

VMware AirWatch Cloud Messaging Guide

Configuring AirWatch Cloud Messaging for an on-premises deployment

Workspace ONE UEM v9.7

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Overview	3
Introduction to AWCM	4
Requirements	4
AWCM Deployment Options	6
Chapter 2: AWCM Installation	7
AWCM Installation Overview	8
Chapter 3: AWCM Configuration	9
AWCM Configuration Overview	10
Install Secure Channel Certificate on AWCM (On-Premises Deployments)	10
Establish Communications with AWCM	10
Enable AWCM to Communicate with Devices	11
Start and Stop AWCM	12
Upgrade AWCM	12
Renew SSL Certificate for AWCM	13
Accessing Other Documents	15

Chapter 1:

Overview

Introduction to AWCM4

Requirements4

AWCM Deployment Options6

Introduction to AWCM

AirWatch Cloud Messaging (AWCM) is used in conjunction with the VMware Enterprise Systems Connector to provide secure communication to your back-end systems. VMware Enterprise Systems Connector uses AWCM to communicate with the Workspace ONE UEM console.

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

AirWatch configures AWCM in SaaS environments for customers who want to use it. If you are a SaaS customer, then you can read this guide to learn more about AWCM, but know that you do not have to perform the configuration steps within.

On-premises customers can use this guide to configure AWCM and Secure Channel. Since AWCM installation occurs during AirWatch application server installation, you can find the installation steps for AWCM in the VMware AirWatch Installation Guide (VMware provides this documentation to you as part of the on-premises installation process).

Benefits

AWCM simplifies device management by offering the following benefits:

- Enabling secure communication to your back-end infrastructure through the VMware Enterprise Systems Connector.
- Enabling Workspace ONE UEM Windows Protection Agent real-time communication.
- Removing the need for third party IDs.
- Delivering Workspace ONE UEM console commands directly to Android and Windows Rugged devices.
- Enabling the ability for remote control and file management on Android Samsung Approved for Enterprise (SAFE) and Windows Rugged devices.
- Enabling the ability to send remote commands such as device wipe and device lock to macOS and Windows 7 devices.
- Increasing the functionality of internal Wi-Fi only devices by enabling push notification in certain circumstances.

Requirements

Each AWCM server requires the following minimum requirements:

Hardware Requirements

The following hardware requirements are for dedicated AWCM servers.

- Windows 2008, or any macOS with Java Virtual Machine (JVM)
- 4GB of RAM
- Dual-core Processor

AWCM is incorporated with the AirWatch installer and you can install it on the following systems:

- On the same server as the AirWatch Console.
- On the Device Services server.
- On a dedicated server.
- On a load-balanced server.
- On a cloud server.
- In a customer's 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 AirWatch Console.

If you're installing AWCM on the Device Services server, then please see the **VMware AirWatch Recommended Architecture Guide**, [available on AirWatch Resources](#), which contains hardware and sizing information when combining these components.

Software Requirements

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

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

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 AirWatch 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 Enterprise Systems 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 Enterprise Systems Connector, and so on), there is a cookie value called **awcm-sessionid**, 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 AirWatch Knowledge Base article: <https://support.air-watch.com/articles/115001666028>.

AWCM Deployment Options

You can deploy the AWCM in four modes. In most cases the Two Instances (Active – Passive Servers) mode is the preferred method. The following is a list of the four available modes and a description of each.

1. Single Instance

Single AWCM server processes all requests. This is the simplest configuration.

2. Two Instances (Active – Passive Servers) *Preferred Deployment*

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 deemed as down, the load balancer switches all the requests to the secondary server until the primary is back online.

This method ensures that high availability is maintained, but the amount of network requests is of no concern. This is preferred for the on-premises customer that is only using Cloud Connector with AWCM and is not requiring AWCM for device-specific functionality (remote control, file manager, GCM replacement, etc).

3. Horizontal Scaling with Multiple Instances (Active – Active Servers, With Implicit Clustering)

AWCM server instances with clients (device agents, console, remote control and the VMware Enterprise Systems Connector, VMware Enterprise Systems Connector) using session persistence (via the awcmsessionid cookie) on a load balancer, which is the optimal solution for horizontal scalability. Multiple AWCM servers run behind a load balancer. Unlike the “active-passive” deployment above, this method is preferred when network traffic becomes a concern with balancing connections from multiple clients (devices, VMware Enterprise Systems Connector, VMware Tunnel) is more important than just high availability.



For more information, see the following AirWatch Knowledge Base article: <https://support.air-watch.com/articles/115001666028>.

AirWatch supports session persistence. VMware Enterprise Systems Connector and remote control provide the session persistence option.

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 performance overhead resulting from inter-node communication to maintain a single view of in-memory data.

Remote control is not supported in this configuration as it requires persistence on the load balancer.



For customers upgrading from AWCM 4.x to AWCM 6.x and wanting to use explicit clustering, please refer to the following KB article: <https://support.air-watch.com/articles/115001665788>.

Chapter 2:

AWCM Installation

AWCM Installation Overview	8
----------------------------------	---

AWCM Installation Overview

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

On-premises customers should follow the installation instructions included in the VMware AirWatch Installation Guide (VMware provides this documentation to you as part of the on-premises installation process). It includes information about installing AWCM if you select **AirWatch Cloud Messaging** when configuring the AirWatch Features on the application server – Console or Device Services – where you want to install AWCM. Most deployments typically use the Devices Services server.

Chapter 3:

AWCM Configuration

AWCM Configuration Overview	10
Install Secure Channel Certificate on AWCM (On-Premises Deployments)	10
Establish Communications with AWCM	10
Enable AWCM to Communicate with Devices	11
Start and Stop AWCM	12
Upgrade AWCM	12
Renew SSL Certificate for AWCM	13

AWCM Configuration Overview

Installation of a **Secure Channel Certificate** on a local AWCN server is for on-premises customers only. Installing the **Secure Channel Certificate** on your local AWCN server establishes security between the AirWatch Console and AWCN. Perform the installation steps on the server running AWCN. Do not download the installation program onto another computer and copy it to the AWCN server. If the download fails on the server running AWCN, then contact Workspace ONE Support for potential workarounds.

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

On-premises customers must install a Secure Channel Certificate to establish security between the AWCN and the following components: AirWatch 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 AWCN server.

Important: Perform the following steps on the server running AWCN. If your AWCN 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 AWCN server. If the download fails on the server running AWCN, then contact Workspace ONE Support for potential workarounds.

1. Navigate to **Groups & Settings > All Settings > System > Advanced > Secure Channel Certificate**.
2. Select **Download AWCN 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. AWCN is only supported on Windows servers.
3. Copy the **Secure Channel Certificate** install script to your local AWCN 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 AWCN](#).
7. Proceed with the installation steps for VMware AirWatch Cloud Connector in the **VMware Enterprise Systems Connector Guide**, available at <https://docs.vmware.com/en/VMware-Identity-Manager/index.html>.

If you make any changes to the Secure Channel Certificate in the AWCN 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 AWCN

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

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 AWCN server.
AirWatch 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 AWCN. 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.
AirWatch External Port	This is the port that is being used by the servername above to communicate with AWCN. 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.
AWCN Server Internal URL	This URL allows you to reach AWCN 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 AWCN 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.

Enable AWCN to Communicate with Devices

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

Android Devices

1. Navigate to **Groups & Settings > All Settings > Device & Users > Android > Agent Settings** and scroll down to the AirWatch Cloud Messaging section.
2. Select the **Use AWCN Instead of C2DM as Push Notification Service** check box to enable AWCN in the profile.

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

Symbian Devices

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Symbian > Agent Settings**.
2. Select the **Use AWCN** check box to enable AWCN in the profile.

Note: You do not need to configure additional settings for Windows Rugged devices, macOS or Windows 7 devices.

Start and Stop AWCN

You can start or stop AWCN on individual devices on-demand.

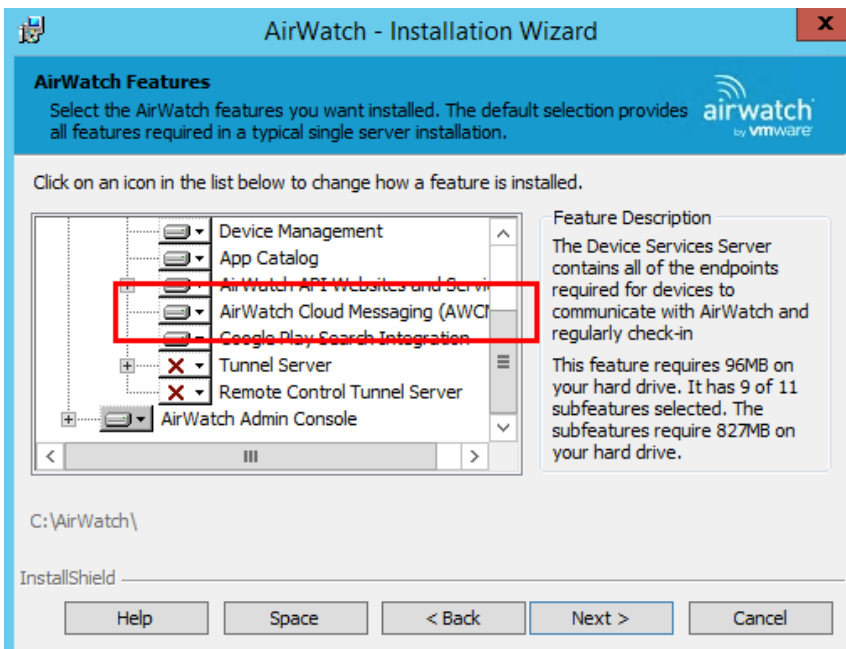
1. Select the device **Friendly Name** from the AirWatch Console **Devices > List View** to launch the device Details View page.
2. Select the **More** drop-down menu to view available device commands.
3. Under **Advanced**, select either **Start AWCN** or **Stop AWCN**.

You can now provision the AWCN-enabled Android, Windows Rugged, macOS, Windows 7 and Symbian profiles to your devices and take advantage of AirWatch's MDM tools and features.


Upgrade AWCN

For SaaS Customers: AWCN is automatically updated.

For On-premises Customers: When a new version of AWCN is available, it will install automatically when you perform an AirWatch upgrade if you have AWCN selected as a component on the **AirWatch Features** screen, as shown below:



See the VMware AirWatch Upgrade Guide (available to partners and existing customers at: <https://resources.air-watch.com/view/xm92c772sbl39zg658k9>) for more information on this process.

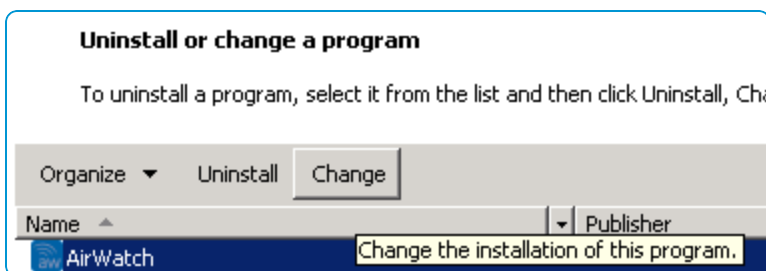
 For customers upgrading from AWCN 4.x to AWCN 6.x and wanting to use explicit clustering, please refer to the following KB article: <https://support.air-watch.com/articles/115001665788>.

Renew SSL Certificate for AWCN

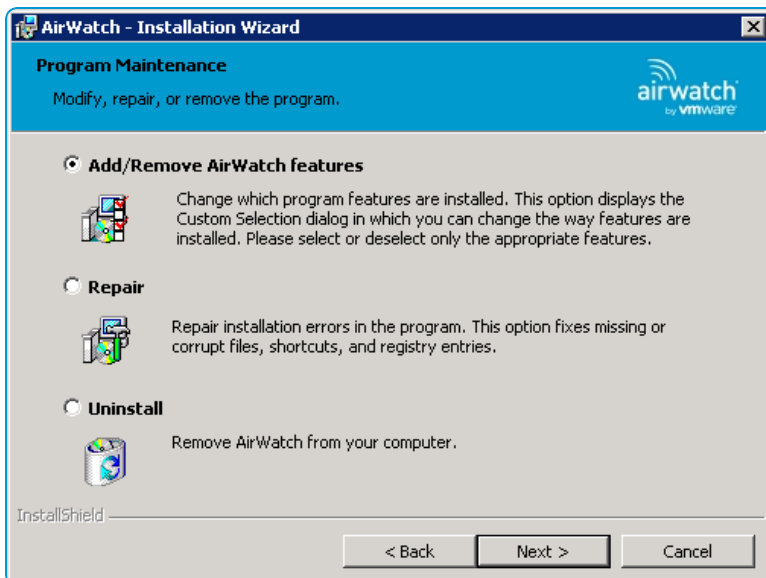
If you are an on-premises customer and you install AWCN with an SSL certificate, then you must update AWCN when that certificate expires to maintain functionality.

Use the following steps to perform this task:

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



Then select **Add/Remove AirWatch features** and proceed to step 4.



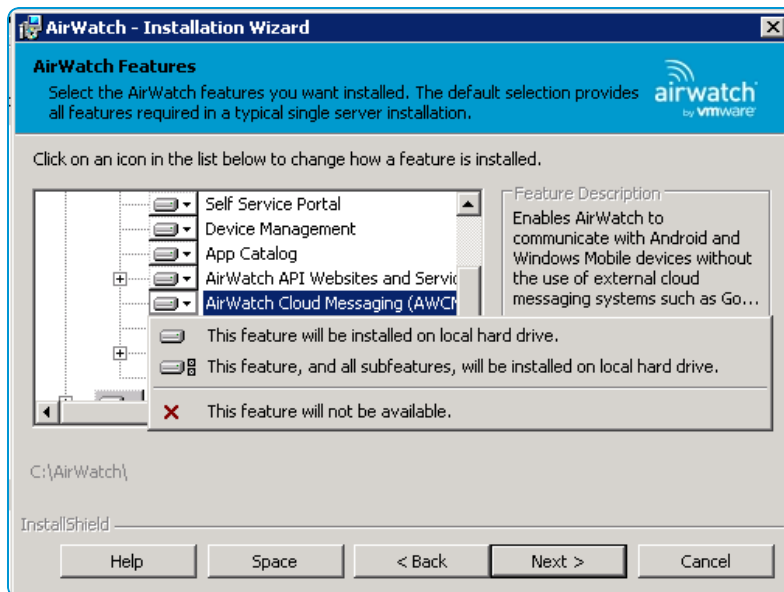
3. If you installed AWCN on a standalone server, then:
 - a. Obtain the full AirWatch installer that corresponds to the current AirWatch version your environment is running and copy it to the server AWCN is on. If you kept your last-used installer, you can use it. Otherwise, contact

AirWatch to receive the installer for your specific AirWatch version.

- b. Run the installer on the server where AWCN is installed.

Important: Depending on which components are installed on your server with AWCN, you could experience disruptions in service or functionality during the re-installation process. Refer to the VMware AirWatch Upgrade Guide (available to partners and existing customers at: <https://resources.air-watch.com/view/xm92c772sbl39zg658k9>) for more details on stopping and restarting services.

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



Proceed with the remainder of the installation to completion.

5. If your AWCN 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** and proceed to step 7.
6. If your AWCN is installed as a standalone server, then run the installer again.
7. 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 AWCN server settings screen with the **Use custom SSL certificate?** check box.
8. Browse to the location of the full chain (.pfx or .p12) of your renewed SSL certificate.
9. Enter the certificate password and select **Next**. Proceed with the remainder of the installation to completion.

You can find additional information about running the AirWatch installer and the specific AWCN options you can configure during installation in the VMware AirWatch Installation Guide (VMware provides this documentation to you as part of the on-premises installation process).

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to docs.vmware.com and search for the document you need. Each release-specific document has a link to its PDF copy on myAirWatch.

Alternatively, you can navigate directly to myAirWatch (resources.air-watch.com) and execute a search. When searching for documentation on myAirWatch, be sure to select your Workspace ONE UEM version. You can use the filters to sort by PDF file type and Workspace ONE UEM v9.7.