Introduction to the AirWatch Cloud Connector (ACC) Guide

The AirWatch Cloud Connector (ACC) provides organizations the ability to integrate AirWatch with their back-end enterprise systems. This document describes setting up ACC for a SaaS deployment, which is when certain AirWatch components, including the ACC, are hosted in the cloud.

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. For a diagram that illustrates this refer to ACC Deployment Model.

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-premise only)

In This Guide

- Before You Begin – This section covers topics and prerequisites you should familiarize yourself with so you can get the most out of using this guide.
- Architecture & Security – This section lets you see the basic architecture type for your deployment.
- Prerequisites for ACC Connectivity in SaaS Environments – This section details all of the prerequisites for running ACC in a SaaS environment.
- ACC Installation – This section details the installation process for the ACC and how to enable it in the AirWatch Admin Console.
- EIS to ACC Migration– This section provides instructions on how to migrate from the legacy EIS to ACC.
- Appendix A – Upgrading ACC – This section gives instructions on how to upgrade the ACC from a previous version and how to set up automatic updates.
- Appendix B – Regenerating Certificates – This section tells you how to regenerate certificates for the ACC.

Before You Begin

Overview

Before configuring the AirWatch Cloud Connector (ACC), you should consider the following prerequisites, requirements, supporting materials, and helpful suggestions from the AirWatch team. Familiarizing yourself with the information available in this section will help prepare you for configuring the ACC.

- Requirements

For a complete listing of all requirements for installing ACC in a SaaS environment, refer to the Prerequisites for ACC Connectivity in SaaS Environments.

Prerequisites for ACC Connectivity in SaaS Environments

Status Checklist	Requirement	Notes	
Hardware Requirements			
	VM or Physical Server	1 CPU Core (2.0+ GHz) 2 GB RAM or higher 1 GB disk space for the ACC application, Windows OS, and .NET runtime. If logging is being done, then it is recommended you have an additional 5 GB of disk space.	

Sizing for up to 200,000 Users

Note: ACC traffic is automatically load-balanced by the AWCM component – it does not require a separate load balancer. To accommodate additional users as part of your sizing requirements you can deploy multiple ACCs, which will all be load balanced by AWCM.

Number of Users	Up to 10,000	10,000 to 50,000	50,000 to 100,000	100,000 to 200,000
CPU Cores	2	2 load-balanced servers with 2 CPU Cores	2 to 3 load-balanced servers with 2 CPU Cores	2 load-balanced servers with 4 CPU Cores
RAM (GB) Per Server	4	4	8	16

Status Checklist	Requirement	Notes
General Requirements		
	Remote access to Windows Servers available to AirWatch and Administrator rights	Recommended to setup Remote Desktop Connection Manager for multiple server management, installer can be downloaded from http://www.microsoft.com/en-us/download/confirmation.aspx?id=21101 See **General Requirements.**
	Installation of Notepad++ (Recommended)	Installer can be downloaded from http://download.tuxfamily.org/notepadplus/6.5.1/npp.6.5.1.Installer.exe
	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.
Software Requirements		
	Windows Server 2008 R2 or Windows Server 2012 or Windows Server 2012 R2	
	Install PowerShell on the	Optional

Status Checklist	Requirement	Notes	
	server		
	Install .NET Framework 4.0	Download from http://www.microsoft.com/en-us/download/confirmation.aspx?id=17718	

	Source Component	Destination Component	Protocol	Port	Verification
Network Requirements					
	ACC Server	AirWatch SaaS 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.) If auto-update is enabled, ACC must be able to query AirWatch Admin Console for updates using port 443.
	ACC Server	AirWatch Admin 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.)
	ACC Server (OPTIONAL)	Internal SMTP	SMTP	25	
	ACC Server (OPTIONAL)	Internal LDAP	LDAP or LDAPS	389, 636, 3268, or 3269	
	ACC Server (OPTIONAL)	Internal SCEP	HTTP or HTTPS	80 or 443	
	ACC Server (OPTIONAL)	Internal ADCS	DCOM	135, 1025-5000, 49152-65535	
	ACC Server (OPTIONAL)	Internal BES	HTTP or HTTPS	80 or 443	

	Source Component	Destination Component	Protocol	Port	Verification
	ACC Server (OPTIONAL)	Internal Exchange 2010 or higher	HTTP or HTTPS	80 or 443	

*

Note: An outbound proxy or any other connection management software or hardware must not terminate or reject the outbound connection from the ACC. In other words, the outbound connection required for use by ACC must remain open at all times.

General Requirements

Remote Access to Servers

Ensure that you have remote access to the servers that AirWatch is installed on.

Architecture & Security

Overview

The AirWatch Cloud Connector (ACC) is a Windows service that can be installed on a physical or virtual server running 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 ACC to the AirWatch Cloud Messaging Service (AWCM), ACC can periodically transmit information from your internal resources such as AD, LDAP, etc. to the AirWatch Admin Console without any firewall changes. If you plan on proxying ACC traffic through an outbound proxy, then there are settings in ACC that will allow for proxying (see Proxy Information).

In This Section

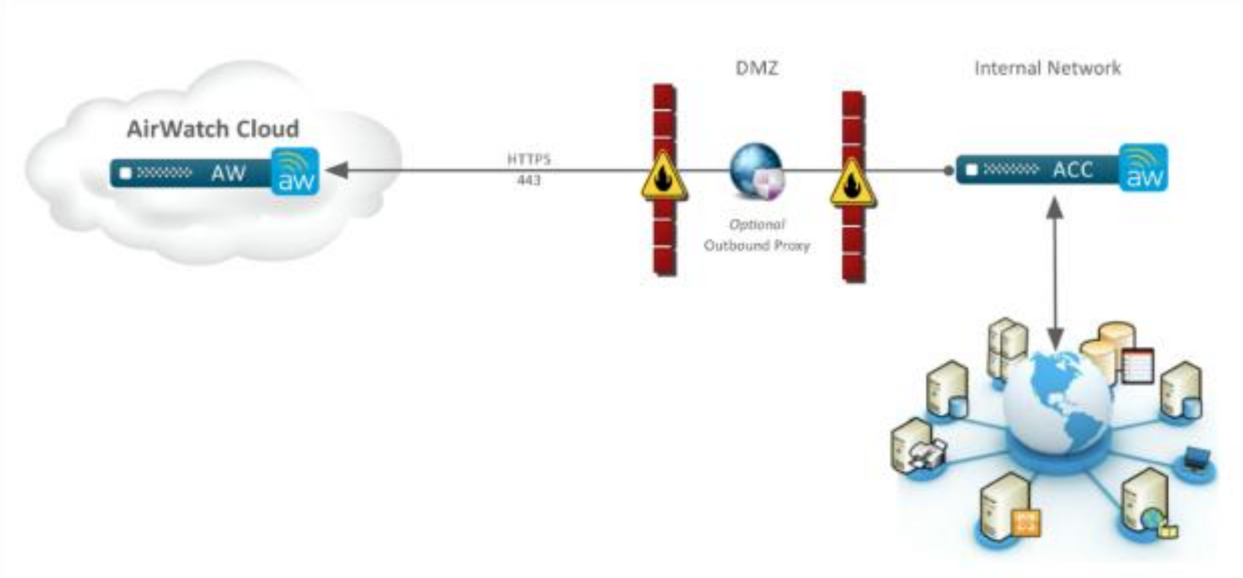
- Supported Configurations – See the supported configurations for the ACC.
- ACC SaaS Deployment Model – See a SaaS deployment model for ACC.

Supported Configurations

Use ACC in the following configurations:

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

ACC SaaS Deployment Model



ACC Installation

Overview

Install the AirWatch Cloud Connector (ACC) by first enabling it in the AirWatch Admin Console and then downloading and running the installer executable file onto the server that will host the service. Installing the ACC includes the following tasks:

- Enabling the use of ACC in the AirWatch Admin Console.
- Generating certificates for the AirWatch server and ACC.
- Configuring the ACC to communicate with the Enterprise and AirWatch services.
- Downloading the ACC installer and installing it.
- Verifying the installation was successful and communications have been established between the AirWatch server to AWCM and the AWCM to ACC.

In This Section

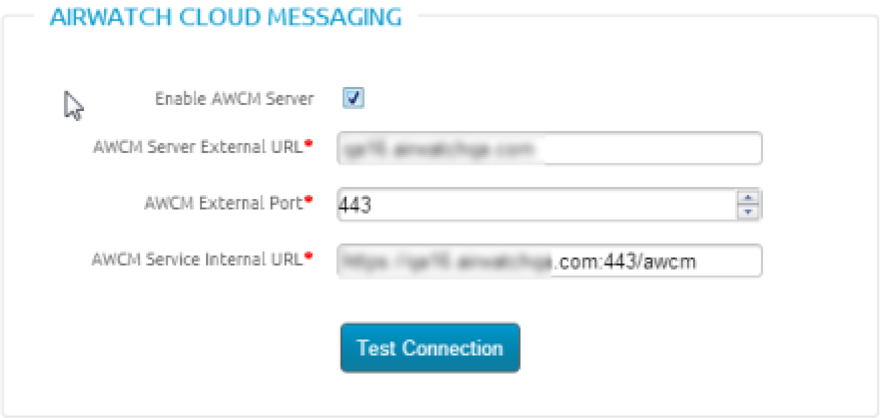
- Enabling ACC from the AirWatch Admin Console – Enable and configure ACC settings that apply to your deployment.
- Running the ACC Installer – Follow these step-by-step instructions by running the installer on the server that will host ACC.
- Verifying a successful ACC installation – Verify ACC is installed correctly and communicating with AWCM.

Establishing Communications with AWCM

The following steps apply to both SaaS and on-premise deployments. Establishing communications with AWCM allows you to configure an AirWatch instance to use a particular AWCM 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.



AIRWATCH CLOUD MESSAGING

Enable AWCM Server ☑

AWCM Server External URL* [redacted]

AWCM External Port* 443

AWCM Service Internal URL* [redacted].com:443/awcm

2. Select the **Enable AWCM Server** check box. This allows the connection between the AirWatch Admin Console and the AWCM server.

3. Enter the **AWCM Server External URL** in the field. This field allows you to enter the servername used by external components and devices (e.g., ACC) to securely (via HTTPS) communicate with AWCM. An example of an ACC URL is: Acme.com.

   Note: Do not add https:// since this is assumed by the application and automatically added.

4. Enter the port in the **AWCM External Port** field. This is the port that is being used by the servername above to communicate with AWCM.

   Note: 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.

5. Enter the **AWCM Server Internal URL** in the field. 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.

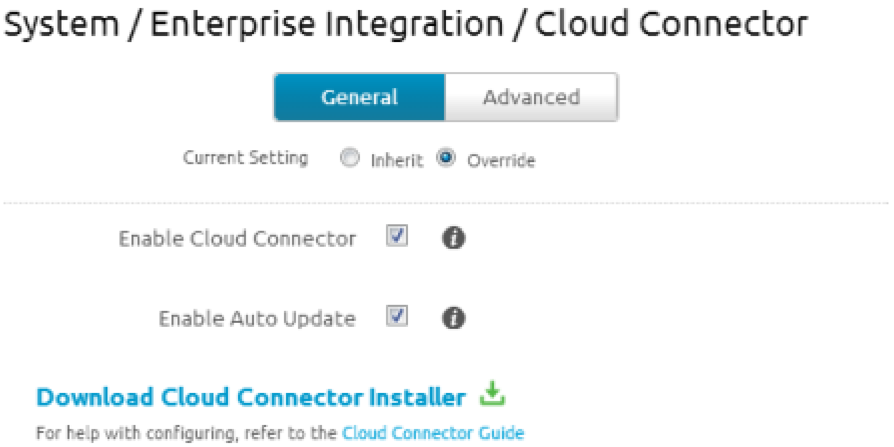
   Note: If your AWCM server and AirWatch Admin Console are internal (within the same network), and you want to bypass offloaded SSL, there is no need for a secure connection, so you can use http instead of https. For example, http://AcmeInternal.Local:2001/awcm. This example shows the server resides within the internal network and is communicating on port 2001.

Enabling ACC from the AirWatch Admin Console

Prepare for the installation by enabling ACC, generating certificates, and selecting enterprise services and AirWatch services by performing the following steps.

Note: Perform the following steps on the server running ACC. Do not download the installation program onto another computer and copy it to the ACC server.

1. Navigate to **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Cloud Connector**.
2. Select the **Enable Cloud Connector** checkbox to enable ACC and display the **General** tab.



System / Enterprise Integration / Cloud Connector

Current Setting ○ Inherit ● Override

Enable Cloud Connector ☑

Enable Auto Update ☑

Download Cloud Connector Installer

For help with configuring, refer to the Cloud Connector Guide

3. Enable ACC to automatically update when a newer version is available. If you want more information regarding auto-update, refer to ACC Auto-Update Option.
4. Select the **Advanced** tab, then select the **Generate Certificates** button to generate a certificate for the ACC and AirWatch server. Certificates are generated for both and displayed under ACC and AirWatch certificates.

   Note: Once certificates are generated, the button changes to **Regenerate Certificates**. For more information about Regenerating Certificates, refer to Appendix B - Regenerating Certificates.

5. Select each checkbox to enable or disable **Enterprise Services**. The services you select (enabled) will integrate with ACC.

   - SMTP (Email Relay)

   Note: AirWatch SaaS offers email delivery through its own SMTP, but you can enable ACC to use another SMTP server here. Enter SMTP servers settings for email in **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Email (SMTP).**

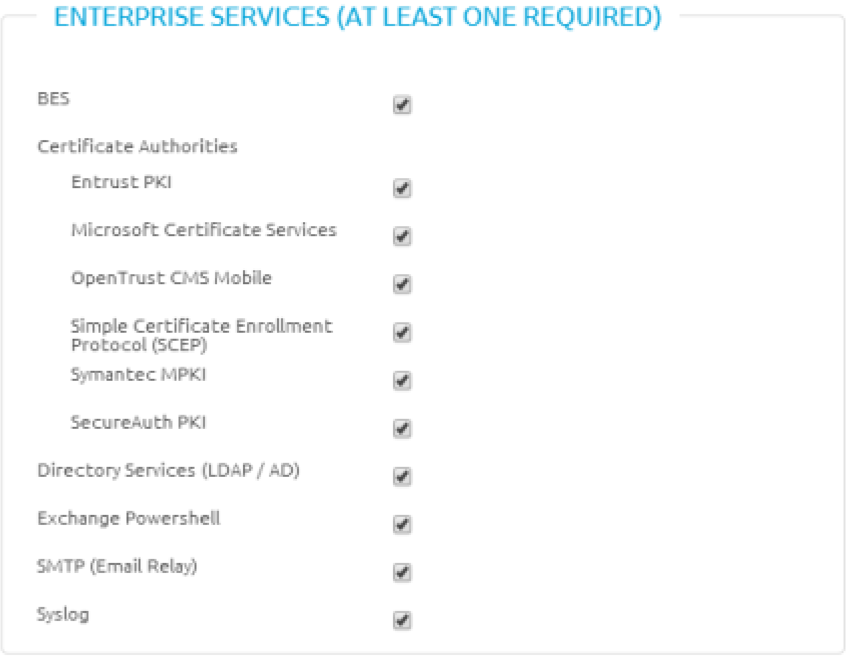
   - Directory Services (LDAP/AD)
   - Exchange PowerShell (for certain Secure Email Gateways)
   - BES (BlackBerry sync user and mobile device information)
   - Syslog (Client/server protocol used to integrate with the AirWatch event log data)

   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)

> **Note:** Since there is no need to go through ACC 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-premise, not in the cloud (SaaS).



ENTERPRISE SERVICES (AT LEAST ONE REQUIRED)

BES ☑

Certificate Authorities

Entrust PKI ☑

Microsoft Certificate Services ☑

OpenTrust CMS Mobile ☑

Simple Certificate Enrollment Protocol (SCEP) ☑

Symantec MPKI ☑

SecureAuth PKI ☑

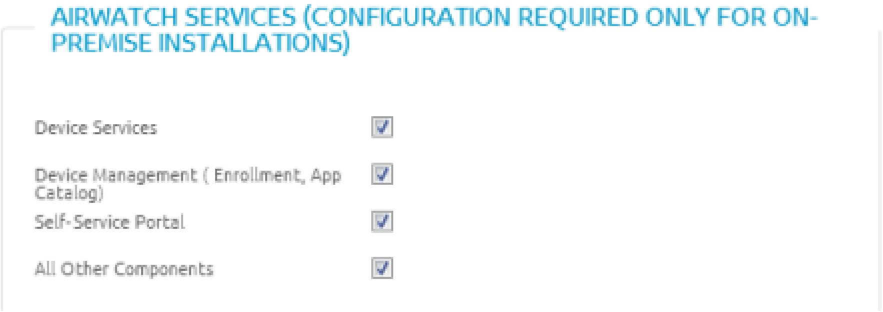
Directory Services (LDAP / AD) ☑

Exchange Powershell ☑

SMTP (Email Relay) ☑

Syslog ☑

6. Select each checkbox to enable or disable **AirWatch Services**. The AirWatch components you select (enabled) will integrate with ACC.
    - 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)



AIRWATCH SERVICES (CONFIGURATION REQUIRED ONLY FOR ON-PREMISE INSTALLATIONS)

Device Services ☑

Device Management (Enrollment, App Catalog) ☑

Self-Service Portal ☑

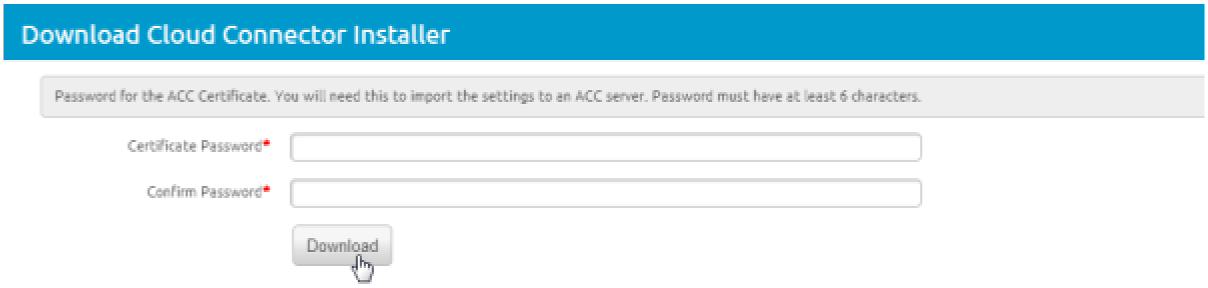
All Other Components ☑

> **Note:** AirWatch recommends leaving all services enabled.

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

8. Select **Download Cloud Connector Installer** located near the bottom of screen on the **General** tab.

9. A **Download Cloud Connector Installer** screen displays. Enter a password for the ACC certificate in the fields. The password will be needed later when you run the ACC installer and need to enter the certificate password.



Download Cloud Connector Installer

Password for the ACC Certificate. You will need this to import the settings to an ACC server. Password must have at least 6 characters.

Certificate Password*

Confirm Password*

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

Running the ACC Installer

Perform the following steps to install the ACC.

Note: SaaS customers should ensure the server you are installing ACC 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.) 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 properly function.

1. Open the installer on the ACC server. When the **Welcome** screen appears select **Next**.

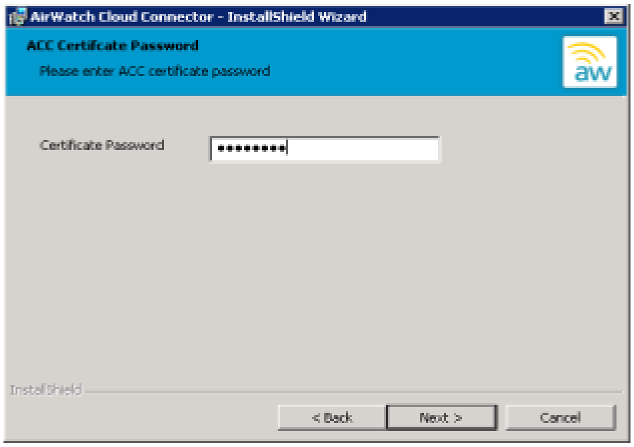
   Note: The installer verifies prerequisites on your ACC server.

   Note: If a previous version of EIS is installed, the installer auto-detects EIS and gives you the option of migrating all EIS settings to ACC. For more information on migrating, see EIS to ACC Migration. 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 Appendix A - Upgrading ACC.

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 AirWatch. Select **Next**.



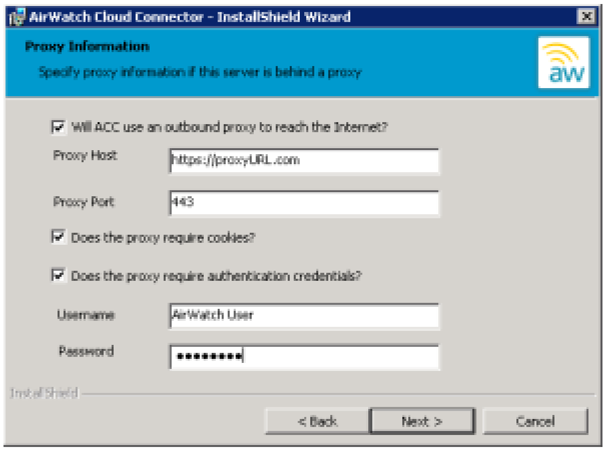
AirWatch Cloud Connector - InstallShield Wizard

ACC Certificate Password

Please enter ACC certificate password

Certificate Password: ●●●●●●●●●

5. If you plan on proxying ACC 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**.



AirWatch Cloud Connector - InstallShield Wizard

Proxy Information

Specify proxy information if this server is behind a proxy

☑ Will ACC use an outbound proxy to reach the Internet?

Proxy Host: https://proxyURL.com

Proxy Port: 443

☑ Does the proxy require cookies?

☑ Does the proxy require authentication credentials?

Username: AirWatch User

Password: •••••••••

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

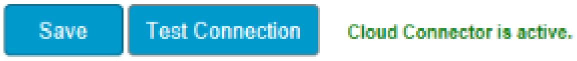
Note: The installer displays a checkbox for auto-updating ACC. For more information on auto-update, see the ACC Auto-Update Option.

7. Select **Finish**.

Verifying a Successful ACC Installation

Perform the following steps to verify that the ACC installation was successful.

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:

   Cloud Connector is active.

   If a message displays saying AirWatch cannot communicate with AWCM, then this is not an ACC issue. This is an AWCM issue, and you should consult with your AirWatch representative .

   If a message displays saying AirWatch can communicate with AWCM but ACC is not responding, then this is an issue with ACC. It probably means there is a certificate issue with ACC, or ACC cannot reach the AWCM server. You could try regnerating the ACC certificate, uninstalling ACC, deleting all ACC folders, re-downloading ACC, and re-installing it.

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

Integrating with your Directory Service

Now that you have successfully installed ACC, you can use it to integrate with your directory service infrastructure. Details for doing so are fully detailed in the **AirWatch Directory Services Guide**,.

EIS to ACC Migration

Overview

The AirWatch Enterprise Integration Service (EIS) has been divided into two products – AirWatch Cloud Connector (ACC) and Mobile Access Gateway (MAG). There are many benefits with the architecture of these new products and simplicity of integrating them into your enterprise. Both products can be used separately, yet complement each other when used together, but neither can be used with EIS. AirWatch will continue to support the existing functionality of EIS in future releases of the AirWatch Admin Console, although, customers who are planning on utilizing any of our latest integration features such as the MAG will need to migrate to ACC.

In This Section

- Prior to Migrating from EIS to ACC – SaaS customers should follow these steps before attempting to migrate from EIS to ACC.
- Migrating Procedure – Follow these instructions to perform the migration process.

Prior to Migrating from EIS to ACC

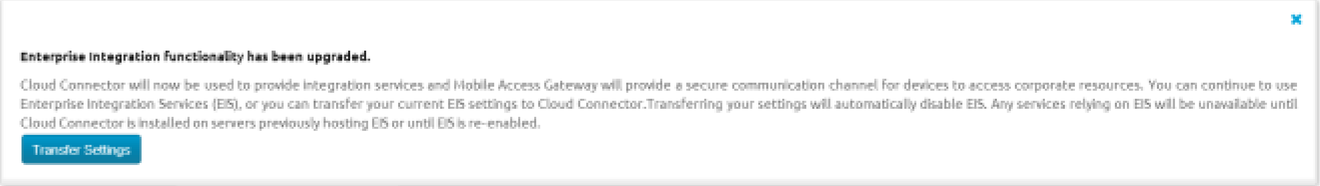
Before you begin, you need to inform your AirWatch representative that you want to migrate from EIS to ACC. Your representative must configure AWCM in our SaaS environment so when you install ACC, it can establish communications with AWCM.

Also, you need to install the MAG. Since ACC and MAG replace EIS, you must also install MAG to preserve the same functionality provided by EIS. MAG must be installed prior to ACC. For more information, refer to the **Mobile Access Gateway Guide**.

Migrating Procedure

To enable migration from the EIS to ACC:

1. Navigate to **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Enterprise Integration Services**. The following message displays at the top of the screen:



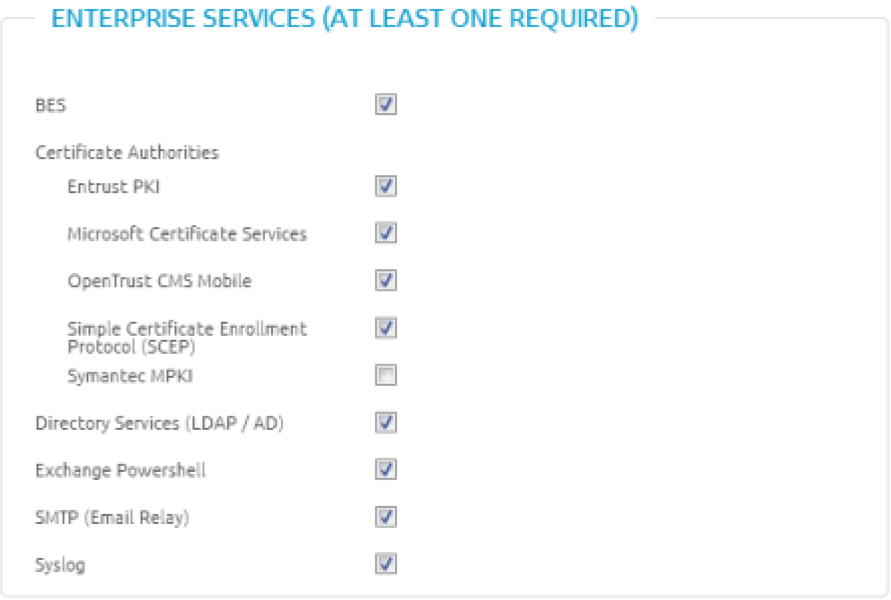
Enterprise Integration functionality has been upgraded.

Cloud Connector will now be used to provide integration services and Mobile Access Gateway will provide a secure communication channel for devices to access corporate resources. You can continue to use Enterprise Integration Services (EIS), or you can transfer your current EIS settings to Cloud Connector.Transferring your settings will automatically disable EIS. Any services relying on EIS will be unavailable until Cloud Connector is installed on servers previously hosting EIS or until EIS is re-enabled.

2. Read the disclaimer regarding ACC replacing EIS and select **Transfer Settings**.

Note: While EIS is migrating to ACC, your AirWatch server will not be able to connect to any external systems such as AD, CAs, etc. All devices will continue to check into AirWatch, and other MDM functionality will remain operational, as expected. Please prepare for this downtime. The ACC migration process should only take less than 30 minutes.

3. Navigate to **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Cloud Connector**. All EIS setting should have been transferred to ACC.
4. Select **Generate Certificates**. The **Download Cloud Connector Installer** link appears at the bottom of the screen.
5. Verify all ACC settings are correct. See examples below:



ENTERPRISE SERVICES (AT LEAST ONE REQUIRED)

BES ☑

Certificate Authorities

Entrust PKI ☑

Microsoft Certificate Services ☑

OpenTrust CMS Mobile ☑

Simple Certificate Enrollment Protocol (SCEP) ☑

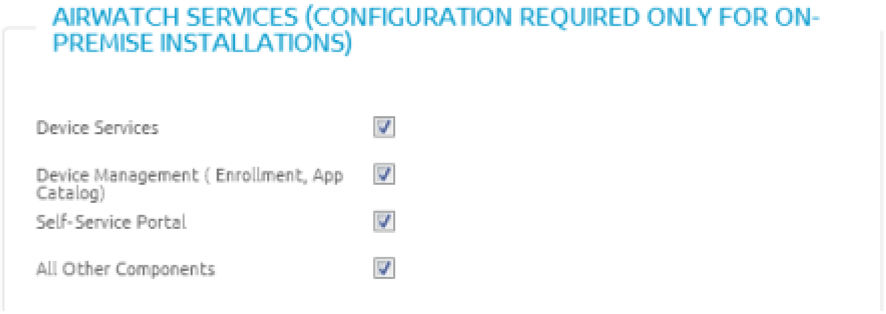
Symantec MPKI □

Directory Services (LDAP / AD) ☑

Exchange Powershell ☑

SMTP (Email Relay) ☑

Syslog ☑



AIRWATCH SERVICES (CONFIGURATION REQUIRED ONLY FOR ON-PREMISE INSTALLATIONS)

Device Services ☑

Device Management (Enrollment, App Catalog) ☑

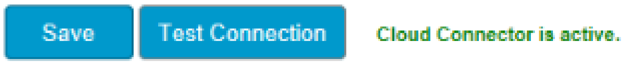
Self-Service Portal ☑

All Other Components ☑

6. Run the ACC installer on the EIS server as noted in Running the ACC Installer.

Note: AirWatch recommends installing ACC on the EIS server in case you need to restore EIS. It is much easier to restore if both reside on the same server. The ACC installer will not delete or overwrite EIS. Once the ACC installer is launched, EIS recognizes the migration process and disables EIS.

7. After the ACC installation is complete, select **Test Connection** on the **Cloud Connector** screen.



Cloud Connector is active.

Note: A successful test (Cloud Connector is Active) means AirWatch, AWCM, and ACC are actively communicating and you have migrated from EIS to ACC.

Appendix A – Upgrading ACC

Overview

Upgrade the AirWatch Cloud Connector (ACC) from the AirWatch Admin 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.

In This Section

- ACC Auto-Update Option – See the benefits of the ACC auto-update option and how the process operates.
- ACC Manual Update Option – See instructions for manually updating the ACC.

ACC Auto-Update Option

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

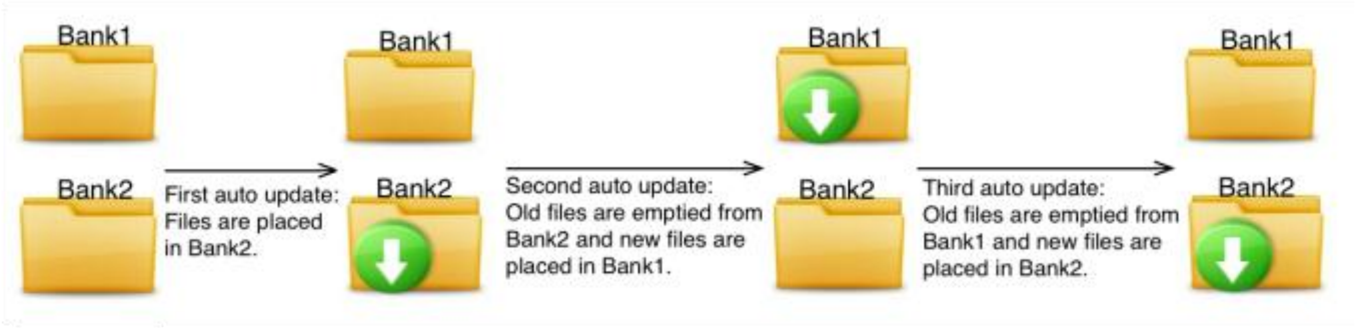
Benefits

- No need to determine manually if you need to upgrade and then have to search for the latest ACC 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

ACC auto-update is performed using the **Bank1** and **Bank2** folders inside the **CloudConnector** 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 below.

Note: Since the **Bank1** and **Bank2** folders are integral to the ACC auto-update process, do **not** delete the **Bank1** or **Bank2** folders.


Bank1
Bank2
First auto update: Files are placed in Bank2.
Bank1
Bank2
Second auto update: Old files are emptied from Bank2 and new files are placed in Bank1.
Bank1
Bank2
Third auto update: Old files are emptied from Bank1 and new files are placed in Bank2.
Bank1
Bank2

ACC auto-updates are performed with security in mind. Every update is signed by the AirWatch Admin Console and verified by ACC, so it will only update 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 Admin Console on port 443, and then an upgrade occurs.

While ACC 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 ACC servers, to ensure all ACC services are not down at the same time, AirWatch incorporates a random timer to the upgrade process so ACC outages will occur at different times for very short periods of time.

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

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

ACC Manual Update Option

1. Ensure auto-update is turned off in the AirWatch Admin 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:
    - 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.
    - 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.

Appendix B – Regenerating Certificates

Overview

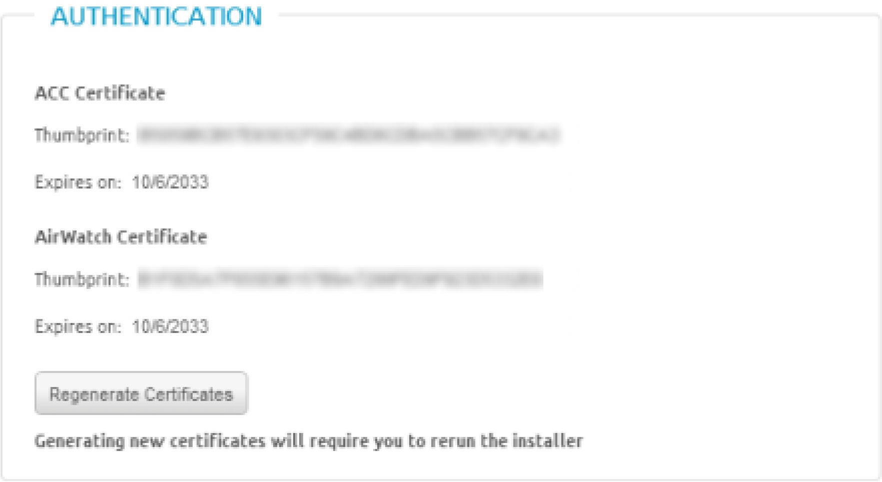
You may find it necessary to regenerate the certificates used for AirWatch and AirWatch Cloud Connector (ACC) servers, for example, if they expire or if your organization requires it on a regularly scheduled basis. The process is simple and is performed from the AirWatch Admin Console, however it does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

Note: 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.

Regenerating Certificates

Perform the following steps to regenerate certificates for AirWatch and ACC servers.

1. Navigate to **Groups & Settings ▶All Settings ▶System ▶Enterprise Integration ▶Cloud Connector**. Both certificates, their thumbprints, and expiration dates are shown.
2. Select **Regenerate Certificates** to generate a new certificate for the ACC and AirWatch servers.



AUTHENTICATION

ACC Certificate

Thumbprint: [redacted]

Expires on: 10/6/2033

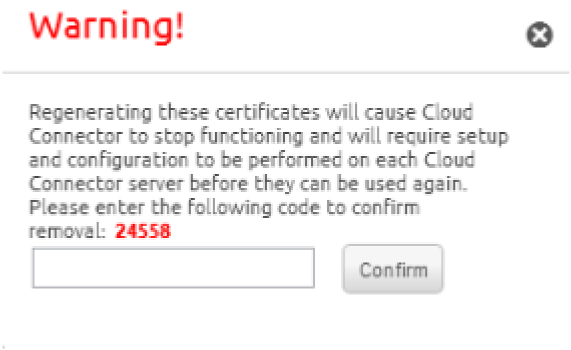
AirWatch Certificate

Thumbprint: [redacted]

Expires on: 10/6/2033

Generating new certificates will require you to rerun the installer

3. When the **Warning** dialog box appears, enter the randomly generated pin code provided and select **Confirm**. Old certificates are deleted and new certificates, thumbprints, and expiration dates are regenerated.



Warning!

Regenerating these certificates will cause Cloud Connector to stop functioning and will require setup and configuration to be performed on each Cloud Connector server before they can be used again. Please enter the following code to confirm removal: 24558

Note: When you select **Confirm**, the ACC will no longer be able to communicate with the AirWatch server. To restore communications between ACC and the AirWatch server, you need to return to Installing ACC and complete all the steps again. This will allow both servers to recognize the latest certificate and regain communications.