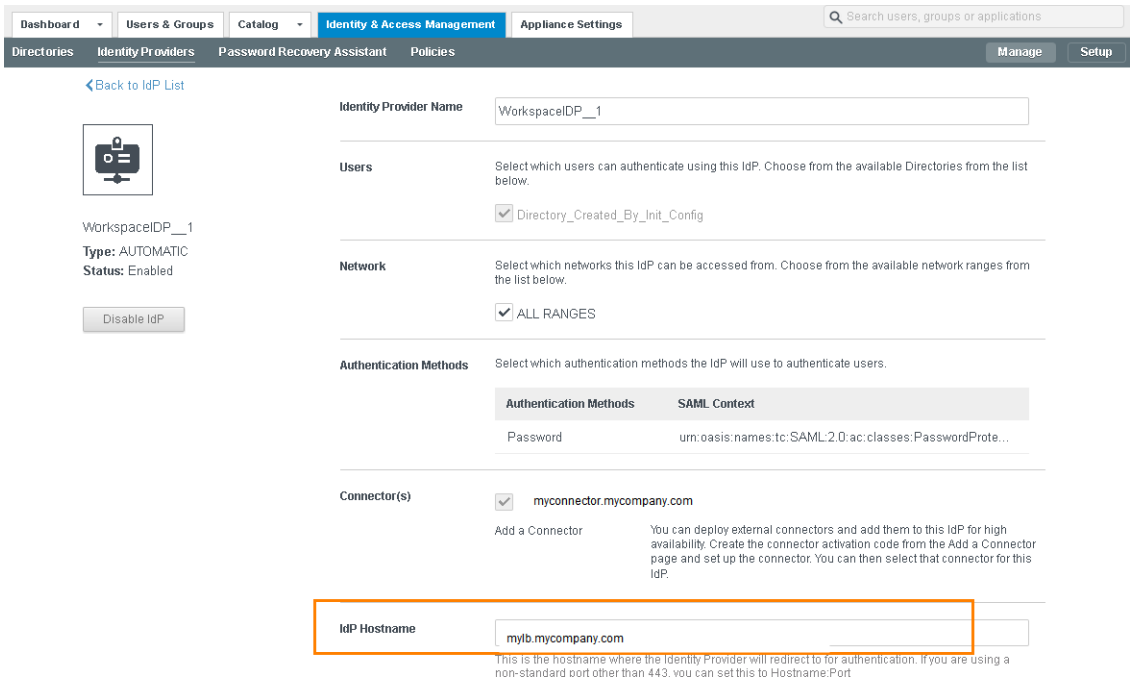
5 In the **IdP Hostname** text box, change the host name from the connector host name to the load balancer host name.

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
```



Deleting a VMware Identity Manager Connector Instance

You can delete a VMware Identity Manager Connector instance from the VMware Identity Manager service. A connector instance cannot be deleted if a directory is associated with it.

You may choose to delete a connector instance when you want to use the same host name for a new connector instance, for example.

Procedure

1. Log in to the VMware Identity Manager administration console.
2. Select the **Identity & Access Management** tab, then click **Setup**.
3. If a directory is associated with the connector you want to delete, delete the directory first.
   a. Click on the directory name in the **Associated Directory** column.
   b. Click **Delete Directory**.
4. In the **Setup > Connectors** page, click the **Delete** icon next to the connector instance you want to delete and click **Confirm**.

   The connector instance is deleted from the VMware Identity Manager service.
5. Uninstall the VMware Identity Manager Connector component from the Windows server on which it is installed.

Upgrading VMware Identity Manager Connector

To upgrade the VMware Identity Manager Connector component of the Enterprise Systems Connector, you download the installer from the new version of the AirWatch console and run the installer.

After upgrade, you do not need to generate a new activation code or activate the VMware Identity Manager Connector again. Your existing configuration applies to the upgraded connector.

Procedure

1. Log in to the new version of the AirWatch console.
2. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > VMware Enterprise Systems Connector**.
3. In the **General** tab, click **Download VMware Enterprise Systems Connector Installer**.

   The Download VMware Enterprise Systems Connector Installer page is displayed.
4. Create a password for the certificate and click **Download**.

   You need this password when you install the ACC component.
5. Save the installer file on the same Windows server on which the earlier version of the connector is installed.
6. Run the installer and follow the prompts to complete the upgrade.
7. If JRE is upgraded during the connector upgrade, you must restore the `cacerts` file that is backed up by the installer during upgrade.

   Copy the `opt\vmware\horizon\workspace\install\cacerts.sav` file to the newly-created `JAVA_HOME\lib\security` folder as a file named `cacerts`, without the `.sav` extension. This replaces the existing `cacerts` file in the folder.

   Note During upgrade, if the installer detects a lower version of JRE on the Windows server than the one packaged with the installer, you are prompted to install the new JRE version.
8. After the upgrade is complete, reboot the Windows server.

   Rebooting the server sets the JAVA_HOME variable to the latest JRE that is installed with the upgrade, enabling the connector to use the latest JRE.

Upgrading Java on the Connector Server

The VMware Identity Manager Connector component requires the Java Runtime Environment (JRE).

The JRE version required for the connector is packaged with the VMware Enterprise Systems Connector installer. When you upgrade the VMware Identity Manager connector component, you are prompted to upgrade the JRE version too. For information on upgrading JRE from the installer, see Upgrading VMware Identity Manager Connector.

If you want to upgrade JRE on the Windows server at any other time, follow these steps to ensure that the VMware Identity Manager connector continues to work correctly after the JRE upgrade.

Procedure

1. Before you upgrade JRE, make a backup of the JAVA_HOME\lib\security\cacerts file.
2. After upgrading JRE, copy the cacerts file to the same directory for the new JRE.
3. Edit the opt\vmware\horizon\workspace\conf\wrapper.conf file and change the `set.JAVA_HOME=C:\Program Files\Java\jreVersion` entry to the new JRE path.
4. Install the JCE Unlimited Strength policy files.

Directory Migration from ACC to the VMware Identity Manager Connector

6

Workspace ONE customers who have deployed Active Directory synchronization with VMware Identity Manager using only their existing ACC connectors must follow a migration procedure if they want to take advantage of the additional functionality included with the VMware Identity Manager Connector component of the Enterprise Systems Connector. This one-time procedure converts the ACC directory of type Other to a directory of type Active Directory over LDAP or Active Directory (Integrated Windows Authentication), which are associated with the VMware Identity Manager Connector. This procedure does not remove the existing directory or any entitlements associated with it.

Note The ACC-only model of directory sync and authentication with VMware Identity Manager is still available and supported by simply updating the ACC going forward. The migration procedure is only required if you want to take advantage of the new functionality.

Converting the Other directory includes the following tasks.

1. Convert the Other Directory to Active Directory over LDAP or Active Directory (Integrated Windows Authentication).
2. Configure additional VMware Identity Manager connector authentication methods for the directory, if necessary. The Password authentication method is available by default.
3. Edit the default policy and any custom policies to use Password or another VMware Identity Manager connector authentication method instead of Password (AirWatch Connector).
4. Stop user and group sync from AirWatch to the VMware Identity Manager directory.

This section includes the following topics:

- Convert Other Directory to Active Directory over LDAP or Active Directory (Integrated Windows Authentication)
- Stop Directory Sync from AirWatch to VMware Identity Manager

Convert Other Directory to Active Directory over LDAP or Active Directory (Integrated Windows Authentication)

You can convert a directory of type Other, which stores users and groups synced from AirWatch, to a directory of type Active Directory over LDAP or Active Directory (Integrated Windows Authentication), which are associated with the VMware Identity Manager connector. After you convert the directory, the VMware Identity Manager connector is used instead of ACC to sync users and groups from your enterprise directory to VMware Identity Manager.

Prerequisites

- Install and activate the VMware Identity Manager Connector component of the VMware Enterprise Systems Connector on a Windows server.

  To use some features, 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, and you must choose to run the IDM Connector service as a Windows domain user.

  This requirement applies to the following cases.

  - If you plan to convert the Other directory to Active Directory (Integrated Windows Authentication)
  - If you plan to use Kerberos authentication
  - If you plan to integrate Horizon View with VMware Identity Manager and want to use the Perform Directory Sync or Configuring 5.x Connection Server options
- The following Active Directory information is required:
  - If you are converting to Active Directory over LDAP, the Base DN, Bind DN, and Bind DN password are required. Using a Bind DN user account with a non-expiring password is recommended.
  - If you are converting to Active Directory (Integrated Windows Authentication), the domain's Bind user UPN address and password are required. Using a Bind DN user account with a non-expiring password is recommended.
  - If the Active Directory requires access over SSL or STARTTLS, the Root CA certificate of the Active Directory domain controller is required.
  - For Active Directory (Integrated Windows Authentication), when you have multi-forest Active Directory configured and the Domain Local group contains members from domains in different forests, make sure that the Bind user is added to the Administrators group of the domain in which the Domain Local group resides. If this is not done, these members are missing from the Domain Local group.

Procedure

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

2 Click the name of the directory that you want to convert.

3 In the directory page, click the **Convert** button.

4 In the Add Directory page, change the name of the directory if required and select the type of directory to which you want to convert the Other directory, **Active Directory over LDAP** or **Active Directory (Integrated Windows Authentication)**.

5 Enter the Active Directory connection information and continue with the wizard to set up the directory.

See "Configuring Active Directory Connection to the Service" in the *Directory Integration with VMware Identity Manager* guide for information.

Follow these guidelines.

- In the **Sync Connector** field, select the VMware Identity Manager connector that you installed.
- In the **Directory Sync and Authentication** section, select **Yes** for **Authentication**, unless you intend to use a third-party identity provider instead of the connector for authentication.
- Ensure that you set up the converted directory identically to the AirWatch directory so that it has the same directory structure. Select the same domains. When you specify the users and groups to sync, make the same selections as the AirWatch directory so that the same users and groups are synced to the converted directory.

6 On the last page of the wizard, click **Sync Directory**.

The directory is converted and set up to use the VMware Identity Manager connector. A Workspace Identity Provider is created, if one did not already exist, and the directory is associated with it automatically. The Password authentication method is already enabled for the directory.

7 (Optional) To enable other authentication methods for the directory, follow these steps.

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

b On the Connectors page, locate the connector and the worker with which the converted directory is associated, and click the link in the **Worker** column.

c In the worker page, click the **Auth Adapters** tab.

d Configure and enable the authentication adapters you want to use for the directory by clicking the link for each and entering the configuration information.

See *VMware Identity Manager Administration* for information about configuring authentication adapters.

8 Edit the default_access_policy_set and any custom policies to select VMware Identity Manager connector authentication methods instead of Password (AirWatch Connector).

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

b Click **Edit Default Policy**.

c Under **Policy Rules**, edit the **Authentication Methods** column for each rule and replace **Password (AirWatch Connector)** with **Password**, which is a VMware Identity Manager connector authentication method.

d Click the **Policies** tab again and edit custom policies, if any, to use Password or any other VMware Identity Manager connector authentication method that you have configured.

Important If you do not change Password (Airwatch Connector) to Password or another VMware Identity Manager connector-based authentication method, users of the converted directory will not be able to log in.

What to do next

Stop directory sync from AirWatch to the converted directory.

Stop Directory Sync from AirWatch to VMware Identity Manager

After you convert the Other directory to Active Directory over LDAP or Active Directory (Integrated Windows Authentication) and associate it with a VMware Identity Manager connector, the VMware Identity Manager connector is used to sync users and groups from your enterprise directory to the converted directory. You must stop user and group sync from AirWatch to the VMware Identity Manager directory.

Procedure

1 In the AirWatch console, navigate to your Organization Group.

2 Navigate to the **Groups & Settings > All Settings > System > Enterprise Integration > VMware Identity Manager** page.

3 Click the **Delete** button at the bottom of the page.

The directory conversion is complete. Users and groups are now synced from your enterprise directory to the VMware Identity Manager service by the VMware Identity Manager connector. Users can continue to log in and access their applications.

Note The domain name displayed on the login page may be different after the directory is converted if the domain name is different from the domain NETBIOS name. With AirWatch sync, the domain NETBIOS name is displayed. With VMware Identity Manager connector sync, the domain name is displayed.