AirWatch On-Premise Configuration Guide

A comprehensive guide for managing your on-premise AirWatch deployment

AirWatch v8.0

Table of Contents

Introduction

The purpose of this document is to provide you with some basic information that will help you manage an on-premise deployment of the AirWatch solution. Note that this document does not cover installing or upgrading your AirWatch environment. For instructions on how to do that, see the **AirWatch Installation and Upgrade guides**, which should be provided to you when scheduling either. This guide covers topics such as supported topologies, hardware requirements and sizing for the various AirWatch components, guidelines for high availability and monitoring your AirWatch solution, and more.

IMPORTANT: In general, every on-premise deployment of AirWatch is unique and poses distinct requirements. This document is not an attempt to address each of these deployment types or describe specific configurations for load balancers, monitoring software, and similar tools. Instead, it offers generic guidelines and recommendations where appropriate. Outside of installing AirWatch, it is up to your organization to decide how best to implement certain features such as high availability and/or disaster recovery. AirWatch can provide guidance for your specific deployment – contact AirWatch for more details.

Topology

The AirWatch software suite is composed of multiple components that work in conjunction to provide a complete mobile device solution. The sections below outline each component, as well as give a short summary of their role to aid in the understanding of the AirWatch architecture.

In This Section

- Required Components – Read more about some of the major components you must have as part of an AirWatch implementation.
- Optional Components – See some of the optional components you can leverage as part of an AirWatch on-premise implementation.
- AirWatch On-premise Configurations – See some sample on-premise configurations.

Required Components

AirWatch Admin Console

Administrators use the AirWatch Admin Console via web browser to secure, configure, monitor and manage their corporate device fleet. The Admin Console also typically contains the AirWatch API, which allows external applications to interact with the MDM solution; this API provides layered security to restrict access both on an application and user level.

Device Services

Device Services are the components of AirWatch that actively communicate with devices. AirWatch relies on this component for processing:

- Device enrollment.
- Application provisioning.
- Delivering device commands and receiving device data.
- Hosting the AirWatch Self-Service Portal, which device users can access (through a web browser) to monitor and manage their devices in AirWatch.

SQL Database

AirWatch stores all device and environment data in a Microsoft SQL Server database. Due to the amount of data flowing in and out of the AirWatch database, proper sizing of the Database server is crucial to a successful deployment. Additionally, AirWatch utilizes Microsoft SQL Reporting Services to report on data collected by the AirWatch solution.

For more information on additional system configurations, see the **AirWatch Installation Guide**, available via AirWatch Resources, or consult with your AirWatch representative.

Optional Components

AirWatch Secure Email Gateway

AirWatch offers advanced email management capabilities such as:

- Detection and Remediation of rogue devices connecting to email.
- Advanced controls of Mobile Mail access.
- Advanced access control for administrators.
- Integration with the AirWatch compliance engine.
- Enhanced traffic visibility through interactive email dashboards.
- Certificate integration for advanced protection.
- Email attachment control (available in AirWatch 6.3+).

Enterprises using certain types of email server(s), such as Exchange 2003/2007 or Lotus Traveler, should use the **AirWatch Secure Email Gateway (SEG)** server in order to take advantage of these advanced email management capabilities. The SEG acts as a proxy, handling all Exchange Active Sync traffic between devices and an enterprise's existing ActiveSync endpoint.

Enterprises using Exchange 2010+, Office 365 BPOS, or Google Apps for Work should not need the Secure Email Gateway server. For these email infrastructures, a different deployment model can be used that does not require a proxy server, such as Microsoft Powershell Integration or Google password management techniques.

Note: Email attachment control functionality requires the use of the Secure Email Gateway proxy server regardless of email server type.

Note: Additional information about SEG requirements, setup, and installation can be found in the **AirWatch SEG Administration Guide**, available via AirWatch Resources.

AirWatch Cloud Messaging (AWCM)

AirWatch Cloud Messaging (AWCM) streamlines the delivery of messages and commands from the Console and eliminates the need for end users to access public Internet and procure Google IDs. AWCM also serves as a comprehensive substitute for Google Cloud Messaging (GCM) for Android devices. AWCM is the only option to provide MDM capabilities for Windows Mobile and Symbian devices. It is typically installed on the Device Services server.

AWCM simplifies device management by:

- Removing the need for third party IDs.
- Delivering AirWatch Console commands directly to Android, Symbian, and Windows Mobile devices.
- Enabling the ability for remote control and file management on Android SAFE and Windows Mobile devices.
- Reducing security concerns by eliminating device communication to public endpoints outside of AirWatch.
- Increasing functionality of internal Wi-Fi only devices.

Note: Additional information about AWCM requirements, setup and installation can be found in the **AirWatch AWCM Guide**, available via AirWatch Resources.

AirWatch Cloud Connector (ACC)

AirWatch Cloud Connector (ACC) provides organizations the ability to integrate AirWatch with their back-end enterprise systems. AirWatch Cloud Connector 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's Mobile Device Management (MDM), running in any configuration, together with those of their existing LDAP, certificate authority, email, and other internal systems.

ACC integrates with the following internal components:

- Email Relay (SMTP)
- Directory Services (LDAP / AD)
- Microsoft Certificate Services (PKI)
- Simple Certificate Enrollment Protocol (SCEP PKI)
- Email Management Exchange 2010 (PowerShell)
- BlackBerry Enterprise Server (BES)
- Third-party Certificate Services (On-premise only)
- Lotus Domino Web Service (HTTPS)
- Syslog (Event log data)

Note: Additional information about ACC requirements, setup and installation can be found in the **AirWatch Cloud Connector Guide**, available via AirWatch Resources.

AirWatch Mobile Access Gateway (MAG)

The AirWatch Mobile Access Gateway (MAG) provides a secure and effective method for individual applications to access corporate sites and resources. When your employees access internal content from their mobile devices, the MAG acts as a secure relay between the device and enterprise system. The MAG is able to authenticate and encrypt traffic from individual applications on compliant devices to the back-end site/resources they are trying to reach.

Use the MAG to access:

- Internal document repositories and content using the AirWatch Content Locker.
- Internal websites and web applications using the AirWatch Secure Browser.
- Internal resources via app tunneling for iOS 7 and higher devices using the AirWatch Tunnel.

Note: Additional information about MAG requirements, setup, configuration and installation can be found in the **AirWatch MAG Admin and Install guides**, available via AirWatch Resources.

AirWatch App Wrapping

AirWatch Application Wrapping, or app wrapping, allows organizations to secure enterprise applications without code changes. It can add an extra layer of security and data loss prevention while offering a consistent user experience. Consistency comes from using AirWatch options such as branding, single sign on (SSO), and authentication.

Modifying your internal applications with app wrapping reduces time and expenses from development on management and security. It lets you access tools already available with AirWatch by simply adding a layer of features over the application. Once the advanced features are applied, deploy the application to your enterprise application catalog for end users to access.

Note: Additional information about app wrapping can be found in the **AirWatch App Wrapping Guide**, available via AirWatch Resources.

Android Market integration (Apache server)

This feature is available for on-premise customers only. It serves as a connection between the AirWatch MDM and the Google Play Store. This needs to be configured before an admin can use the **Search App Store** feature for Android apps.

AirWatch On-Premise Configurations

When deployed within an organization's network infrastructure, AirWatch can adhere to strict corporate security policies by storing all data onsite. In addition, AirWatch has been designed to run on virtual environments, which allows for seamless deployments on a number of different setups.

AirWatch can be deployed in a variety of configurations to suit diverse business requirements. Common deployment topologies include single-server, multi-server, and hybrid models. The primary difference between these deployment models are how AirWatch components (Admin Console, Device Services, AWCM, Database Server, Secure Email Gateway, ACC, and MAG) are grouped, and how they are positioned within the corporate network.

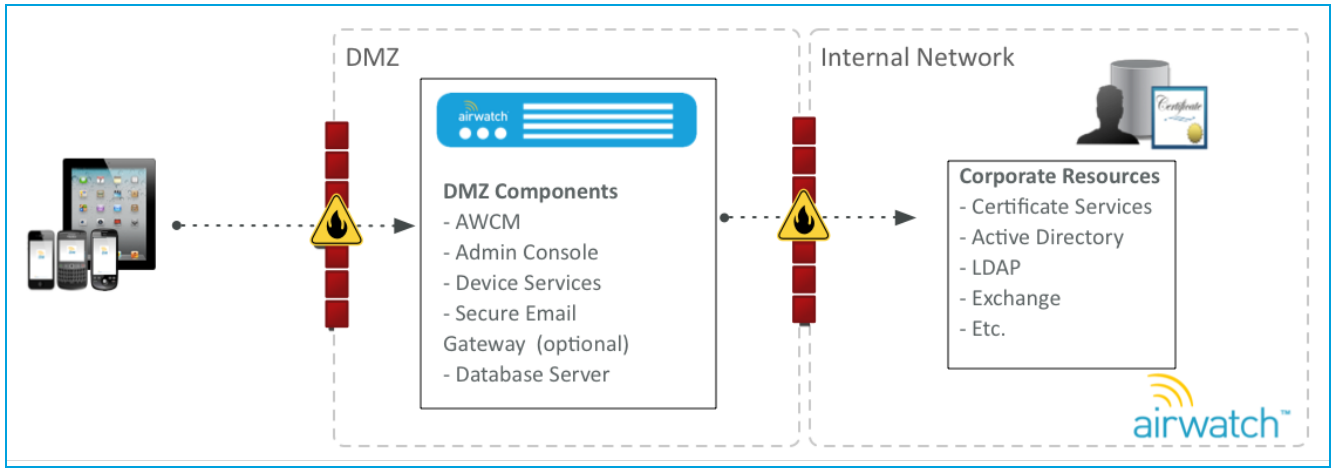
IMPORTANT: While three common permutations are further detailed below, the AirWatch solution is highly customizable to meet your organization's specific needs. If necessary, contact AirWatch to discuss the possible server combinations that best suit your organization's needs.

For more information on hardware sizing, see Hardware Requirements.

Note: Most typical AirWatch topologies support reverse proxies. A reverse proxy can be used to route incoming traffic from devices and users on the Internet to the AirWatch servers in your corporate network. Supported reverse proxy technologies include: Bluecoat, Microsoft, F5 Networks, IBM, and Cisco. Consult your AirWatch representative for additional support for technologies not listed here, as support is continuously evolving.

Basic/Single App Server Deployment

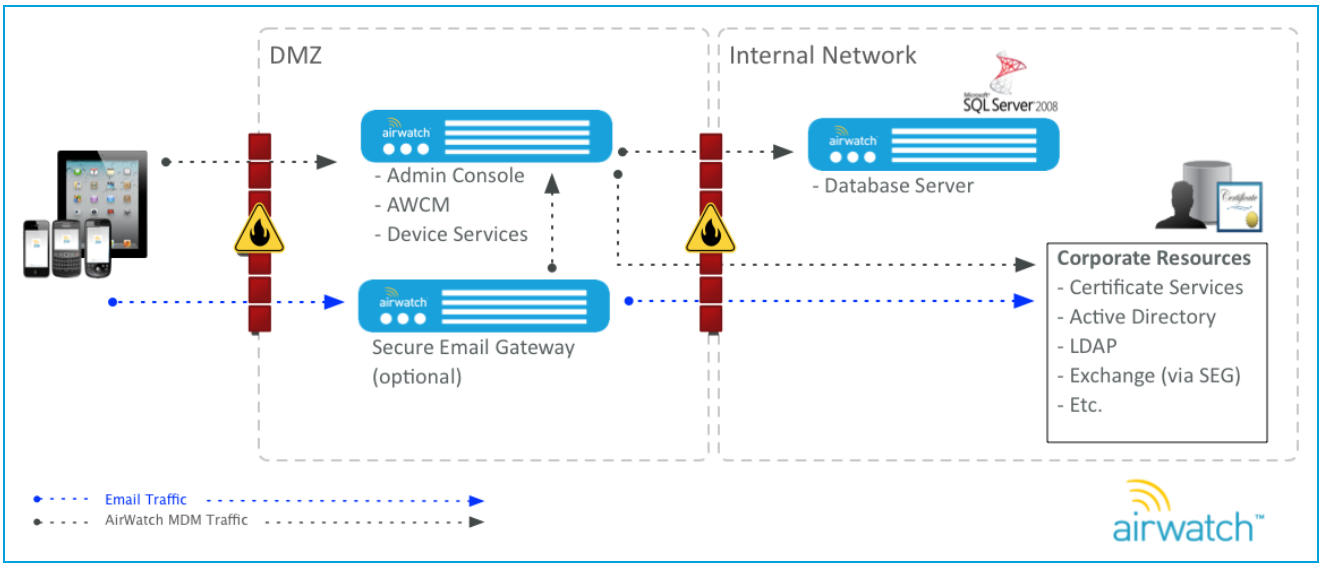
This delivery model can be used for organizations managing less than 1,000 devices. This configuration allows for simplified installation and maintenance, while allowing future scalability and flexibility as deployments grow. A single-server deployment allows for easy integration to enterprise services, as well as simplified control and validation over the entire environment.



Hybrid Server Deployment

A hybrid-server deployment model is recommended for organizations managing between 1,000 and 5,000 devices, however it can be used even for deployments of less than 1,000 devices. This configuration differs from the single server model by separating the Secure Email Gateway (SEG) and the Database Server each onto separate servers.

The advantage of this topology comes in segregating the email management infrastructure to be maintained and scaled independently, as well as isolating the database server for ease of troubleshooting and future scale.

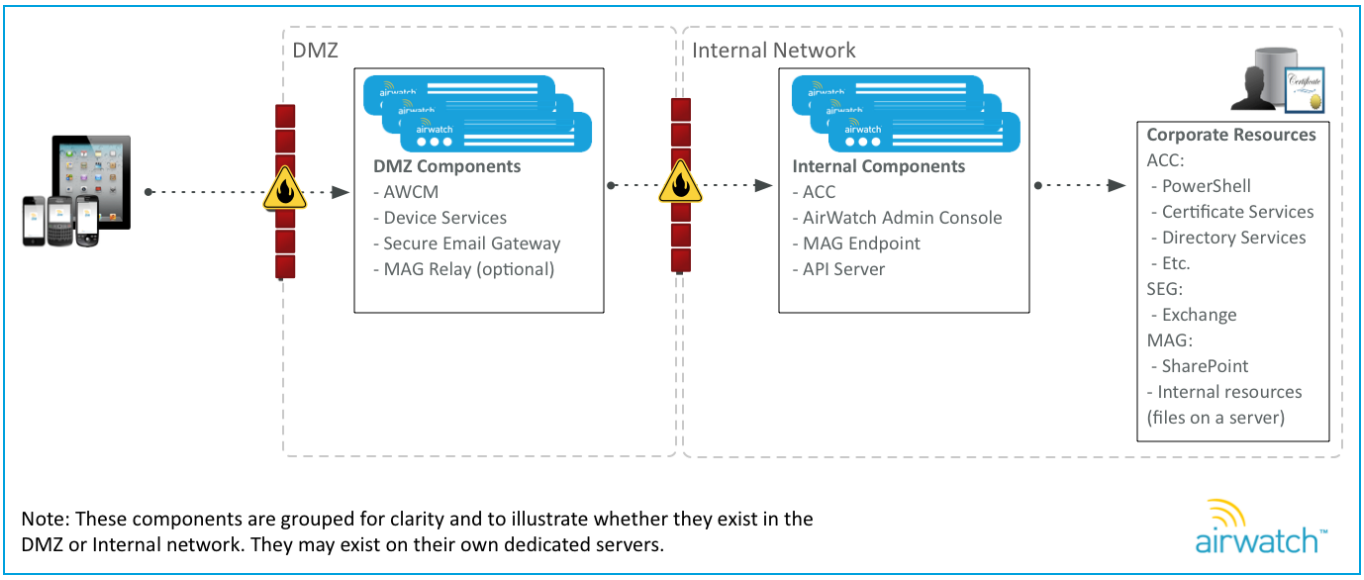


Multiple Server Deployment

A multi-server deployment model is recommended for organizations managing 5,000 or more devices and/or those wanting to utilize a DMZ architecture to segment the administrative console server into the internal network for increased security. This deployment model allows for increased resource capacity by allowing each server to be dedicated to AirWatch components. The following diagrams illustrate how to leverage ACC and MAG in an on-premise environment.

IMPORTANT: While these components are combined in the diagrams below for illustrative purposes, they can reside on a dedicated server. Many configuration combinations exist and may apply to your particular network setup. Please contact AirWatch and schedule a consultation to discuss the appropriate server configuration for your on-premise deployment.

Multi Server with ACC and MAG



Hardware Requirements

When determining the hardware requirements needed to build out an AirWatch environment, it is important to consider the number of managed devices, the device transaction frequency, the device check-in interval and the number of administrative users that AirWatch will be managing. It may also be beneficial to consider the growth potential of the organization's device fleet as well.

The sizing recommendations listed below are written against device transaction data gathered from AirWatch Cloud deployments. Sizing for an AirWatch environment should begin with an initial assessment of critical factors to provide a clear view of system usage.

Sizing for 100 to 25,000 Devices

<table>
<tr><th colspan="2">Up to how many devices?</th><th>100</th><th>500</th><th>1,000</th><th>2,500</th><th>5,000</th><th>10,000</th><th>25,000</th></tr>
<tr><td rowspan="6">Database Server</td><td>CPU Cores</td><td>1</td><td>1</td><td>2</td><td>2</td><td>2</td><td>4</td><td>8</td></tr>
<tr><td>RAM (GB)</td><td>4</td><td>4</td><td>4</td><td>8</td><td>8</td><td>16</td><td>32</td></tr>
<tr><td>DB Size (GB)</td><td>10</td><td>20</td><td>25</td><td>50</td><td>100</td><td>175</td><td>250</td></tr>
<tr><td>Trans Log Size (GB)
(Log backups every 15 minutes)</td><td>3</td><td>5</td><td>10</td><td>20</td><td>40</td><td>50</td><td>100</td></tr>
<tr><td>Temp DB (GB)</td><td>3</td><td>5</td><td>10</td><td>20</td><td>40</td><td>50</td><td>100</td></tr>
<tr><td>Avg IOPS
(DB & Temp DB)</td><td>30</td><td>30</td><td>30</td><td>75</td><td>150</td><td>300</td><td>750</td></tr>
<tr><td>Peak IOPS
(DB & Temp DB)</td><td>40</td><td>50</td><td>60</td><td>150</td><td>300</td><td>600</td><td>1500</td></tr>
<tr><td colspan="2">Admin Console (includes API component)</td><td colspan="5" rowspan="3">1x Application Server ‡ ±</td><td colspan="2">1x Application Server per 50 concurrent admin users ‡ ±</td></tr>
<tr><td colspan="2">Device Services</td><td>1x Application Server ‡ ±</td><td>2x Application Servers * ‡</td></tr>
<tr><td colspan="2">Device Services and AWCM</td><td>1x Application Server ‡ ±</td><td>2x Application Servers* ‡</td></tr>
<tr><td colspan="2">SEG Proxy Server †</td><td colspan="7">See Secure Email Gateway Server Hardware Assumptions below</td></tr>
<tr><td colspan="2">MAG</td><td colspan="7">See Mobile Access Gateway Server Hardware Assumptions below</td></tr>
</table>

‡ Each Application Server needs to be a server or virtual machine (VM) configured with at least 2 CPU cores and 4GB RAM. An Intel processor is required.

± When using a 1x Application Server for the DB, AirWatch Console, and Device Services, add the total RAM

requirements in the table above for all three and then verify the Application Server has the proper amount of RAM installed. If using AWCM on the same server as Device Services, add 4GB RAM for each Application Server.

† If a SEG is implemented (optional), for every 2,000 devices, use one CPU core with 2GB of RAM (e.g., 8K devices need 4 CPU cores with 8GB RAM). For every 16K devices you deploy, (e.g., 8 CPU cores with 16GB RAM), AirWatch recommends you add a SEG (e.g., 40K devices requires three SEGs). For more information, consult the **AirWatch Managing and Protecting Mobile Email** overview or the **AirWatch Secure Email Gateway Proxy Server Configuration Guide**.

* Load Balancing provided by customer.

Sizing for 50,000 to 250,000+ Devices

Up to how many devices?		50,000	100,000	150,000	200,000
Database Server	CPU Cores	8	16	32	48
	RAM (GB)	64	128	192	256
	DB Size (GB)	500	1 TB	1.5 TB	2 TB
	Trans Log Size (GB) (Log backups every 15 minutes)	200	400	600	800
	Temp DB (GB)	200	400	600	800
	Avg IOPS (DB & Temp DB)	1500	3000	4500	6000
	Peak IOPS (DB & Temp DB)	3000	6000	9000	12000
Admin Console (includes API component)†		2 load-balanced application servers with 2 CPU cores/4GB RAM each and 50 GB storage		2 load-balanced application servers with 2 CPU cores/8GB RAM each and 50 GB storage	2 load-balanced application servers with 4 CPU cores/8GB RAM each and 50 GB storage
Device Services		2 load-balanced application servers with 2 CPU cores/4GB RAM each and 50 GB storage	2 load-balanced application servers with 2 CPU cores/8GB RAM each and 50 GB storage	2 load-balanced application servers with 4 CPU cores/8GB RAM each and 50 GB storage	2 load-balanced application servers with 4 CPU cores/16GB RAM each and 50 GB storage
Device Services with AWCM		2 load-balanced application servers with 2 CPU cores/8GB RAM each and 50 GB storage	2 load-balanced application servers with 2 CPU cores/12GB RAM each and 50 GB storage	2 load-balanced application servers with 4 CPU cores/12GB RAM each and 50 GB storage	2 load-balanced application servers with 4 CPU cores/20GB RAM each and 50 GB storage
Reporting Server (SSRS)		1 reporting server with 1 CPU core/4 GB RAM and 50 GB storage			1 reporting server with 2 CPU core/8 GB RAM and 50 GB storage
API Server (if dedicated)*		2 load-balanced servers with 2 CPU cores/ 4GB RAM each and 50 GB storage		2 load-balanced servers with 4 CPU cores/ 4GB RAM each and 50 GB storage	2 load-balanced servers with 4 CPU cores/ 8GB RAM each and 50 GB storage
SEG Proxy Server		4 load-balanced servers with 8 CPU cores/16 GB RAM each and 50 GB storage	8 load-balanced servers with 8 CPU cores/16 GB RAM each and 50 GB storage	12 load-balanced servers with 8 CPU cores/16 GB RAM each and 50 GB storage	16 load-balanced servers with 8 CPU cores/16 GB RAM each and 50 GB storage

*If your API server is standalone then the network requirements for the API server is to ensure connectivity to the database. All other AirWatch services (Console, Device Services, SEG, MAG) should be enabled to communicate to the API server over HTTPS (443).

† These numbers are for the combined Console+API server requirements given standard API usage. Ultimately these requirements will depend on how you use the APIs, with heavy use resulting in different sizing numbers. Since API use is situational, AirWatch does not provide a standard recommendation for cases of heavy API use.

For Application Servers, an Intel processor is required.

General Assumptions

The following are general assumptions that will help you determine if you need to adjust the hardware requirements shown in the table above based on the hardware needs of your environment.

- High Availability is easily accomplished in AirWatch. See High Availability for more information.
- Sizing estimates include allocation for 1GB of cumulative app storage. Increase the server disk space and DB disk space to account for increased storage (for example, a 5GB app deployment will require an additional 4GB disk space for the database and application servers).
- Sizing estimates include allocation for 1GB of cumulative content storage for the AirWatch Content Locker. Increase the server disk space to account for increased storage (for example, 5GB of content requires an additional 4GB disk space for the application servers).
- Servers must be set up in English. AirWatch must be set up on an English Operating System.

Application Server Hardware Assumptions

Unless otherwise specified, the following assumptions are made regarding server hardware used to host the AirWatch application(s):

- The AirWatch application may be installed on virtual or physical hardware.
- Servers should provide, at minimum:
    - 1x 64-bit Dual Core Processor*, 4GB RAM, 40GB free space for AirWatch application

      *An Intel processor is required.

Database Server Hardware Assumptions

Unless otherwise specified, the following assumptions are made regarding server hardware used to host the AirWatch database:

- AirWatch recommends using physical hardware for the database server.
    - AirWatch may be deployed using a virtualized database layer given the I/O requirements can be met and the overall virtual architecture will support AirWatch's requirements.
- If AirWatch is to be installed on a shared database server, AirWatch should be given its own instance with earmarked resources as defined in the sizing table.

Secure Email Gateway Server Hardware Assumptions

The following assumptions are made regarding server hardware used to host the Secure Email Gateway (SEG) application:

- The AirWatch SEG server should be sized in accordance with the enterprise mail server:

SEG	CPU Core*	RAM**	Notes
SEG without content transformation (Attachment handling, hyperlinks security, tagging, etc.)	1	2 GB	Per 2,000 devices, up to a maximum of 16,000 devices (8 CPU/16GB RAM)
SEG with content transformation (Attachment handling, hyperlinks security, tagging, etc.)	1	2 GB	Per 1,000 devices, up to a maximum of 8,000 devices (8 CPU/16 GB RAM)

*An Intel processor is required.

**A minimum of 2 GB RAM is required per SEG CPU core.

Note: Sizing estimates vary based on actual email and attachment usage. Add additional SEG servers as necessary.

- When installing SEG servers in a load balanced configuration, sizing requirements can be viewed as cumulative. For example, a SEG environment requiring 4 CPU Cores and 8GB of RAM can be supported by either:
  - One single SEG server with 4 CPU cores and 8GB RAM

    or
  - Two load balanced SEG servers with 2 CPU core and 4GB RAM each

Mobile Access Gateway Server Hardware Assumptions

The following assumptions are made regarding server hardware used to host the Mobile Access Gateway (MAG):

Hardware Requirements per MAG

- Virtual machine (VM) or physical server
- 1 CPU Core* (2.0+ GHz)

  *An Intel processor is required.
- 2 GB RAM or higher
- 1 GB Disk (approximate application footprint)

Sizing for up to 100,000 Devices

Number of Devices	Up to 5,000	10,000 to 50,000	50,000 to 100,000	100,000+
CPU Cores* ***An Intel processor is required.**	1	4 or 2 load-balanced w/ 2 CPU Cores	4 or 2 load-balanced w/ 2 CPU Cores	2 load-balanced with 4 CPU Cores
RAM (GB)	4	4	8	16

Monitoring Guidelines

Monitoring your AirWatch solution is an important part of ensuring it operates effectively. Many tools and software packages exist to help you do this. Examples include Nagios, Splunk, Symantec Altiris, Spotlight, Ignite, and Montastic. Consult your local IT policy for specific recommendations on monitoring tools if you do not already have a solution in place. The section below details some generic hardware load capacity recommendations and information about log files and URL endpoints. This section does not explicitly cover how to configure a monitoring solution. If you need further assistance, please contact AirWatch.

Hardware Load Capacity Recommendations

Hardware	Monitoring	Recommendation
CPU	CPU load-hour	Alerting at high-load
RAM	Free memory	Alerting at low free memory
Hard Disk	Free hard disk space	Alerting at low hard disk space

AirWatch Logs

AirWatch-specific warnings and errors are written to log files in the `\AirWatch\Logs` directory, as well as the Windows Event Viewer. The level of logging ("Error" or "Verbose") is controlled by configuration files in the AirWatch directory structure. Automatic monitoring of these files is not required, however you should consult these files should issues arise.

Health Checks – AirWatch Endpoints

The following URL endpoints for the various AirWatch components can be monitored to ensure a fully functioning, healthy AirWatch environment. The endpoints and expected status codes are listed below.

Device Services

Note: Since most typical on-premise configurations have the components listed here as part of the Device Services server, they are grouped together as "Device Services".

Description	URL Endpoint	Status code
Device Services Endpoint	/DeviceServices/airwatchbeacon.svc	HTTP 200 – Test Page
Device Services Enrollment	/enroll or /DeviceManagement/enrollment	HTTP 200
Self-Service Portal	/MyDevice	HTTP 200

Description	URL Endpoint	Status code
App Catalog	/DeviceManagement/appcatalog?uid=0	HTTP 200 – Text on page: "An error has occurred."
Device Services AWCM	/AWCM/Status	HTTP 200 – Status Page
Device Services WinMo Tracker	/DeviceServices/tracker.aspx?id=0	HTTP 200 – Text on page: "OK"

Console Server

Description	URL Endpoint	Status code
Web Console	/AirWatch/login/index	HTTP 200
API Endpoint	/AirWatchServices/LocationGroupServiceEndpoint.svc	HTTP 200 – Test Page

Secure Email Gateway

Description	URL Endpoint	Status code
SEG Console	/SegConsole/default.aspx	HTTP 200
EAS Integration	/SegConsole/management.ashx?ping	HTTP 200
ActiveSync Connectivity	/Microsoft-Server-Activesync	HTTP/1.1 401

Mobile Access Gateway

Description	URL Endpoint	Status code
Content	/Content/default.aspx	HTTP 200
HTTP	://<MAG_URL>:<HTTP_Port>	HTTP 407
HTTPS	://<MAG_URL>:<HTTPS_Port>	HTTP 407

AirWatch Database

The AirWatch database should be monitored to ensure a fully-functioning, healthy AirWatch environment. The table below provides several recommendations for monitoring on the AirWatch database.

Monitor	Description
Data Files	Monitor and alert for resizing when free space in data files drops below 10%.
Transaction Logs	Monitor and resize if free space in log drops below 10%
Index Rebuild	Monitor for fragmentation between 10% and 29%. Reorganize with an update of statistics. Indexes with fragmentation greater than 29% should be rebuilt.
SQL Server CPU	Monitor sustained high CPU utilization (Over 90% for a 15 minute duration)

SQL Server Job History	Monitor failed SQL Server Agent Jobs (in particular, AirWatch Jobs)
SQL Server Page Life Expectancy	Monitor SQL Server Page Life Expectancy (dropping below 3000)
SQL Server Disk Space	Monitor disk space usage on all Data and Log Drives for 'AirWatch' and 'tempdb' Databases
SQL Server Disk Queueing	Monitor Disk Queueing on all Data and Log Drives for 'AirWatch' and 'tempdb' Databases

Health Checks

Synthetic transactions are the strongest indicator of a healthy AirWatch environment. They can mimic end user actions (for example, enrollment) and report if there are issues. Many different use cases could be considered, and high-use scenarios should be tested with synthetic transactions. An example synthetic transaction could be:

1. Navigate to the **AirWatch Admin Console**
2. Log in using credentials
3. Navigate to **Hub** ▸ **Reports & Analytics** ▸ **Reports** ▸ **List View**.
4. Run a report
5. Logout

Typically, a tool like Keynote or AlertSite would be used to generate and monitor synthetic transactions.

Maintenance Guidelines

This section describes some of the recommended maintenance tasks to perform for your on-premise deployment.

AirWatch Database

AirWatch Database Regular database maintenance should be performed. Maintenance standards vary per company. Please check with you local database team for best practices. The following table provides AirWatch recommended database maintenance guidelines.

Task	Frequency	Description	Responsible Party
Transaction Log Backups	Nightly	Keeps high percentage of free space in log file.	Customer DBA
AirWatch Purge Job	Nightly	Removes expired session data provided by AirWatch.	AirWatch Built-In Function
Index Rebuild	Nightly	Routine index maintenance, especially after purge job.	Customer DBA
Daily Differential Backup	Nightly	Creates a backup file of database changes since the previous full backup.	Customer DBA
Weekly Full Backup	Weekly	Creates a backup file of the entire database. Full backups should be retained per your organization's policies.	Customer DBA
Multiple Data Files	One time	This helps reduce the IO burden of their installation.	Customer DBA
Disable Hyperthreading	One time	Improves performance and decreases memory usage on computers running SQL Server and BizTalk Server.	Customer DBA
Backup Validation	As Needed	Ensures full and differential backups are being performed and retained on schedule.	Customer DBA
Database Consistency Check (DBCC CHECKDB)	As Needed	Checks the logical and physical integrity of all database content.	Customer DBA
Resize Data Files	As Needed	This prevents VLFs and keeps enough free space in log file.	Customer DBA
Resize Transaction Log	As Needed	This prevents VLFs and keeps enough free space in log file.	Customer DBA

AirWatch Logs

Over time, it may be necessary to archive or purge old AirWatch log files to conserve disk space. If logging is set to verbose on AirWatch services or websites, archiving or purging should occur more frequently. Hard disk space should be monitored, as recommended above. If disk space becomes low, archiving or purging old log files is recommended.

The following DOS script can be used to delete AirWatch logs with “LastAccessTime” greater than a set number of days in \AirWatch\Logs:

```
start /wait powershell -command "dir e:\AirWatch\logs -recurse | where
{((getdate) - $_.LastAccessTime).days -ge 14} | remove-item -force –recurse"
```

Windows Update

It is recommended that auto-update functionality is turned off and manual updates are performed every 2-4 weeks or per your organization's policy.

High Availability

In addition to carefully monitoring your AirWatch solution to ensure uptime, you can also configure load balancing solutions to achieve high availability within your AirWatch environment. This section lists the various AirWatch components and whether they support load balancing and session persistence as part of a highly available system.

AirWatch Modules

Application servers receive requests from the console and device users and process the data and results. No persistent data is maintained on these servers, but user and device sessions are maintained for a short period of time. High availability is achieved through the use of load balancing and session persistence. See Monitoring for information on health checks on the servers. The following table outlines both for each AirWatch component:

Note: While supported, IP-based session persistence is not recommended. Contact AirWatch if you have specific questions or concerns in regards to your specific deployment.

Application Modu	Load Balanci Supported?	Health Check Implementation	Session Persistence	Recommended Time Value
Console	Yes*	https://<host>/airwatch/awhealth/v1	Source IP / Session ID / Cookie persistence	60 minutes
IMPORTANT: *The Scheduler service should only be active on **one** Console server. All other services/endpoints of the Console can be load-balanced in an active-active configuration.				
Device Services**	Yes	https://<host>/deviceservices/awhealth/v1 **Device Management:** https://<host>/devicemanagement/awhealth/v1 **App Catalog:** Not currently available **Self-Service Portal:** https://<host>/selfserviceportal/awhealth/v1	Cookie/session persistence is recommended. Source IP may be used in certain scenarios.	20 minutes
Note: **Since a typical on-premise configuration will have the components listed here as part of the Device Services server, they are grouped together as "Device Services".				

Application Modu	Load Balanci Supported?	Health Check Implementation	Session Persistence	Recommended Time Value
AirWatch Cloud Messaging	Yes	https://<host>/awcm/status	Session ID / Cookie persistence (query parameter – Http header: awcmsessionid)	N/A
Mobile Access Gateway	Yes	Not currently available	MAG Relay: Cookie/session persistence is recommended. Source IP may be used in certain scenarios. MAG Endpoint: Source IP / Session ID / Cookie persistence	30 minutes
Secure Email Gateway	Yes	Not currently available	Cookie/session persistence is recommended. Source IP persistence may be used in certain scenarios.	Configure to be the same as the persistence timeout value for your Exchange ActiveSync Servers based on recommendations from the Mail Solution vendor.
AirWatch Cloud Connector	Not required (see **Note**)	Not currently available	Not required	N/A
API (SOAP and REST)	Yes	Not currently available	Source IP / Session ID / Cookie persistence	

Note: ACC traffic is automatically load-balanced by the AWCM component – it does not require a separate load balancer because there are no incoming connections. To accommodate additional users as part of your sizing requirements you can deploy multiple ACCs, which will all be load balanced by AWCM.

Health Check for Load Balancers

A load balancer performs a health check of the servers in the pool to ensure connectivity is active. If it does not receive a response, then it marks that server as down and any subsequent requests will be directed to a new server. You can use the following health check test for your load balancer to test connectivity to the Console, Device Services, Device Management, Self-Service Portal, Autodiscovery, and APNs Provisioning Portal endpoints.

1. Configure the following in your load balancer: **GET to /airwatch/awhealth/v1**.
2. Add your load balancer's IP address in the AirWatch Admin Console under **System Settings ▸ Admin ▸ Monitoring**.

Load Balancer Recommendations

- You can configure load balancers with an algorithm of your choosing. AirWatch supports simple algorithms such as Round Robins and more sophisticated ones such as Least Connections.
- Below are some examples for configuring persistence for each of the following components:
  - **Device Services:** Session persistence timeout of 20 minutes is required based on the default configuration of AirWatch.

    Note: If the **Enrollment Session Timeout** values are modified in **AirWatchConsole Settings**, then you need to set the **Persistence Timeout** values to the same value.

  - **Admin Console:** Session persistence timeout of one hour is required based on the default configuration of AirWatch.

    Note: If the **Idle Session Timeout** values are modified in the **AirWatchConsole Settings**, then you need to set the **Persistence Timeout** values to the same value.

  - **Secure Email Gateway:** Session persistence timeout value for the Secure Email Gateway needs to be the same as the persistence timeout value for your Exchange ActiveSync Servers based on recommendations from the Mail Solution vendor.
  - **Mail (EAS) Servers:** AirWatch recommends that you follow the recommendations from your load balancer and mail environment vendors to configure the load balancer in front of the EAS server(s) when using the SEG(s). In general, using a Source IP-based persistence is not recommended when using the SEG(s).
- Load balancers are also recommended to redirect all HTTP requests to HTTPS.

Database Servers

All critical data and configurations for AirWatch are stored in the database and this is the data tier of the solution. AirWatch databases are based on the Microsoft SQL server platform. Microsoft provides multiple options to maintain a highly available SQL Server Environment. Depending on IT Policy, one or more of the recommended options can be implemented.

IMPORTANT: You can configure HA for your database servers using whatever method meets your organization's policies or needs. AirWatch has no dependency upon your HA configuration for database servers. However, AirWatch strongly recommends you have some type of failover for high availability and disaster recovery scenarios, since all of your device data is stored there.

To achieve high availability of database servers, the options available are:

- Failover Clustering
- Database Mirroring

More information is available at http://msdn.microsoft.com/en-us/library/ms190202.aspx

Disaster Recovery

AirWatch components can be deployed to accommodate most of the typical disaster recovery scenarios. A robust backup policy for application servers and database servers can restore an AirWatch environment in another location with minimal steps. You can configure disaster recovery for your AirWatch solution using whatever procedures and methods meet your organization's DR policies. AirWatch has no dependency upon your DR configuration, however, AirWatch strongly recommends you have some type of failover for DR scenarios.

Since every organization is unique, It is ultimately up to your organization how to deploy and maintain a disaster recovery policy. As such, no specific recommendations or steps are listed here. If you would like assistance from AirWatch with disaster recovery, please contact AirWatch.

Appendix: Services

The following is a list of AirWatch services with descriptions.

Service Name	Service Description
AirWatch Agent Builder Services	Service that generates a CAB file that's available for download from the Admin Console.
AirWatch Alert Adapter	The Alert Adapter processes data from AirWatch to generate alerts.
AirWatch Alert Delivery Service	Takes alerts from the adapter and delivers them to end users.
AirWatch Batch Processing Service	This service extracts user information from Bulk Import Spreadsheets and puts the data in the Database.
AirWatch Cloud Connector	Enables integration with your back-end enterprise resources.
AirWatch Cloud Messaging Service	This service allows device to securely establish a persistent connection to AirWatch. It delivers the messages and processes commands from the Console.
AirWatch Content Delivery	This service is responsible for pushing staging and provisioning content to relay servers.
AirWatch Device Scheduler	The Device Scheduler Service reads the schedule settings from the database and writes it to the two queues APNSOutbound and C2DMOutbound per the query schedule setup in System Settings.
AirWatch Device Tunnel Queue Monitor Service	This service reads information from a Queue that the Tunnel Server writes to. It then writes this information to the database.
AirWatch Diagnostic Service	Service used to report diagnostics information. Monitoring these is up to your organization. If they go down they will no longer report diagnostics information, but will not cause service interruptions.
AirWatch EAS Integration Service	Processes mail requests routed through the AirWatch Secure Email Gateway.
AirWatch Entity Change Queue Monitor	This service monitors the event log MSMQ and sends the outbound event logs.
AirWatch GEM Inventory Service	AirWatch GEM Inventory Service communicate instance-specific information to a GEM installation.
AirWatch Integration Service	
AirWatch Interrogator Queue Monitor	Processes samples from devices that have been stored in various queues, and writes those samples to the database.

Service Name	Service Description
AirWatch Interrogator Server	Handles incoming samples from devices and stores them in a common queue to be processed later.
AirWatch Log Manager Queue Monitor	The Log Manager Queue Service processes incoming data samples from Windows Mobile Devices.
AirWatch Master Queue Service	Service that processes inbound samples from a device in an Intermediate queue, and distributes to individual batch sample queues.
AirWatch MEG Queue Service	Reads and processes mobile email gateway requests from MSMQ.
AirWatch Messaging Service	The Messaging service reads the scheduled messages from the APNSOutbound and C2DMOutbound queues and sends them to the respective Cloud services.
AirWatch Mobile Access Gateway	Adds Proxy to all your internal resources.
AirWatch Policy Engine	This service is used to determine product/product set applicability and compliance for devices, if needed, product jobs are sent to the device to install, uninstall profiles, file/actions and applications.
AirWatch Remote Control Tunnel Service	This service reads information from a Queue that the Tunnel Server writes to. It then writes this information to the database.
AirWatch SMS Service	The messaging service is used by the Web Console to send messages to devices.
Tunnel Server	Tunnel Server service maintains open connections for communication to Windows Mobile devices.

Appendix: Message Queues

The following is a list of AirWatch message queues and descriptions.

Message Queues	Description
apnsoutbound	iOS Outbound APNS Messages
awadminbatchqueue	AirWatch Admin Batch Queue
awapplecaregsxintegration	Model Information Request to AppleCare
awapplicationeventsample	Application Analytics for iOS Content Locker
awapplicationfeedback	
awapplicationlistsample	iOS Application List Samples (From Device)
awappscantpiqueue	App Scan requests to Third Party Apps
awautodiscovery	Used for auto discovery messages
awbluetoothinformationsample	Android/BlackBerry/WinMo Bluetooth Samples (From Device)
awcalllogsample	Android/BlackBerry/WinMo Call Log Samples (From Device)
awcellinformationsample	Android/BlackBerry/WinMo Cellular Information Samples (From Device)
awcellsignalqualitysample	Android/BlackBerry/WinMo Cell Signal Quality Samples (From Device)
awcelltowerinformationsample	Android/BlackBerry/WinMo Cell Tower Information Samples (From Device)
awcertificatelistsample	iOS Certificate List Samples (From Device)
awcompliancedevicequeue	AirWatch Compliance Device Queue
awdevicecapabilitysample	AirWatch Device Capability Sample
awdevicecustomattributelistsample	List of device custom attributes, used primarily by rugged devices (Android, QNX, WinMo, Mac, PCs, etc.)
awdevicesampledata	Used for initializing devices for compliance
awdiskencryptionsample	AirWatch Disk Encryption Sample
aweventlog	Keeps various events related to device / system activities
awgpscoordinatesample	Android/BlackBerry/WinMo GPS Coordiante Samples (From Device)
awgpsextendedcoordinatessample	Android/BlackBerry/WinMo Extended GPS Coordinate Samples (From Device)
awintegrationservice	
awlogmanagerxml	WinMo LogManager XML Samples (From Device)
awmanagedmedialistsample	Managed Media List Sample (Managed Books)
awmastersamplequeue	iOS Master Queue Samples (From Device)
awmegpayloads	MEG Payload Samples (from API)
awmemorysample	Android/BlackBerry/WinMo Memory Samples (From Device)

Message Queues	Description
awmetricssample	New Product Provisioning
awmobiledatausagesample	AirWatch Mobile Data Usage Sample
awnetworkadaptersample	Android/BlackBerry/WinMo Network Adapter Samples (From Device)
awnetworkadaptersample	Android/BlackBerry/WinMo Network Adapter Samples (From Device)
awnetworkwlansample	Android/BlackBerry/WinMo Network WLAN Samples (From Device)
awnetworkwlansample	Android/BlackBerry/WinMo Network WLAN Samples (From Device)
awnonmobiledatausagesample	AirWatch Non Mobile Data Usage Sample
awoutboundeventlog	AirWatch Outbound Event Log
awpolicylistsample	New Product Provisioning
awpolicyproductlistsample	New Product Provisioning
awpowersample	Android/BlackBerry/WinMo Power Samples (From Device)
awpowersampleex	Android/BlackBerry/WinMo Extended Power Samples (From Device)
awprinternotification	Common MSMQ to send notifications to Zebra and Toshiba Print Servers
awprofilelistsample	iOS Configuration Profile List Samples (From Device)
awprovisioningprofilesample	iOS Provisioning Profile Samples (From Device)
awpublishqueue	iOS Bulk Profile Publish (From Console)
awrestrictionslistsample	iOS Restrictions List Samples (From Device)
awsbrowserinformationsample	Browser Information Sasmple (Windows 8 Devices only)
awsecurityinformationsample	iOS Security Information Samples (From Device)
awsegcompliance	Compliance Information for SEG
awsegfastcompliance	MEM High Priority Compliance Commands
awsmartgroupevent	Data for Monitoring User Group Change Events
awsmslogsample	Android/BlackBerry/WinMo SMS Log Samples (From Device)
awswindowsinformationsample	Windows Information Sample (Windows 8 Devices only)
awswindowsrestrictionsample	Restriction Setting Sample (Windows 8 Devices only)
awsystemsample	Android/BlackBerry/iOS/WinMo Device/System Information Samples (From Device)
awtomagoutboundqueue	Queues message to be sent to MAG via AWCM
awtunnel	WinMo Tunnel Server (From Tunnel Server)
awuserbatchqueue	AirWatch User Batch Queue
awwnsnotification	Windows Notification Service (WNS) Noifications
c2dmoutbound	Android Outbound C2DM Messages

Message Queues	Description
fastlaneapnsoutbound	Admin initiated iOS and GCM Outbound APNs Messages
gcmoutbound	Android Google Cloud Messaging Outbound
sensorchangequeue	Sensor Change Queue
workflow-devicecommands	Workflow – Device Commands

Appendix: Error Handling for AirWatch Components

The following sections list out the error codes or messages for the major AirWatch components. You can use these error codes and message to better monitor your AirWatch deployment.

AirWatch Cloud Connector

Error Type	Error Message	Followed by Exception?
Start-up	Cannot read configuration	Yes
Start-up	AccIdentifier is missing	No
Start-up	AwIdentifier is missing	No
Start-up	AwcmUrl is invalid: {AwcmUrl}	Yes
Start-up	Unable to load the certificate with thumbprint	Possibly
Start-up	Configuration specifies to use a proxy, but no proxy address is provided	No
Start-up	Invalid proxyAddress	Yes
Start-up	Cannot decrypt the proxy password using the ACC certificate	Yes
Start-up	Error while starting listener tasks	Yes
Shut down	All listener thread have terminated; killing application	No
Shut down	Attempt to stop background tasks timed out; killing application	No
Shut down	Error when canceling background tasks	Yes
Update	Update check delay was interrupted by an exception	Yes
Update	Unable to check for update with {AutoUpdateUrl}	Yes
Update	Update returned an error: {ErrorMessage}	No
Update	The application needs update, but no update file was sent	No
Update	Failed to write the update file	Yes
Update	Unable to verify the update file signature	Yes
Update	Update file was signed by an unexpected certificate: {InfoAboutSigningCert}	Yes
Update	Unable to rename the update file to remove the .untrusted extension	Yes
Update	Error while checking for or performing update; cannot ensure the service is up-to-date.	Yes
Update	Cannot delete old file: {FilePath}	No
Update	Cannot delete old folder: {FolderPath}	No

Error Type	Error Message	Followed by Exception?
Update	Failed to repair the new configuration file after an upgrade; download a new installer to upgrade	Yes
Update	Cannot continue without a valid configuration; please download the Cloud Connector installer	No
Update	Error unloading old AppDomain {Name}	Yes
Update	It appears that we ran the same version after update	No
Update	Error invoking AirWatch.CloudConnector.DiagnosticService.IComponentUpdater:Check via AWCM({UpdateUrl}): Timeout after 120 seconds	Yes
Update	Error reaching AWCM({UpdateUrl}) to invoke AirWatch.CloudConnector.DiagnosticService.IComponentUpdater:Check: {Reason}	Yes
Update	Received a Failure message from AWCM: {ErrorMessage}	Yes
Update	Received an error response to AirWatch.CloudConnector.DiagnosticService.IComponentUpdater:Check: {ErrorMessageFromConsole}	Yes
Update	Update check is bypassed. AirWatch Cloud Connector is configured to bypass its check for updates; THIS CONFIGURATION IS UNSUPPORTED!It is important to keep ACC up-to-date! Please remove the 'bypassUpdate' attribute from the .config file ASAP.	Yes
Update	Update check failed to complete. AirWatch Cloud Connector received a notice to check for an update, but it was unable to do so. The component may be out-of-date; THIS CONFIGURATION IS UNSUPPORTED! Please resolve the issue and restart the service to retry the update check.	Yes
Update	This version is out-of-date. AirWatch Cloud Connector is out-of-date with the latest installer; THIS CONFIGURATION IS UNSUPPORTED! Installed Version: {LocalVersion};Current Version: {ServerVersion} An update is required, but the AutoUpdate feature is disabled in the Console; you must update ACC manually. Please upgrade as soon as possible. For your convenience, the update package has been downloaded to{PathToDownloadedZip} Unzip its contents into {PathToInactiveBank}and restart the service. Or if you prefer, obtain a new installer through the AirWatch Web Console.	Yes

Error Type	Error Message	Followed by Exception?
Runtime	ACC Listener Task faulted with state {Reason}; {Action}. {Reason} = Unknown, CannotConnect, SecurityError, Disconnected, Timeout, Canceled, SerializingError, SecuringError,DeserializingError, ProcessingError, ReceivedFailure, InvalidResponse, ErrorResponse {Action} = retrying now; retrying in X seconds; exiting	Yes
Runtime	Failed to process a received message	Yes
Runtime	Cannot read request: ({ExceptionType}) {ExceptionMessage}	Yes
Runtime	Cannot create service instance: ({ExceptionType}) {ExceptionMessage}	Yes
Runtime	Exception from service operation: ({ExceptionType}) {ExceptionMessage}	Yes
Runtime	Reply task terminated with exception	Yes
Runtime	Reply resulted in {NumberNot1} results from AWCM	No
Runtime	Reply resulted in a {AwcmMessageTypeNotSuccess} result from AWCM	No
Runtime	Error processing service result.	Yes

Mobile Access Gateway

Code	Name	Meaning
0	UNKNOWN	A runtime exception while processing the request
1	MISSING_HEADER	Proxy-Authorization header is missing
2	WRONG_ENCODING	Proxy-Authorization header value is not Base64 encoded
3	TOKENS_DONT_MATCH	Client identification tokens in Proxy-Authorization header don't follow *alg:%s;uid:%s;bundleid:%s* format
4	INVALID_ALGO	The algorithm in the Proxy-Authorization token is not supported
5	EMPTY_CERT_CHAIN	There is no certificate present in the digital signature passed in the Proxy-Authorization header
6	SINGLE_SIGNER	The request is expected to be signed by only one entity
7	SINGLE_SIGNER_CERT	The request signer should sign it with only one certificate
8	INVALID_SIGN	The signer information couldn't be verified
9	UNTRUSTED_ISSUER	The certificate used for signing wasn't issued by Device-Root of the given OG
10	MISSING_SIGN_TIME	The signing time attribute which is used to determine potential replay attack is missing in the signature
11	POTENTIAL_REPLAY	There is more than a 15 minute interval between signature creation by the requester (AW Browser, Wrapping, etc) and verification by MAG

Code	Name	Meaning
12	INVALID_SIGN_DATA	There is discrepancy in the data that was signed by the requester (AW Browser, Wrapping, etc) and what was expected to be signed by MAG
13	DATA_UNAVAILABLE	The requester's (AW Browser, Wrapping, etc) related data is not available with MAG even after making an API call
14	INVALID_THUMBPRINT	The thumbprint of the certificate used by the requester (AW Browser, Wrapping, etc) for signing and the one expected by MAG is different
15	NOT_COMPLIANT	The device making the request is not compliant (Must be in compliance states of 'Compliant' or 'Not Available')
16	NOT_MANAGED	The device is not managed by AirWatch
17	INVALID_CERT	The certificate used by the requester (AW Browser, Wrapping, etc) for signing is not valid (ex. signing time does not fall in the certificate lifetime)
18	NEED_CHUNK_ AGGREGATION	Chunk aggregation is not enabled in MAG.properties file
19	HOST_DISCREPANCY	Host name in the URI does not match the one in the host header, deemed as a potential replay attack

Secure Email Gateway

Error Code ID	Component	Area	Message
SEG-11001	Integration Service	Application Infrastructure	SocketException getting host name
SEG-11002	Integration Service	Application Infrastructure	Exception getting host name
SEG-11003	Integration Service	Application Infrastructure	Unable to read mobileEmailGatewayConfiguration section from config file
SEG-11004	Integration Service	Application Infrastructure	Error stopping Event Processor
SEG-11005	Integration Service	Server / Network	AirWatchLoggedServiceException encountered while executing {0} .Â Id: {1}
SEG-11006	Integration Service	Server / Network	AirWatchServiceException encountered while executing {0} .Â ErrorCode: {1}, Message: {2}
SEG-11007	Integration Service	Server / Network	CallContextException encountered while while executing {0} .Â Id: {1}, ServiceName: {2}, OperationName: {3}, Message: {4}
SEG-11008	Integration Service	Server / Network	CommunicationException encountered while while executing
SEG-11009	Integration Service	Server / Network	TimeoutException encountered while while executing

Error Code ID	Component	Area	Message
SEG-11010	Integration Service	Server / Network	Exception encountered while while executing
SEG-11011	Integration Service	Server / Network	Error getting general access policy
SEG-11012	Integration Service	Server / Network	Error getting account policies
SEG-11013	Integration Service	Server / Network	Error getting mail client policies
SEG-11014	Integration Service	Server / Network	Error getting EAS device type policies
SEG-11015	Integration Service	Server / Network	Error getting sync filters policies
SEG-11016	Integration Service	Server / Network	Error getting device policies
SEG-11017	Integration Service	Server / Network	Cannot retrieve managed attachment policy
SEG-11018	Integration Service	Server / Network	Error getting managed attachment policy
SEG-11019	Integration Service	Server / Network	Cannot retrieve unmanaged attachment policy
SEG-11020	Integration Service	Server / Network	Error getting unmanaged attachment policy
SEG-11021	Integration Service	Server / Network	Error getting encryption key data
SEG-11022	Integration Service	Server / Network	Error getting impersonation credentials
SEG-11023	Integration Service	Server / Network	Error getting emailSecurityTagPolicy
SEG-11024	Integration Service	Application Infrastructure	Error validating ActiveSync request. DefaultAllowActiveSyncRequest is set to {0}.
SEG-11025	Integration Service	Server / Network	Cannot reach airwatch service(API) server
SEG-11026	Integration Service		Sync Filters policies do not exist in cache
SEG-11027	Integration Service	Policy Cache	Attachment policies do not exist in cache for EAS identifier '{0}'

Error Code ID	Component	Area	Message
SEG-11028	Integration Service	Policy Cache	Encryption key data does not exist in cache for EAS identifier '{0}'
SEG-11029	Integration Service	Policy Cache	Encryption key data does not exist in cache for unmanaged devices. EAS identifier '{0}'
SEG-11030	Integration Service	Application Infrastructure	Error loading Gateway Settings from app config.Â Using internal defaults
SEG-11031	Integration Service	Application Infrastructure	Cannot decrypt the existing password
SEG-11032	Integration Service	Application Infrastructure	Configuration file, {0}, does not exist
SEG-11033	Integration Service	Application Infrastructure	Failed to load settings on service start
SEG-11034	Integration Service	Application Infrastructure	Became Master node, but failed to load settings or start PolicyManager
SEG-11035	Integration Service	Application Infrastructure	Service host faulted. Restarting....
SEG-12001	Gateway Module	Request Handling	Error encountered decoding user name
SEG-12002	Gateway Module	Request Handling	Error encountered decoding password
SEG-12003	Gateway Module	Request Handling	Error encountered encoding authentication header
SEG-12004	Gateway Module	Request Handling	Exception replacing auth header
SEG-12005	Gateway Module	Request Handling	BeginRequest sender is null
SEG-12006	Gateway Module	Request Handling	Unhandled exception encountered in BeginRequest
SEG-12007	Gateway Module	Request Handling	AuthenticateRequest sender is null
SEG-12008	Gateway Module	Request Handling	Unhandled exception encountered in AuthenticateRequest
SEG-12009	Gateway Module	Request Handling	EndRequest sender is null
SEG-12010	Gateway Module	Request Handling	Unhandled exception encountered in EndRequest

Error Code ID	Component	Area	Message
SEG-12011	Gateway Module	Request Handling	ModifyResponseHeaders sender is null
SEG-12012	Gateway Module	Request Handling	Unhandled exception encountered in ModifyResponseHeaders
SEG-12013	Gateway Module	Request Handling	Proxy operation failed.Â HttpException - Status: '{0}', ExMessage: '{1}'
SEG-12014	Gateway Module	Authentication	Client certificate is not valid.Â Ensure the Certificate Authority is trusted
SEG-12015	Gateway Module	Authentication	Client certificate is not yet valid. ValidFrom date: {0}
SEG-12016	Gateway Module	Authentication	Client certificate is expired. ValidUntil date: {0}
SEG-12017	Gateway Module	Authentication	Could not retrieve Kerberos token
SEG-12018	Gateway Module	Request Handling	Exception processing 451 redirect response. Response StatusCode: 400 BadRequest. RequestTid: '{0}'
SEG-12019	Gateway Module	Application Infrastructure	Unable to check event bypass condition
SEG-12020	Gateway Module	Content Transform	Properties of attachment causing exception : '{0}'
SEG-12021	Gateway Module	Content Transform	Base64 attachment string causing exception : '{0}'
SEG-12022	Gateway Module	Content Transform	Base64 format exception occurred while decoding attachment. Attachment will be removed. Filename: '{0}'
SEG-12023	Gateway Module	Content Transform	Base64 string causing exception : '{0}'
SEG-12024	Gateway Module	Content Transform	Unable to decode WBXML: '{0}'
SEG-12025	Gateway Module	Content Transform	Unable to get bytes from hex
SEG-12026	Gateway Module	Server / Network	SocketException encountered while {0}(descriptor) {1} (commDirectionText). Socket read error: {2}(Error Code): {3}(Exception Message). Terminating client connection.
SEG-12027	Gateway Module	Server / Network	IOException encountered while {0}(descriptor) {1}(commDirectionText). Underlying socket is closed. Terminating client connection.
SEG-12028	Gateway Module	Server / Network	WebException encountered while '{0}'(descriptor) '{1}' (commDirectionText).Â WebExStatus: '{2}', RequestTid: '{3}', Status Code: '{4}', Status Description: '{5}', ExMessage: '{6}'

Error Code ID	Component	Area	Message
SEG-12029	Gateway Module	Server / Network	WebException inner IOException indicates connection failure. Terminating client connection.
SEG-12030	Gateway Module	Server / Network	WebException status ({0}) indicates connection failure. Terminating client connection.
SEG-12031	Gateway Module	Server / Network	WebException status ({0}) indicates endpoint could not be found or could not be resolved. Sending 400 BadRequest to client.
SEG-12032	Gateway Module	Server / Network	WebException status ({0}) indicates maximum request length exceeded. Sending 400 BadRequest to client.
SEG-12033	Gateway Module	Server / Network	WebException status ({0}) indicates unknown error. Sending 400 BadRequest to client.
SEG-12034	Gateway Module	Server / Network	ThreadAbortException encountered while {0}(descriptor) {1}(commDirectionText). Response StatusCode: 400 BadRequest for non-ping requests.Check httpRuntime executionTimeout setting in the Listener web.config. It should be set higher than the easRequestTimeOut setting.
SEG-12035	Gateway Module	Server / Network	HttpException encountered while {0}(descriptor) {1}(commDirectionText). Error Code: {2}, WebEventCode: {3}, Status Code: {4}, Status Message: {5}
SEG-12036	Gateway Module	Server / Network	Exception encountered while {0}(descriptor) {1}(commDirectionText). Response StatusCode: 400 BadRequest
SEG-13001	SEG Console	Server / Network	A SSL error occurred with the following message: {0}
SEG-13002	SEG Console	Server / Network	Error ping Airwatch Service: {0}
SEG-14001	SEG Setup	Server / Network	AirWatchFaultException encountered.Â ActivityId: '{0}'
SEG-14002	SEG Setup	Server Configuration	Fail to set KCD authentication configuration with exception : {0}
SEG-14003	SEG Setup	Server Configuration	Fail to create web application for lotus notes with exceptionï¼š {0}
SEG-14004	SEG Setup		Unable to save configuration
SEG-14005	SEG Setup	Server / Network	Error closing HttpWebResponse
SEG-14006	SEG Setup	Setup Validation	URL is empty
SEG-14007	SEG Setup	Setup Validation	The email server's name is empty

Error Code ID	Component	Area	Message
SEG-14008	SEG Setup	Server Configuration	Unable to read XML settings file \"{0}\". Moving it so we don't try again
SEG-14009	SEG Setup	Server Configuration	Failed to rename the file; this error will likely occur again
SEG-14010	SEG Setup	Server Configuration	Configuration file, {0}, does not exist
SEG-14011	SEG Setup	Server Configuration	Unable to create user:'{0}'. Please check Password Policies and Directory Service permissions.
SEG-14012	SEG Setup	Server Configuration	Unable to read XML file \"{0}\". Moving it so we don't try again.
SEG-14013	SEG Setup	Server Configuration	An error occured while attempting to make '{0}' writable
SEG-15001	SEG Cluster		Exception when processing received message message to application {0} from node {1}
SEG-15002	SEG Cluster		Ignoring heartbeat packet from unknown source {0} with {1} bytes
SEG-15003	SEG Cluster		Received invalid heartbeat packet from {0} with {1} bytes
SEG-15004	SEG Cluster		Failed to process received application message
SEG-15005	SEG Cluster		JoinQuery error from {0}: {1}
SEG-15006	SEG Cluster		Invalid response to JoinQuery: {0}
SEG-15007	SEG Cluster		JoinResponse error from {0}: {1}
SEG-15008	SEG Cluster		Invalid response to JoinRequest: {0}
SEG-15009	SEG Cluster		Failed to join Cluster '{0}', stopping
SEG-15010	SEG Cluster		Received ReconnectNow message from node not in the cluster; ignoring
SEG-15011	SEG Cluster		Master reports it is shutting down; blocking app messages until we have a new one.
SEG-15012	SEG Cluster		Unable to update directory using provider {0}
SEG-15013	SEG Cluster		Failed to send to {0}

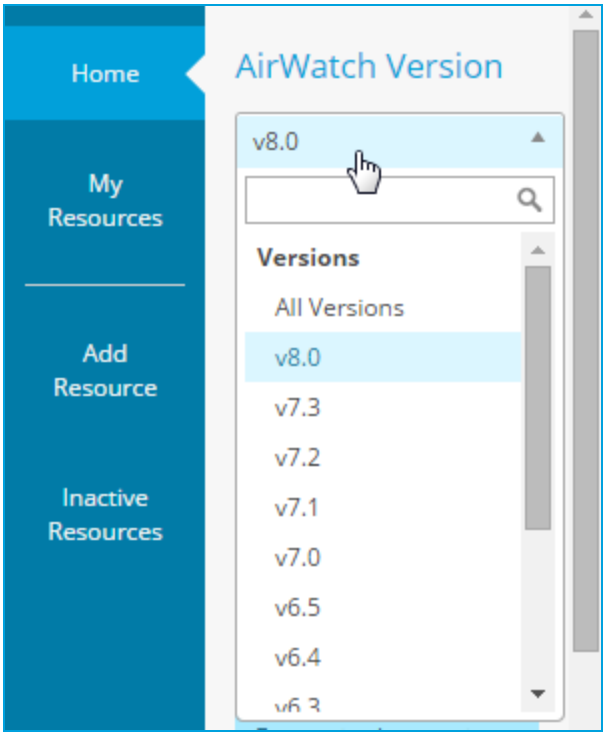
Finding Additional Documentation

While reading through this documentation you may encounter topics that reference other documents that are not included here. You may also be looking for separate documentation that is not a part of this resource. You can access this additional documentation through the AirWatch Resources page (https://resources.air-watch.com) on myAirWatch.

Note: It is always recommended you pull the document from AirWatch Resources each time you need to reference it.

To search for and access additional documentation via the AirWatch Resources page, perform the following step-by-step instructions:

1. Navigate to http://my.air-watch.com and log in using your AirWatch ID credentials.
2. Select **AirWatch Resources** from the navigation bar or home screen. The AirWatch Resources page displays with a list of recent documentation and a list of Resources Categories on the left.
3. Select your AirWatch Version from the drop-down list in the search parameters to filter a displayed list of documents. Once selected, you will only see documentation that pertains to your particular version of AirWatch.



4. Access documentation using the following methods:
   - Select a resource category on the left to view all documents belonging to that category. For example, selecting **Documentation** filters your search to include the entire technical documentation set. Selecting **Platform** filters your search to only include platform guides.
   - Search for a particular resource using the search box in the top-right by entering keywords or document names.
   - Add a document to your favorites and it will be added to **My Resources**. Access documents you have favorited by selecting **myAirWatch** from the navigation bar and then selected My Resources from the toolbar.

- Download a PDF of a document by selecting the button. Note, however, that documentation is frequently updated with the latest bug fixes and feature enhancements. Therefore, it is always recommended you pull the document from AirWatch Resources each time you need to reference it.

Having trouble finding a document? Make sure a specific **AirWatch Version** is selected. **All Versions** will typically return many results. Make sure you select **Documentation** from the category list, at a minimum. If you know which category you want to search (e.g., **Platform**, **Install & Architecture**, **Email Management**) then selecting that will also further narrow your search and provide better results. Filtering by **PDF** as a **File Type** will also narrow your search even further to only include technical documentation manuals.