VMware AirWatch Cloud Connector

VMware Workspace ONE UEM 2005

vmware®

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

https://docs.vmware.com/

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

Contents

VMware AirWatch Cloud Connector

1

The VMware AirWatch Cloud Connector provides organizations with the ability to integrate Workspace ONE UEM powered by AirWatch with their back-end enterprise systems. This documentation describes setting up AirWatch Cloud Connector for on-premises and SaaS deployments.

In an on-premises deployment, your organization hosts all Workspace ONE UEM components and servers on its internal networks. For on-premises deployments, before proceeding with this guide, you should have read and performed the procedures in the **VMware AWCM Guide**. In a SaaS deployment, certain Works components are hosted in the cloud. If you are unsure whether your deployment is on-premises or SaaS, contact a VMware support representative.

The VMware AirWatch Cloud Connector runs in the internal network, acting as a proxy that securely transmits requests from Workspace ONE UEM to the organization's critical enterprise infrastructure components. This allows organizations to leverage the benefits of VMware Mobile Device Management (MDM), running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems. Refer to the Chapter 2 VMware AirWatch Cloud Connector Architecture for more information.

The VMware AirWatch Cloud Connector integrates with the following internal components:

- Email Relay (SMTP)
- Directory Services (LDAP/AD)
- Email Management Exchange 2010 and later (PowerShell)
- Lotus Domino Web Service (HTTPS)
- Syslog (Event log data)
- Microsoft Certificate Services (PKI)
- Simple Certificate Enrollment Protocol (SCEP PKI)
- Third-party Certificate Services (on-premises only)

This chapter includes the following topics:

VMware AirWatch Cloud Connector System Requirements (On Premises and SaaS)

To deploy the VMware AirWatch Cloud Connector as part of an on-premises or SaaS deployment, ensure your system meets the necessary requirements.

Hardware Requirements

Use the following requirements as a basis for creating your VMware AirWatch Cloud Connector server. For SaaS deployments, the AirWatch Cloud Connector Server can be a VM or physical server.

Table 1-1. ACC Hardware Requirements

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
CPU Cores	2 CPU cores	2 load-balanced servers with 2 CPU cores	2 load-balanced servers with 2 CPU cores	3 load-balanced servers with 2 CPU cores
RAM	4 GB	4 GB each	4 GB each	8 GB each
Disk Space	50 GB	50 GB each	50 GB each	50 GB 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 on the same server, add these requirements to the ACC requirements.

Table 1-2. VMware Identity Manager Connector Requirements

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores
RAM	6 GB each	8 GB each	16 GB each	16 GB each
Disk Space	50 GB each	50 GB each	50 GB each	50 GB each

Notes:

- VMware AirWatch Cloud Connector traffic is automatically load-balanced by the AWCM component. It does not require a separate load balancer. Multiple VMware AirWatch Cloud Connectors 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.
- 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 VMware AirWatch Cloud Connector application, Windows OS, and .NET runtime. Additional disk space is allocated for logging.

Software Requirements

Ensure your VMware AirWatch Cloud Connector server meets all the following software requirements.

Requirement	Notes
Windows Server 2008 R2 SP1 or Windows Server 2012 R2 or Windows Server 2016 Windows Server 2019 Desktop Experience	The VMware AirWatch Cloud Connector is intended to run on an English-language Windows OS.
Install PowerShell on the server	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.
Install .NET Framework 4.8	The VMware AirWatch Cloud Connector will not auto update to v1912 unless .NET 4.8 is installed. Install .NET 4.8 on the VMware AirWatch Cloud Connector servers to allow auto update to continue.

General Requirements

Ensure your VMware AirWatch Cloud Connector is set up with the following general requirements to ensure a successful installation.

Requirement	Notes
Ensure that you have remote access to the servers that Workspace ONE UEM is installed on	Workspace ONE UEM 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 a Workspace ONE UEM consultant provides. Some customers also provide Workspace ONE UEM with VPN credentials to directly access the environment as well.
Installation of Notepad++ (Recommended)	Workspace ONE UEM 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, PowerShell, etc.

On Premises Network Requirements: Core Components

For configuring the ports listed below, all the 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 VMware AirWatch Cloud Connector. The outbound connection required for use by VMware AirWatch Cloud Connector must remain open at all times.

Source Component	Destination Component	Protocol	Port	Verification
VMware AirWatch Cloud Connector Server	AWCM Server	HTTPS	2001	Telnet from VMware AirWatch Cloud 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, VMware AirWatch Cloud Connector must be able to query Workspace ONE UEM console for updates using port 443. If you are using VMware AirWatch Cloud Connector 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.
VMware AirWatch Cloud Connector Server	Workspace ONE UEM console	HTTP or HTTPS	80 or 443	Telnet from VMware AirWatch Cloud Connector to the 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, VMware AirWatch Cloud Connector must be able to query Workspace ONE UEM console for updates using port 443.
VMware AirWatch Cloud Connector Server	API server (or wherever API is installed)	HTTPS	443	Verify by navigating to the URL of your API server.
VMware AirWatch Cloud Connector Server	CRL: http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	For various services to function properly

On Premises Network Requirements: Optional Integrations

For configuring the ports listed below, all the 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 VMware AirWatch Cloud Connector. The outbound connection required for use by VMware AirWatch Cloud Connector must remain open at all times.

Source Component	Destination Component	Protocol	Port
VMware AirWatch Cloud Connector Server	Internal SMTP	SMTP	25
VMware AirWatch Cloud Connector Server	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269
VMware AirWatch Cloud Connector Server	Internal SCEP	HTTP or HTTPS	80 or 443
VMware AirWatch Cloud Connector Server	Internal ADCS	DCOM	135, 1025-5000, 49152-65535
VMware AirWatch Cloud Connector Server	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443

SaaS Network Requirements: Core Components

For configuring the ports listed below, all the 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 VMware AirWatch Cloud Connector. The outbound connection required for use by VMware AirWatch Cloud Connector must remain open at all times.

Source Component	Destination Component	Protocol	Port	Verification
VMware AirWatch Cloud Connector Server	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.)
VMware AirWatch Cloud Connector Server	Workspace ONE UEM 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, VMware AirWatch Cloud Connector must be able to query Workspace ONE UEM console for updates using port 443.

Source Component	Destination Component	Protocol	Port	Verification
VMware AirWatch Cloud Connector Server	Workspace ONE UEM 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.) VMware AirWatch Cloud Connector to API access is required for the proper functioning of the AirWatch Diagnostics service.
VMware AirWatch Cloud Connector Server	CRL: http://crl3.digicert.com/sha2-assured-cs-g1.crl	HTTP	80	For various services to function properly

SaaS Network Requirements: Optional Integrations

For configuring the ports listed below, all the 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 VMware AirWatch Cloud Connector. The outbound connection required for use by VMware AirWatch Cloud Connector must remain open at all times.

Source Component	Destination Component	Protocol	Port
VMware AirWatch Cloud Connector Server	Internal SMTP	SMTP	25
VMware AirWatch Cloud Connector Server	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269
VMware AirWatch Cloud Connector Server	Internal SCEP	HTTP or HTTPS	80 or 443
VMware AirWatch Cloud Connector Server	Internal ADCS	DCOM	135, 1025-5000, 49152-65535
VMware AirWatch Cloud Connector Server	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443

AWCM Pre-install Requirement (On-Premises)

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

VMware AirWatch Cloud Connector Architecture

2

The VMware AirWatch Cloud Connector is a Windows service that can be installed on a physical or virtual server running an English-language version of Windows 2008 R2 or higher. It operates from within your internal network and can be configured behind any existing Web Application Firewalls (WAF) or load balancers.

By initiating a secure HTTPS connection from VMware AirWatch Cloud Connector to the AirWatch Cloud Messaging Service (AWCM), VMware AirWatch Cloud Connector can periodically transmit information from your internal resources such as AD, LDAP, etc. to the Workspace ONE UEM console without any firewall changes. If you plan on proxying VMware AirWatch Cloud Connector traffic through an outbound proxy, then there are settings in VMware AirWatch Cloud Connector that allow for proxying.

Supported Configurations

Use VMware AirWatch Cloud Connector in the following configurations:

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

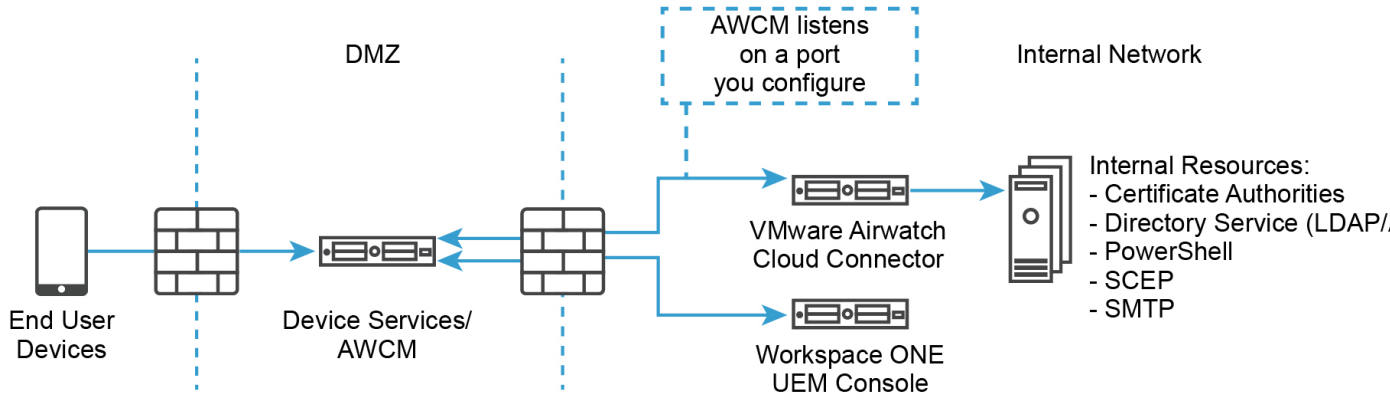
This chapter includes the following topics:

VMware AirWatch Cloud Connector Deployment Model

Your VMware AirWatch Cloud Connector deployment has a different configuration depending on whether you are deploying the ACC on-premises or in SaaS model.

ACC On-Premises Deployment Model

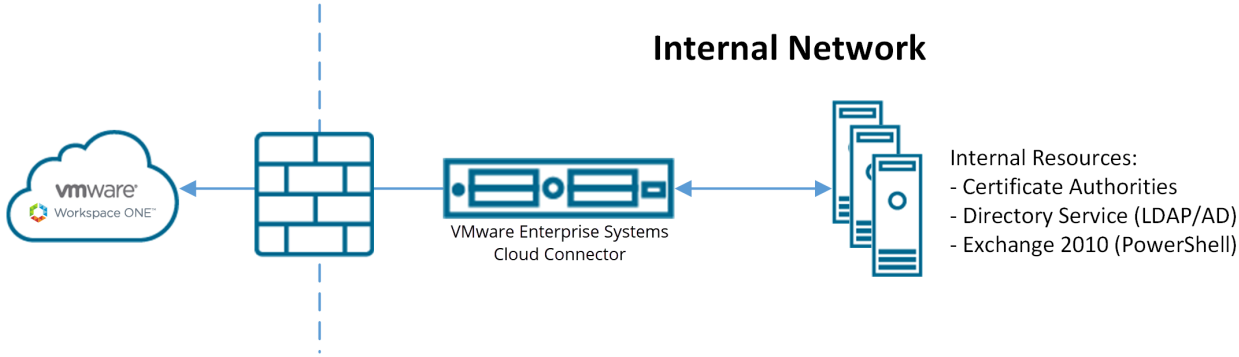
In an on-premises deployment model, the VMware AirWatch Cloud Connector resides in your internal network and communicates with AWCM, which typically is installed on the device services server.



ACC SaaS Deployment Model

In a SaaS deployment model, the VMware AirWatch Cloud Connector resides in your internal network and integrates with your internal systems, allowing AirWatch to leverage them for various functionality (e.g. certificates, directory services).

Figure 2-1. ACC Saas Deployment Model



ACC Certificate Integration Workflows

Certificates are used to authenticate communication between the Workspace ONE UEM console and VMware AirWatch Cloud Connector. In on-premises deployments, data and traffic between AWCM and VMware AirWatch Cloud Connector is encrypted and signed.

How Certificates are Generated

1 You enable the VMware AirWatch Cloud Connector and then generate certificates for Workspace ONE UEM and VMware AirWatch Cloud Connector.

- Both certificates are unique to the group selected in the Workspace ONE UEM console and reside on the Workspace ONE UEM server.
- Both certificates are generated from a trusted Workspace ONE UEM root.

2 You install VMware AirWatch Cloud Connector. The VMware AirWatch Cloud Connector certificate that Workspace ONE UEM generates is automatically bundled and installed with VMware AirWatch Cloud Connector.

How Data is Routed (On-Premises only)

1 Workspace ONE UEM sends requests to AWCM. Requests are SSL encrypted using HTTPS.

2 The VMware AirWatch Cloud Connector queries AWCM for Workspace ONE UEM requests. Requests are SSL encrypted using HTTPS.

3 All data is sent through AWCM.

The VMware AirWatch Cloud Connector configuration trusts only messages signed from the Workspace ONE UEM environment. This trust is unique per group.

Any additional VMware AirWatch Cloud Connector servers set up in the same Workspace ONE UEM group as part of a highly available (HA) configuration are issued the same unique VMware AirWatch Cloud Connector certificate. For more information about high availability, please refer to the **VMware Recommended Architecture Guide**, available on docs.vmware.com.

How Data is Secured (On-Premises only)

The Workspace ONE UEM server sends each request as an encrypted and signed message to the AWCM.

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

VMware AirWatch Cloud Connector Installation Process

3

You must perform several tasks to configure and install the VMware AirWatch Cloud Connector in your internal network.

Procedure

1. (On-premises customers only) Install Secure Channel Certificate on AWCM (On-Premises Deployments).

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

2. 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.

3. Enable VMware AirWatch Cloud Connector from the Workspace ONE UEM console.

   Before you install VMware AirWatch Cloud 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 VMware AirWatch Cloud Connector.

4. Run the VMware AirWatch Cloud Connector Installer.

   Run the VMware AirWatch Cloud Connector installer on your configured server that meets all of the prerequisites.

5. Verify a Successful VMware AirWatch Cloud Connector Installation.

   After you install VMware AirWatch Cloud Connector you can verify a successful installation from within the Workspace ONE UEM console.

Install Secure Channel Certificate on AWCM (On-Premises Deployments)

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

This step is applicable to on-premises deployments. If you have not already installed a **Secure Channel Certificate**, then follow the steps below to do so, which walk you through installing a **Secure Channel Certificate** on a local AWCM server.

Important Perform the following steps on the server running AWCM. If your AWCM server does not have access to the console server, then you can download the installer file from another server (for example, the console server) and copy it to the AWCM server. If the download fails on the server running AWCM, then contact Workspace ONE Support for potential workarounds.

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 Establish Communications with AWCM.
7. Proceed with the installation steps for VMware AirWatch Cloud Connector, available at docs.vmware.com.

What to do next

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

Establish Communications with AWCM

SaaS and on-premises customers should establish communications with AWCM. Performing this action allows you to configure a Workspace ONE UEM 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 AWCM Server	Check this box to allow the connection between the Workspace ONE UEM console and the AWCM server.
AWCM Server External URL	This field allows you to enter the servername used by external components and devices (e.g., VMware AirWatch Cloud Connector) to securely (using HTTPS) communicate with AWCM. An example of an VMware AirWatch Cloud Connector URL is: Acme.com. Do not add https:// since this is assumed by the application and automatically added.
AWCM 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 Service Internal URL	This URL allows you to reach AWCM from internal components and devices (e.g., Admin console, Device Services, etc.). Examples of AWCM URLs are: https://Acme.com:2001/awcm or http://AcmeInternal.Local/awcm. If your AWCM server and Workspace ONE UEM 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.
Test Connection	Send a test communication from the UEM console to the configured AWCM URL to verify that the connection is valid and functional. When the test completes, a **View Trace** button appears. Select this button to view the trace route of the connection you configured.

Enable VMware AirWatch Cloud Connector from the Workspace ONE UEM console

Before you install VMware AirWatch Cloud Connector, you must first enable it, generate certificates, and select the enterprise services and Workspace ONE UEM services to be integrated. After completing this step, you can install VMware AirWatch Cloud Connector.

Important Perform the following steps on the server running VMware AirWatch Cloud Connector. Do not download the installation program onto another computer and copy it to the VMware AirWatch Cloud 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 VMware AirWatch Cloud Connector and display the **General** tab.
Enable Auto Update	Select to enable VMware AirWatch Cloud Connector to automatically update when a newer version is available. For more information regarding auto-update, refer to Run the VMware AirWatch Cloud Connector Installer.

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

Setting	Description
Communication with AWCM	Select how the VMware AirWatch Cloud 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 VMware AirWatch Cloud Connector server from resolving the External AWCM URL. For example, if VMware AirWatch Cloud Connector is on your internal network and your AWCM server is in a DMZ.
Enterprise Services	Select the **Enabled** or **Disabled** buttons to enable or disable **Enterprise Services**. The services you select (enabled) will integrate with VMware AirWatch Cloud Connector. ■ SMTP (Email Relay) Workspace ONE UEM SaaS offers email delivery through its own SMTP, but you can enable VMware AirWatch Cloud 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) ■ Syslog (Client/server protocol used to integrate with the AirWatch 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) ■ 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 VMware AirWatch Cloud 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 Workspace ONE UEM components you enable integrate with VMware AirWatch Cloud Connector. VMware 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)

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** screen displays.

6 Enter a password for the VMware AirWatch Cloud Connector certificate in the fields.

The password will be needed later when you run the VMware AirWatch Cloud Connector installer and need to enter the certificate password.

7 Select **Download** and save the **AirWatch Cloud Connector x.x.x.x Installer.exe** file on the VMware AirWatch Cloud Connector server for use later in Running the VMware AirWatch Cloud Connector Installer.

Run the VMware AirWatch Cloud Connector Installer

Run the VMware AirWatch Cloud Connector installer on your configured server that meets all of the prerequisites.

Prerequisites

On-premises customers should ensure the server you are installing VMware AirWatch Cloud Connector on can reach AWCM by browsing to "https://{url}:<port>/awcm/status", where {url} is the Workspace ONE UEM environment URL and <port> is the external port you configured for AWCM to communicate.

SaaS customers should ensure the server you are installing VMware AirWatch Cloud Connector on can reach AWCM by browsing to "https://awcmXXX.awmdm.com/awcm/status". (Replace 'XXX' with the same number as used in your environment URL, for example, '100' for cn100.). If your server fails to connect to the AWCM URL, ensure that the URL matches the URL provided in your onboarding documents.

Note If you previously used the VMware Enterprise Systems Connector and you want to install the AirWatch Cloud Connector on the same server, you must download the VMware Identity Manager Connector installer and run it again before running the AirWatch Cloud Connector installer.

You should see the status of the AWCM with no SSL errors. If there are errors, resolve them before continuing or the VMware AirWatch Cloud Connector will not properly function.

Procedure

1 Open the installer on the VMware AirWatch Cloud Connector server. When the **Welcome** screen appears, select **Next**.

The installer verifies prerequisites on your VMware AirWatch Cloud Connector server.

If a previous version of VMware AirWatch Cloud Connector is installed, the installer auto-detects it and offers the option to upgrade to the latest version. For more information on updating VMware AirWatch Cloud Connector, see Chapter 4 VMware AirWatch Cloud Connector Upgrades.

2 Accept the license agreement and then select **Next**.

3 Select **Change...** to select the installation directory and then select **Next**.

4 Enter the **Certificate Password** that you provided on the **System Settings** page in Workspace ONE UEM. Select **Next**.

5 If you plan on proxying VMware AirWatch Cloud Connector traffic through an outbound proxy, then select the check box and provide proxy server information. If needed, enter the **Username** and **Password** credentials and then select **Next**.

6 When the installation screen appears, select **Install** to begin the installation.

The installer displays a checkbox for auto-updating VMware AirWatch Cloud Connector. For more information on auto-update, see Chapter 4 VMware AirWatch Cloud Connector Upgrades.

7 Select **Finish**.

Verify a Successful VMware AirWatch Cloud Connector Installation

After you install VMware AirWatch Cloud Connector you can verify a successful installation from within the Workspace ONE UEM console.

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 **Cloud Connector is active** message displays.

3 If migrating, determine which features are new in VMware AirWatch Cloud Connector and test the new functionality to verify the migration was successful.

What to do next

Now that you have successfully installed VMware AirWatch Cloud Connector, you can use it to integrate with your directory service infrastructure.

VMware AirWatch Cloud Connector Upgrades

4

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

VMware AirWatch Cloud Connector Auto-Update

VMware AirWatch Cloud Connector is set to auto-update by default. This toggle is available in the UEM console. Auto-update allows VMware AirWatch Cloud Connector to upgrade automatically to the latest version without any user intervention by querying Workspace ONE UEM for newer versions of VMware AirWatch Cloud Connector. VMware recommends that you allow auto-update, but this configuration is optional for those environments and situations in which manual upgrades are preferred.

Benefits

- No need to determine manually if you need to upgrade and then have to search for the latest VMware AirWatch Cloud Connector version – the software does it for you.
- Since it assures you stay updated, you always have the latest features, enhancements and fixes.
- Most importantly, it ensures you have the most up-to-date security.

Update Process

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

Important Do not delete the **Bank1** or **Bank2** folders. The **Bank1** and **Bank2** folders are integral to the VMware AirWatch Cloud Connector auto-update process.

Figure 4-1. ACC Auto-Update Flow

Auto-Update Security

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

While VMware AirWatch Cloud Connector is upgrading to the latest version, it will not be available, so there will be a short loss of service (i.e., approx. 1 minute). For those who have multiple VMware AirWatch Cloud Connector servers, to ensure all VMware AirWatch Cloud Connector services are not down at the same time, AirWatch incorporates a random timer to the upgrade process so VMware AirWatch Cloud Connector outages will occur at different times for very short periods of time.

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

Effects of Disabling Auto-Update

If you choose to disable this feature, then there are some drawbacks by having to do all VMware AirWatch Cloud Connector upgrades manually. If VMware AirWatch Cloud Connector is not upgraded, it will continue to remain operational until any one of the following occurs:

- If VMware AirWatch Cloud Connector is powered Off and then On (purposely or power outage).
- If VMware AirWatch Cloud Connector needs to be reinstalled.
- If Workspace ONE UEM console is upgraded to a later version.
- If Workspace ONE UEM, AWCM, or VMware AirWatch Cloud Connector certificates are regenerated, which would then require the latest version of VMware AirWatch Cloud Connector installed and a reboot to recognize the new certificate(s).

This chapter includes the following topics:

Perform a Manual VMware AirWatch Cloud Connector Update

Workspace ONE UEM does not recommend performing a manual VMware AirWatch Cloud Connector 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 VMware AirWatch Cloud Connector Auto-Update.

Procedure

1 Download the **AirWatch Cloud Connector x.x.x.x Installer.exe**.

   For more information, see Enable VMware AirWatch Cloud Connector from the Workspace ONE UEM console.

2 Run the installer again.

   For more information, see Run the VMware AirWatch Cloud Connector Installer.

Regenerate Certificates

You may find it necessary to regenerate the certificates used for Workspace ONE UEM and VMware AirWatch Cloud Connector 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 Workspace ONE UEM console, however it does require you to download and run the VMware AirWatch Cloud Connector 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, VMware AirWatch Cloud Connector 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.

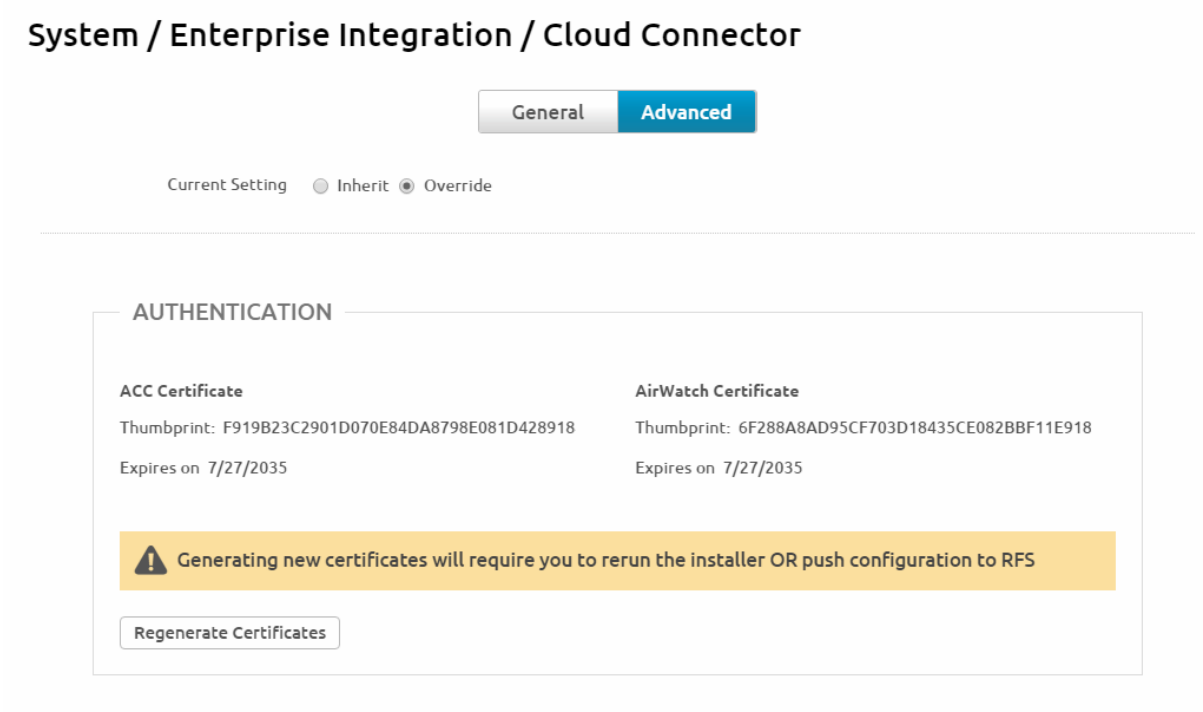
Perform these steps to regenerate certificates for Workspace ONE UEM and VMware AirWatch Cloud Connector servers.

Procedure

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

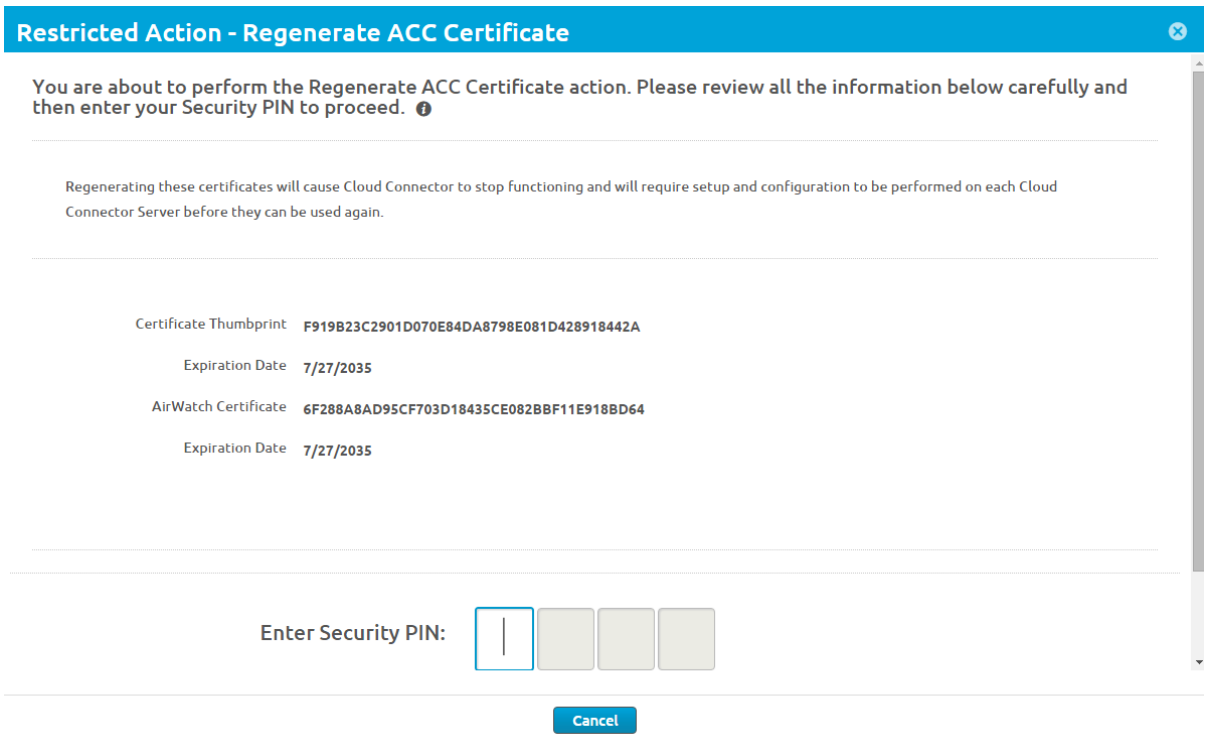
   Both certificates, their thumbprints, and expiration dates are shown on the **Advanced** tab.

2 Select **Regenerate Certificates** to generate a new certificate for the VMware AirWatch Cloud Connector and Workspace ONE UEM 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.



Results

When you enter your PIN to confirm, the VMware AirWatch Cloud Connector will no longer be able to communicate with the Workspace ONE UEMserver.

What to do next

To restore communications between VMware AirWatch Cloud Connector and the Workspace ONE UEM server, you need to return to Chapter 3 VMware AirWatch Cloud Connector Installation Process and complete all the steps again. This will allow both servers to recognize the latest certificate and regain communications.