AirWatch Cloud Messaging (AWCM)

VMware Workspace ONE UEM 1902

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 AirWatch Cloud Messaging (AWCM)

1

VMware AirWatch Cloud Messaging (AWCM) provides secure communication to your back-end systems in conjunction with the VMware AirWatch Cloud Connector (ACC). The ACC uses AWCM to securely communicate with the Workspace ONE UEM console.

AWCM also streamlines the delivery of messages and commands from the UEM console to devices by eliminating the need for end users to access the public Internet or utilize consumer accounts, such as Google IDs. AWCM serves as a comprehensive substitute for Google Cloud Messaging (GCM) or Firebase Cloud Messaging (FCM) for Android devices and is the only option for providing Mobile Device Management (MDM) capabilities for Windows Rugged devices.

Workspace ONE UEM configures AWCM in SaaS environments for customers who want to use it. If you are a SaaS customer, this documentation can help you understand how AWCM functions within your deployment, but you do not have to perform the configuration steps described here.

On-premises customers can use this guide to configure AWCM and Secure Channel.

Benefits

AWCM simplifies device management by offering the following benefits:

- Secure communication to your back-end infrastructure through the VMware AirWatch Cloud Connector.

- Real-time communication with Workspace ONE UEM Windows Protection Agent.

- Removing the need for third party IDs.

- Workspace ONE UEM console commands delivered directly to Android and Windows Rugged devices.

- Remote commands such as device wipe and device lock delivered to macOS devices.

- Increased functionality of internal Wi-fi only devices using push notifications in certain circumstances.

This chapter includes the following topics:

- AWCM Server Requirements

- AWCM Deployment Options

- Install AWCM

AWCM Server Requirements

To deploy VMware AirWatch Cloud Messaging, your system confiuration must meet certain requirements.

Hardware Requirements

The following hardware requirements are for dedicated AWCM servers.

- Minimum: Windows Server 2008 R2; Supported: Windows Server 2012 R2, Windows Server 2016

- 8GB of RAM

- 4-core CPU (minimum 2GHz)

AWCM is incorporated with the Workspace ONE UEM installer and you can install it:

- On the Device Services server.

- On a dedicated server.

- On a load-balanced server.

- On a cloud server.

- In a customer network with no access to the Internet.

Regardless of the deployment method, the device must have access to both AWCM and the Device Services server. Once the system is established on a server, an administrator creates a complete connection in the Workspace ONE UEM console.

If you install AWCM on the Device Services server, then reference the **VMware AirWatch Recommended Architecture Guide**, which contains hardware and sizing information when combining these components.

Software Requirements

The following software requirements are for the application server on which the AWCM is installed.

- 64-bit Java (Java Runtime Environment version 8).

    Note   The necessary version of Java is included with the Workspace ONE UEM Installer, and will install automatically during Workspace ONE UEM installation.

Network Requirements

- Devices must have access to both AWCM and the Device Services server, if they are not on the same application server.

- Devices must reach the AWCM server on port 2001 by default (configurable).

- The Workspace ONE UEM console, Device Services, API, and the Self-Service Portal must be configured to connect to your AWCM server on port 2001 by default (configurable).

  Note You can configure access to the AWCM server to be done over port 443, provided that AWCM is not on a server already using that port.

- VMware Tunnel and VMware AirWatch Cloud Connector must have access to the AWCM endpoint.

Load Balancing AWCM in an On-Premises Deployment

To deploy AWCM with multiple nodes behind a load balancer without clustering, you must account for persisting the connections to the AWCM servers. In the HTTP request that is sent to AWCM (from a device, the device services server, the console server, VMware AirWatch Cloud Connector, and so on), there is a cookie value called **awcmsessionid**, which is used to establish request level affinity to an AWCM node from a pool of nodes. You must configure your load balancer or proxy to parse the HTTP request for this value and use it for persistence.

For more information on how to achieve this on an F5 LTM, see the following Workspace ONE Knowledge Base article: https://support.workspaceone.com/articles/115001666028.

AWCM Deployment Options

You can deploy the AWCM in four modes, depending on the resources and requirements unique to your deployment.

1 Single Instance

   A single AWCM server processes all requests.

   This is the simplest configuration, but it has no redundancy in case of server failure.

2 Two Instances (Active-Passive Servers)

   Both servers (an active primary server and a passive secondary server) run behind a load balancer. The load balancer periodically checks the health of the primary and secondary servers. If the primary server is down, the load balancer switches all the requests to the secondary server until the primary is back online.

   The Active-Passive Server setup ensures that high availability is maintained when the number of network requests is of no concern.

   This setup is best for on-premises customers using ACC with AWCM who do not use AWCM for device-specific communication.

3 Horizontal Scaling with Multiple Instances (Active-Active Servers with Implicit Clustering)

Multiple AWCM servers run behind a load balancer and communicate with clients using session persistence (using the awcmsessionid cookie).

This setup is best if balancing network traffic from multiple clients is more important than high availability. This is also the optimal solution for horizontal scalability.

For more information, see the following Workspace ONE UEM Knowledge Base article: https://support.workspaceone.com/articles/115001666028.

4   Multiple Instances (Active – Active Servers, With Explicit Clustering)

Multiple AWCM instances are active behind a load balancer. These servers establish a cluster by means of TCP communication using the default port 5701 within your internal LAN.

The caveat with this deployment option is increased performance overhead resulting from inter-node communication to maintain a single view of in-memory data.

Install AWCM

The installation files for AirWatch Cloud Messaging are included in the installation procedure for VMware Workspace ONE UEM. AWCM should only be included in your installation of Workspace ONE UEM in certain configurations.

The AWCM component is not downloaded from the Workspace ONE UEM console like other enterprise integration components. In addition, SaaS customers who want to use AWCM should contact Workspace ONE UEM to configure it for your environment.

On-premises customers should follow the installation instructions included in the VMware Workspace ONE UEM Installation documentation, available at docs.vmware.com. It includes information about installing AWCM if you select **AirWatch Cloud Messaging** when configuring the Workspace ONE UEM Features on the application server where you want to install AWCM. Most deployments typically use the Devices Services server.

AWCM Configuration

2

Once AirWatch Configuration Manager is installed, configure your setup to meet your deployment needs.

The topics in this section cover configuring AWCM after it has been installed alongside the VMware AirWatch Cloud Connector as part of your Workspace ONE UEM deployment.

This chapter includes the following topics:

- Install Secure Channel Certificate on AWCM (On-Premises Deployments)
- Establish Communications with AWCM
- Enable AWCM to Communicate with Devices
- Upgrade AWCM
- Renew SSL Certificate for AWCM

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.

Setting	Description
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 AWCM to Communicate with Devices

Certain platforms require you to enable AWCM as the push notification service of choice when communicating with Android devices.

Procedure

1   Navigate to **Groups & Settings > All Settings > Device & Users > Android > Intelligent Hub Settings** and scroll down to the **AirWatch Cloud Messaging** section.

2   Select the **Use AWCM Instead of C2DM/GCM as Push Notification Service** check box to enable AWCM in the profile.

The **AWCM Client Deployment Type** drop-down menu is automatically changed to **Always Running** and can no longer be modified.

Upgrade AWCM

For SaaS Customers: AWCM is automatically updated.

For On-premises Customers: When a new version of AWCM is available, it will install automatically when you perform a Workspace ONE UEM upgrade if you have **AirWatch Cloud Messaging (AWCM)** selected as a component on the **Workspace ONE UEM Features** screen.

Renew SSL Certificate for AWCM

If you are an on-premises customer and you install AWCM with an SSL certificate, then you must update AWCM when that certificate expires to maintain functionality.

Procedure

1   Obtain the full chain (.pfx or .p12) of your renewed SSL certificate.

2   If your AWCM is shared with other AirWatch components, then on the server where they are all installed, navigate to Programs and Features (Add/Remove Programs), locate AirWatch, and select **Change**.

3   Then select **Add/Remove AirWatch features**.

4   If you installed AWCM on a standalone server, complete the required steps.

   a   Obtain the full AirWatch installer that corresponds to the current AirWatch version your environment is running and copy it to the server AWCM is on. If you kept your last-used installer, you can use it. Otherwise, contact AirWatch to receive the installer for your specific AirWatch version.

   b   Run the installer on the server where AWCM is installed.

Important   Depending on which components are installed on your server with AWCM, you could experience disruptions in service or functionality during the re-installation process. Refer to the Workspace ONE UEM Upgrade Guide for more details on stopping and restarting services.

5   During installation, on the AirWatch Features screen, right-click **AirWatch Cloud Messaging** and select **This feature will not be available.**

6   If your AWCM is shared with other AirWatch components, then once again navigate to Programs and Features and select **Change** for the AirWatch application. Then select **Add/Remove AirWatch features**.

7   If your AWCM is installed as a standalone server, then run the installer again.

8   On the AirWatch Features screen, right-click **AirWatch Cloud Messaging** and select **This feature will be installed on the local hard drive.** Proceed with the installation until you reach the AWCM server settings screen with the **Use custom SSL certificate?** check box.

9   Browse to the location of the full chain (.pfx or .p12) of your renewed SSL certificate.

10   Enter the certificate password and select **Next**.