vmware airwatch

VMware AirWatch Recommended Architecture Guide

Setting up and managing your on-premises AirWatch deployment

Workspace ONE UEM v9.4

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.workspaceone.com/.

Table of Contents

Chapter 1:
Overview

Introduction to Workspace ONE UEM Recommended Architecture

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

Every on-premises deployment of Workspace ONE UEM 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 Workspace ONE UEM, it is up to your organization to decide how best to implement certain features such as high availability or disaster recovery. VMware AirWatch can provide guidance for your specific deployment. Contact Workspace ONE Support for more details.

Chapter 2:
Topology

AirWatch Topology Overview

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

Workspace ONE UEM Console

Administrators use the Workspace ONE UEM console through a 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 Workspace ONE UEM that actively communicate with devices. Workspace ONE 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.

AirWatch Cloud Messaging (AWCM)

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

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

AWCM is typically installed on the Device Services server for deployments up to 50,000 devices.

AWCM simplifies device management by offering the following benefits:

- Enabling secure communication to your back-end infrastructure through the VMware Enterprise Systems Connector.
- Enabling AirWatch Unified Windows Agent real-time communication.
- Removing the need for third party IDs.
- Delivering Workspace ONE UEM console commands directly to Android and Windows Rugged devices.
- Enabling the ability for remote control and file management on Android Samsung Approved for Enterprise (SAFE) and Windows Rugged devices.

- Enabling the ability to send remote commands such as device wipe and device lock to macOS and Windows 7 devices.
- Increasing the functionality of internal Wi-Fi only devices by enabling push notification in certain circumstances.

Additional information about AWCM requirements, setup and installation can be found in the **VMware AirWatch AWCM Guide**, available on docs.vmware.com.

API

The AirWatch API component comprises REST (Representational State Transfer) and SOAP (Simple Object Access Protocol) APIs. These APIs are used for developers creating their own applications that wish to invoke AirWatch functionality and utilize the information stored in their AirWatch environment.

When developing any new applications, AirWatch recommends the use of Version 2 of the REST API, both for ease of use and for optimal support long-term.

SQL Database

Workspace ONE UEM 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.

For more information on system configurations, see the **Workspace ONE UEM Installation Guide**, available on docs.vmware.com, or consult with your Workspace ONE representative.

VMware Identity Manager Service

VMware Identity Manager provides identity-based services for the Workspace ONE UEM solution, including:

- Application provisioning
- Self-service catalog
- Conditional access controls
- Single Sign-On functionality

VMware Enterprise Systems Connector

VMware Enterprise Systems Connector provides organizations the ability to integrate AirWatch and VMware Identity Manager with their back-end enterprise systems. VMware Enterprise Systems Connector runs in the internal network, acting as a proxy that securely transmits requests from AirWatch and VMware Identity Manager to critical enterprise infrastructure components. This allows organizations to harness the benefits of AirWatch Mobile Device Management (MDM) and VMware Identity management, together with those of their existing LDAP, certificate authority, email, and other internal systems.

VMware Enterprise Systems Connector 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-premises only)
- Lotus Domino Web Service (HTTPS)
- Syslog (Event log data)
- Horizon
- RSA

Additional information about VMware Enterprise Systems Connector requirements, setup, and installation can be found in the **VMware Enterprise Systems Connector Guide, available at https://www.vmware.com/support/pubs/workspaceone-pubs.html**.

AirWatch Secure Email Gateway (Classic and V2)

Enterprises using certain types of email servers, such as Exchange 2010 or Lotus Traveler, can use the **AirWatch Secure Email Gateway (SEG)** server 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 existing ActiveSync endpoint.

AirWatch Secure Email Gateway offers advanced email management capabilities:

- 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 and hyperlink transform.

Enterprises using Exchange 2010+, Office 365 BPOS, or Google Apps for Work do not necessarily require 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.

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

Additional information about SEG requirements, setup, and installation can be found in the **VMware AirWatch SEG Administration Guide**, available on docs.vmware.com.

VMware Tunnel and Unified Access Gateway (Tunnel)

The VMware Tunnel 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 VMware Tunnel acts as a secure

relay between the device and enterprise system. The VMware Tunnel can authenticate and encrypt traffic from individual applications on compliant devices to the back-end site or resources they are trying to reach.

Use the VMware Tunnel to access:

- Internal websites and Web applications using the VMware Browser.
- Internal resources through app tunneling for iOS 8 and higher devices using the VMware Tunnel.

Additional information about AirWatch Tunnel requirements, setup, configuration, and installation can be found in the **VMware Tunnel Guide**, available on docs.vmware.com.

AirWatch Content Gateway and Unified Access Gateway (Content Gateway)

The Content Gateway, together with VMware Content Locker, lets your end users securely access content from an internal repository. This means that your users can remotely access their documentation, financial documents, board books, and more directly from content repositories or internal file shares. As files are added or updated within your existing content repository, the changes will immediately be reflected in VMware Content Locker, and users will only be granted access to their approved files and folders based on the existing access control lists defined in your internal repository. Using the Content Gateway with VMware Content Locker allows you to provide unmatched levels of access to your corporate content without sacrificing security.

Additional information about AirWatch Content Gateway requirements, setup, configuration, and installation can be found in the **VMware AirWatch Content Gateway Admin and Install guides**,available on docs.vmware.com.

AirWatch Email Notification Service (Classic and V2)

The Email Notification Service (ENS) adds Apple Push Notification support to Exchange. On iOS, this means the VMware Boxer and VMware AirWatch Inbox email apps can get notifications utilizing either Apple's background app refresh or Apple Push Notification Service (APNs) technologies. Background app refresh is used by default, however iOS attempts to balance the needs of all apps and the system itself. This means that each app may provide notifications at irregular periods using this method. To provide notifications quickly and consistently, Apple also provides APNs. This allows a remote server to send notifications to the user for that application, however Exchange does not natively support this. ENS adds APNs support to your deployment to allow quick and consistent notifications about new items in your end users' email inboxes.

You can download the most up-to-date versions of the **VMware AirWatch Email Notification Service Installation Guides**, which includes configuration and installation, from docs.vmware.com.

Workspace ONE Intelligence

Workspace ONE Intelligence gives you insights into your digital workspace. It enables enterprise mobility management (EMM) planning and offers automation. All these components help to optimize resources, to strengthen security and compliance, and to increase user experience across your entire environment.

You can download the most up-to-date version of the **Workspace ONE Intelligence Guide**, which includes configuration and installation, from docs.vmware.com.

Adaptiva

Workspace ONE UEM offers a peer distribution system to deploy Win32 applications to enterprise networks. Peer distribution can reduce the time to download large applications to multiple devices in deployments that use a branch office structure.

For more information, see the **VMware AirWatch Mobile Application Management (MAM) Guide**, which includes configuration and installation, from docs.vmware.com.

Memcached

As deployments begin to scale over 5,000 devices, it is recommended that all environments have a caching solution in place. Caching solutions aid in reducing load on the database server that comes from the sheer volume of calls that need to be made to the database. Once caching is configured, the AirWatch components will first reach out to the caching solution in attempts to obtain the DB information they require. If the information that is needed does not reside on the cache server, the component will reach out to the DB and subsequently store the value on the cache server for future use.

For more information on configuring Memcached please see the **Memcached Integration with AirWatch** guide, available on docs.vmware.com. If the Memcached setting is not available, please reach out to Workspace ONE Support for assistance.

Workspace ONE UEM On-Premises Deployment Model

When deployed within a network infrastructure, Workspace ONE UEM can adhere to strict corporate security policies by storing all data onsite. In addition, Workspace ONE UEM has been designed to run on virtual environments, which allows for seamless deployments on several different setups.

Workspace ONE UEM can be deployed in various configurations to suit diverse business requirements. In a standard Workspace ONE UEM deployment you can use a multiple servers deployment model and deploy any of the Workspace ONE UEM components on dedicated or shared servers. The primary difference between deployment sizes (by number of devices) is how Workspace ONE UEM components (UEM console, Device Services, AWCM, Database Server, Secure Email Gateway, VMware Enterprise Systems Connector, and VMware Tunnel) are grouped, and how they are positioned within the corporate network. The Workspace ONE UEM solution is highly customizable to meet your specific needs. If necessary, contact Workspace ONE Support to discuss the possible server combinations that best suit your needs. For more information on hardware sizing, see Hardware Sizing.

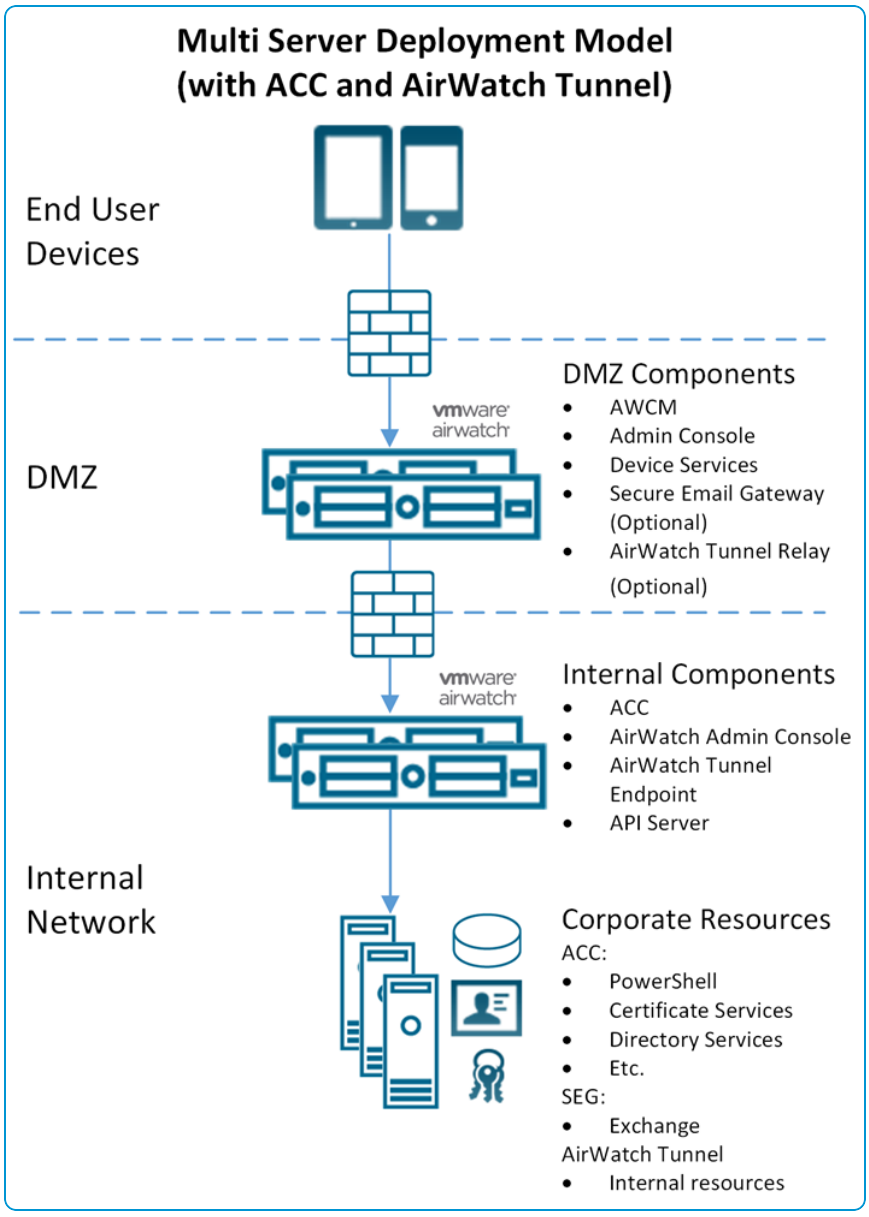
Most typical Workspace ONE UEM topologies support reverse proxies. A reverse proxy can be used to route incoming traffic from devices and users on the Internet to the Workspace ONE UEM servers in your corporate network. Supported reverse proxy technologies include: Bluecoat, Microsoft, F5 Networks, IBM,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

For more information about configuring reverse proxies with Workspace ONE UEM, see the following Workspace ONE UEM Knowledge Base article: https://support.air-watch.com/articles/115001665868.

Standard Deployment Model

In a standard Workspace ONE UEM deployment you will use multiple servers for the various components. If desired, you can use 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 Workspace ONE UEM components. The following diagrams illustrate how to use VMware Enterprise Systems Connector and VMware Tunnel in an on-premises environment.

While these components are combined in the diagrams for illustrative purposes, they can reside on a dedicated server. Many configuration combinations exist and may apply to your particular network setup. For a detailed look at these configurations based on deployment size, see Hardware Sizing. Contact Workspace ONE Support and schedule a consultation to discuss the appropriate server configuration for your on-premises deployment.



Chapter 3:
Hardware Sizing

On-Premises Recommended Architecture Hardware Sizing Overview

When determining the hardware specifications needed to build out a Workspace ONE UEM 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 Workspace ONE UEM must manage. It may also be beneficial to consider the growth potential of the organization's device fleet .

The sizing recommendations listed are written against device transaction data gathered from Workspace ONE UEM Cloud deployments. Sizing for a Workspace ONE UEM environment begins with an initial assessment of critical factors to provide a clear view of system use. Workspace ONE UEM continually conducts performance testing to validate sizing requirements and as such the figures listed in this section may change over time.

On-Premises Architecture Sizing for up to 5,000 and 25,000 Devices

Use the table to determine the sizing recommendations for a deployment of up to 25,000 devices. Each column represents the recommended specs for a deployment up to that number of devices. The columns are not cumulative – each column contains the recommended specs for the listed number of devices.

Consider the following figures as starting points. You may need to adjust them as you implement different features of the Workspace ONE UEM solution. Transaction frequency, number of concurrent connections, and other metrics affect performance, and you may need to tweak the numbers to accommodate your specific deployment. Contact Workspace ONE Support if you require extra assistance.

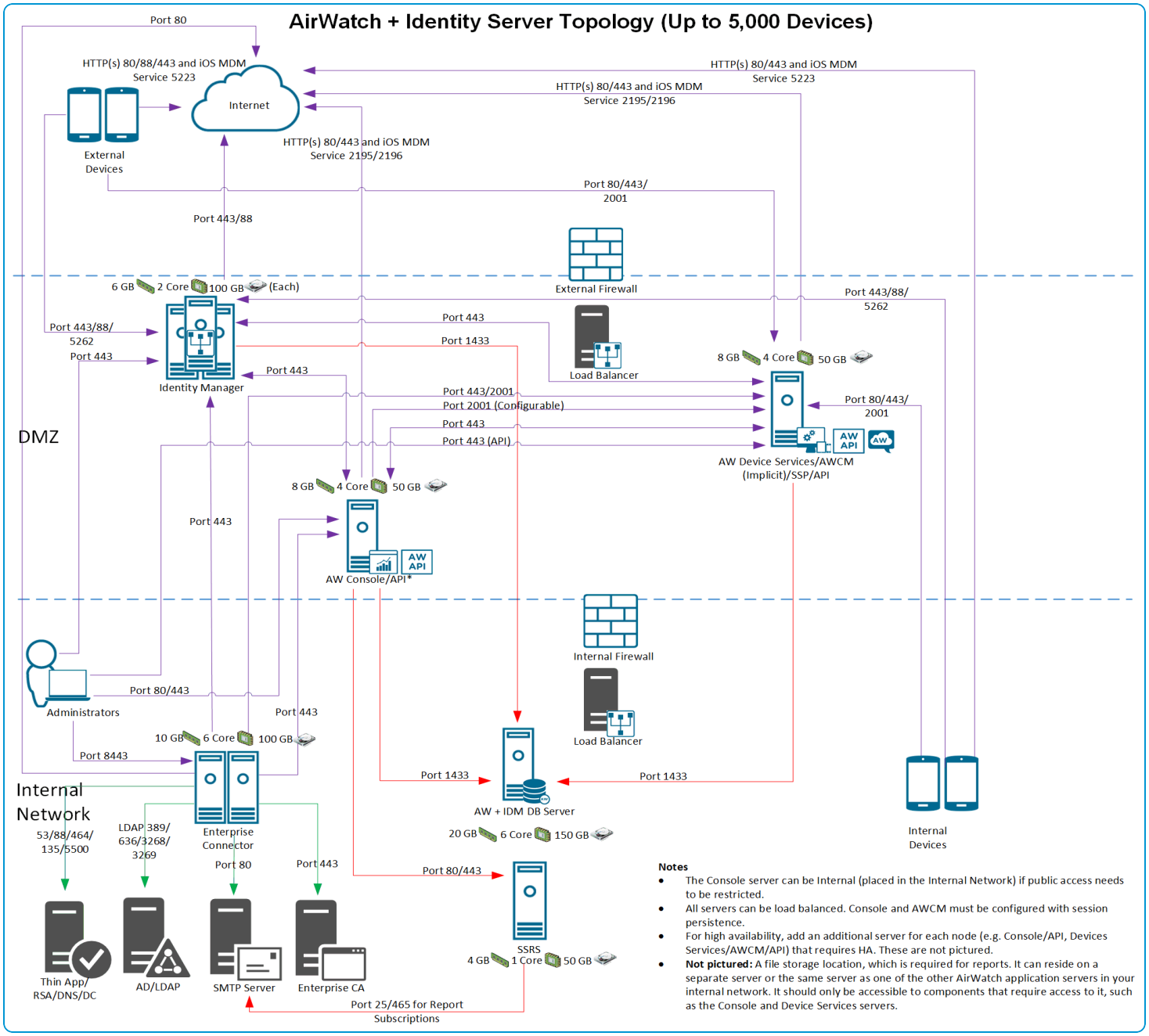
Additional notes to consider:

- Certain SQL versions have a maximum supported RAM limit, so review your SQL version's RAM limitation to ensure that all hardware functions as intended.
- Load balancing for application servers is provided by the customer.
- The file storage requirement for reports may affect the amount of hard disk space needed on the Console and Device Services servers, depending on whether you enable caching. See Reports Storage Requirements on page 30 for more information.

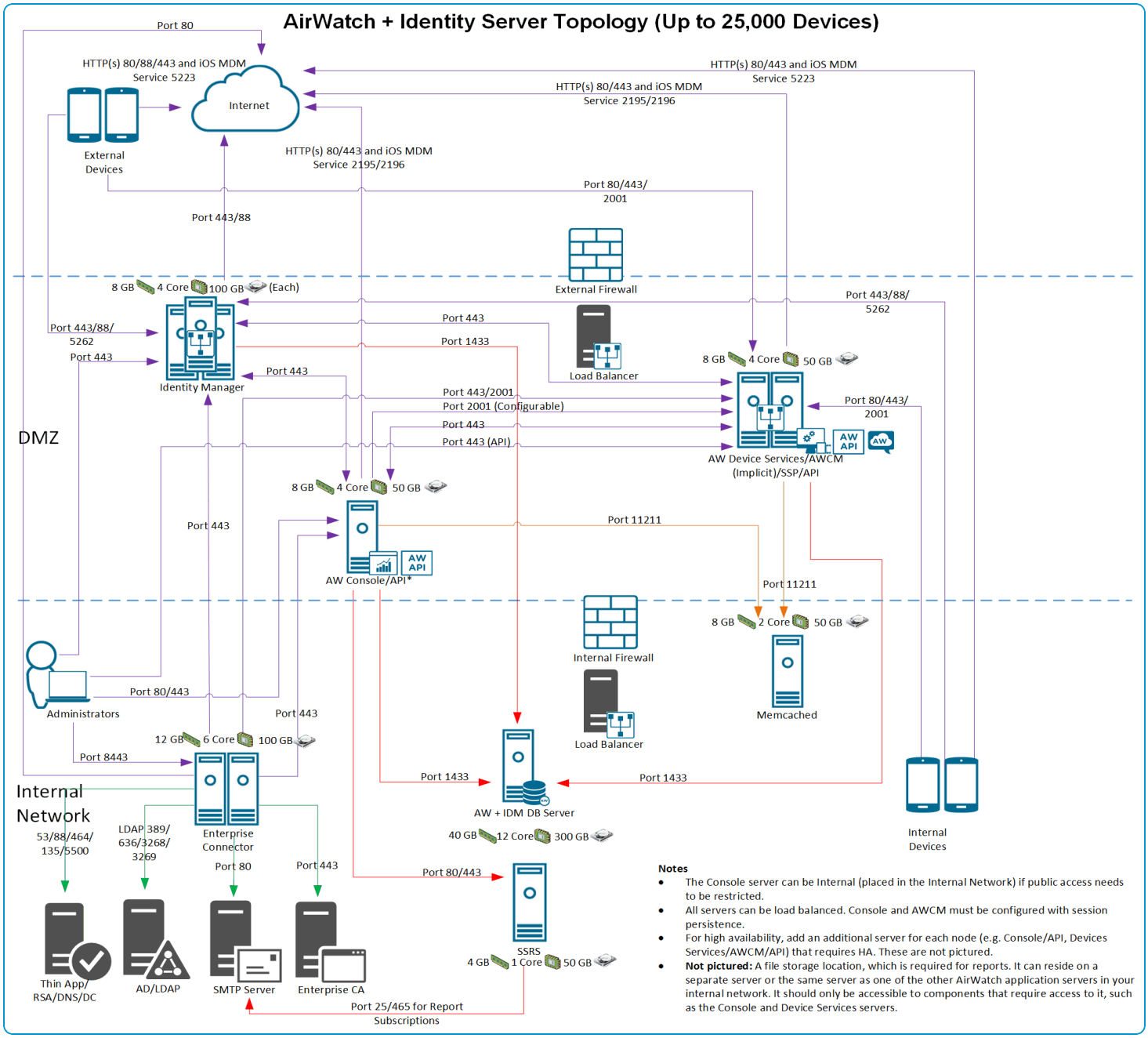
		Up to 5,000 Devices	Up to 25,000 Devices
Database Server	CPU Cores	4	8
	RAM (GB)*	16	32
	DB Size (GB)	100	250
	Trans Log Size (GB) (Log backups every 15 minutes)	40	100
	Temp DB (GB)	40	100
	Avg IOPS (DB & Temp DB)	150	750
	Peak IOPS (DB & Temp DB)	300	1500
UEM console (includes API component) Refer to **AirWatch API Endpoint Installation**.		1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage	1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage
Device Services with AWCM (includes API component) Refer to **AirWatch API Endpoint Installation**.		1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage	2 load-balanced application servers, each with: 4 CPU cores, 8 GB RAM, and 50 GB storage
Reporting Server (SSRS)		1 reporting server with 1 CPU core, 4 GB RAM, and 50 GB storage	
VMware Identity Manager Service		See VMware Identity Manager Service Hardware Sizing	
VMware Enterprise Systems Connector		See VMware Enterprise Systems Connector Server Hardware Sizing	
SEG Proxy Server		See Secure Email Gateway Server Hardware Sizing	
VMware Tunnel		See VMware Tunnel Server Hardware Sizing	
Email Notification Service		See Email Notification Service Hardware Sizing	
Content Gateway		See Content Gateway Hardware Sizing	
Workspace ONE Intelligence		See Workspace ONE Intelligence on page 30	
Adaptiva		See Adaptiva on page 30	

Important: For application servers, a 64-bit dual core Intel processor is required.

Server Sizing Topology (Up to 5,000 Devices)



Server Sizing Topology (Up to 25,000 Devices)



On-Premises Architecture Sizing for up to 50,000 Devices

Use the table to determine the sizing requirements for a deployment of up to 50,000 devices. Each column represents the requirements for a deployment up to that number of devices. The columns are not cumulative – each column contains the exact requirements for the listed number of devices.

Consider the following figures as starting points. You may need to adjust them as you implement different features of the Workspace ONE UEM solution. Transaction frequency, number of concurrent connections, and other metrics affect performance, and you may need to tweak the numbers to accommodate your specific deployment. Contact Workspace ONE Support if you require extra assistance.

Additional notes to consider:

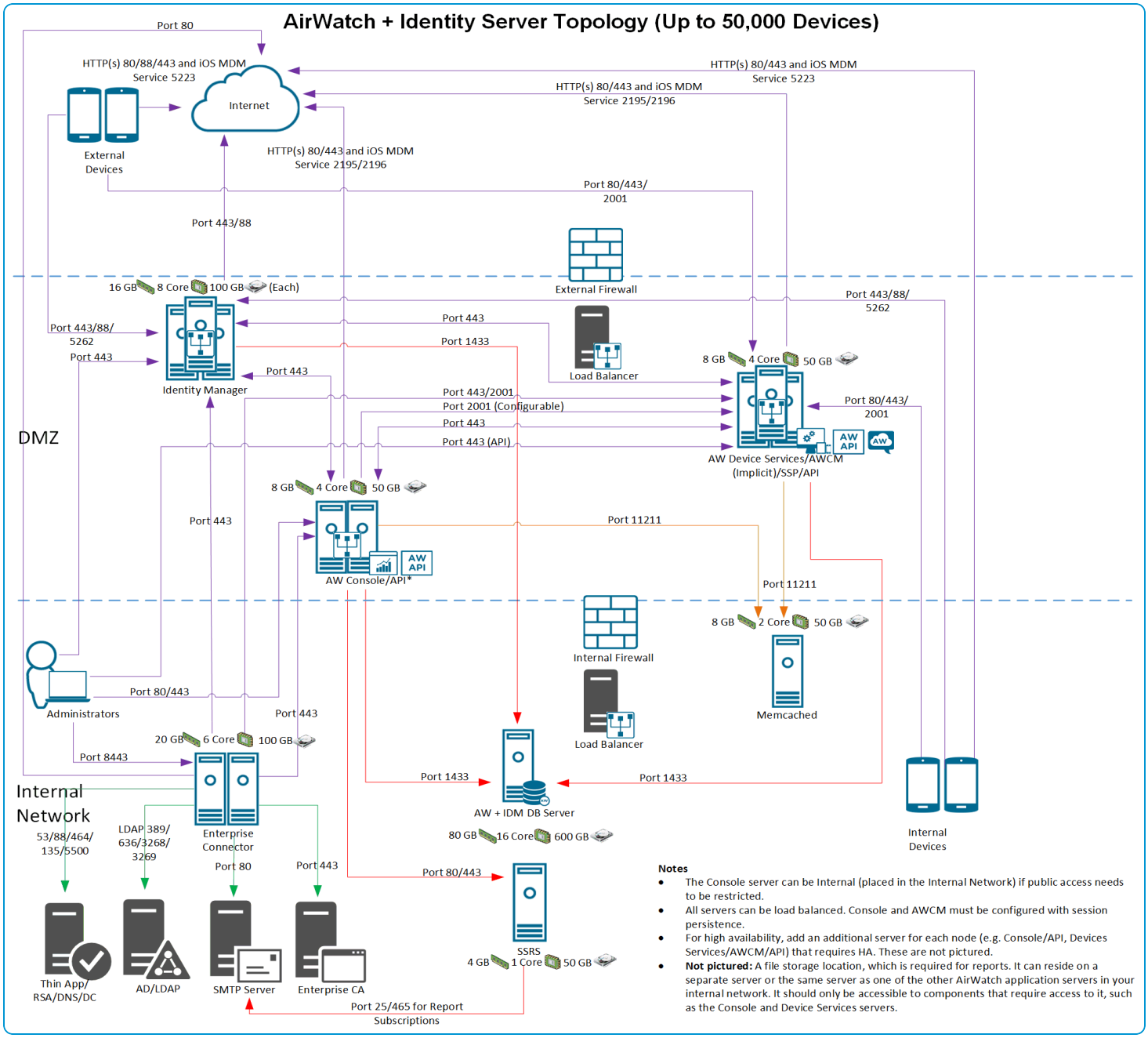
- Certain SQL versions have a maximum supported RAM limit, so review your SQL version's RAM limitation to ensure that all hardware functions as intended.
- Load balancing for application servers is provided by the customer.
- The file storage requirement for reports may affect the amount of hard disk space needed on the Console and Device Services servers, depending on whether you enable caching. See Reports Storage Requirements on page 30 for more information.

Server		Up to 50,000 Devices
Database server	CPU/Cores	2x 4-core
	RAM (GB)	64
	DB Size (GB)	500
	Trans Log Size (GB) (Log backups every 15 minutes)	200
	Temp DB (GB)	200
	Avg IOPS (DB & Temp DB)	1,500
	Peak IOPS (DB & Temp DB)	3,000
UEM console (includes API component) **Refer to Workspace ONE UEM API Endpoint Installation.**		2 load-balanced application servers, each with: 4 CPU cores, 8 GB RAM, and 50 GB storage

Server	Up to 50,000 Devices
Device Services with AWCM (includes API component) **Refer to Workspace ONE UEM API Endpoint Installation.**	3 load-balanced application servers, each with: 4 CPU cores, 8 GB RAM, and 50 GB storage **Note :** If your Workspace ONE UEM deployment manages a majority of devices that require AWCM (Android, Windows Desktop, and Rugged devices), you must deploy additional resources. Each AWCM server must have 8 CPU and 8GB RAM per 40,000 devices and active connections. For example, 120,000 Android Devices requires 3 servers with 8CPU and 8GB RAM each.
VMware Identity Manager Service	See VMware Identity Manager Service Hardware Sizing
VMware Enterprise Systems Connector	See VMware Enterprise Systems Connector Server Hardware Sizing
SEG Proxy Server	See Secure Email Gateway Server Hardware Sizing
VMware Tunnel	See VMware Tunnel Server Hardware Sizing
Email Notification Service	See Email Notification Service Hardware Sizing
Workspace ONE Intelligence	See Workspace ONE Intelligence on page 30
Adaptiva	See Adaptiva on page 30

Important: For application servers, a 64-bit dual core Intel processor is required.

Server Sizing Topology (Up to 50,000 Devices)



Workspace ONE UEM API Endpoint Installation

For deployments up to 50,000 devices, the Workspace ONE UEM API endpoint is installed on both the Console and Device Services servers, with the API Site URL pointing to the Console server by default. If you anticipate performing third-party API integrations in the future, or if you want to make this component publicly accessible, then you should configure the API Site URL to point instead to the Device Services server. For instructions on how to perform this best practice procedure, refer to the **Verify Correct Site URL Population** procedure in the VMware AirWatch Installation Guide (VMware provides this document to you as part of the on-premises installation process), which includes this task as part of the post-installation process. Using the API endpoint on the Device Services server may increase the sizing requirements for the server. These requirements depend on how you use the APIs, with heavy use resulting in different sizing numbers. Since API use is situational, Workspace ONE UEM does not provide a standard recommendation for cases of heavy API use. Refer to the sizing disclaimers in the specific sections based on deployment size.

For existing installations, if the API component is already pointing to the Console and you change it to point to the Device Services server instead, you must re-install any Workspace ONE UEM products that use the API URL (for example, VMware Tunnel).

For deployments of up to 100,000 devices and higher, Workspace ONE UEM recommends a standalone API server, in which case you should change the Site URL to match your dedicated API server URL.

On-Premises Architecture Sizing for up to 100,000 Devices

Use the table to determine the sizing requirements for a deployment of up to 100,000 devices. Each column represents the requirements for a deployment up to that number of devices. The columns are not cumulative – each column contains the exact requirements for the listed number of devices.

Consider the following figures as starting points. You may need to adjust them as you implement different features of the Workspace ONE UEM solution. Transaction frequency, number of concurrent connections, and other metrics affect performance, and you may need to tweak the numbers to accommodate your specific deployment. Contact Workspace ONE Support if you require extra assistance.

Additional notes to consider:

- Certain SQL versions have a maximum supported RAM limit, so review your SQL version's RAM limitation to ensure that all hardware functions as intended.
- Load balancing for application servers is provided by the customer.
- The file storage requirement for reports may affect the amount of hard disk space needed on the Console and Device Services servers, depending on whether you enable caching. See Reports Storage Requirements on page 30 for more information.

Important: For sizing information for deployments with more than 100,000 devices, please contact Workspace ONE Support.

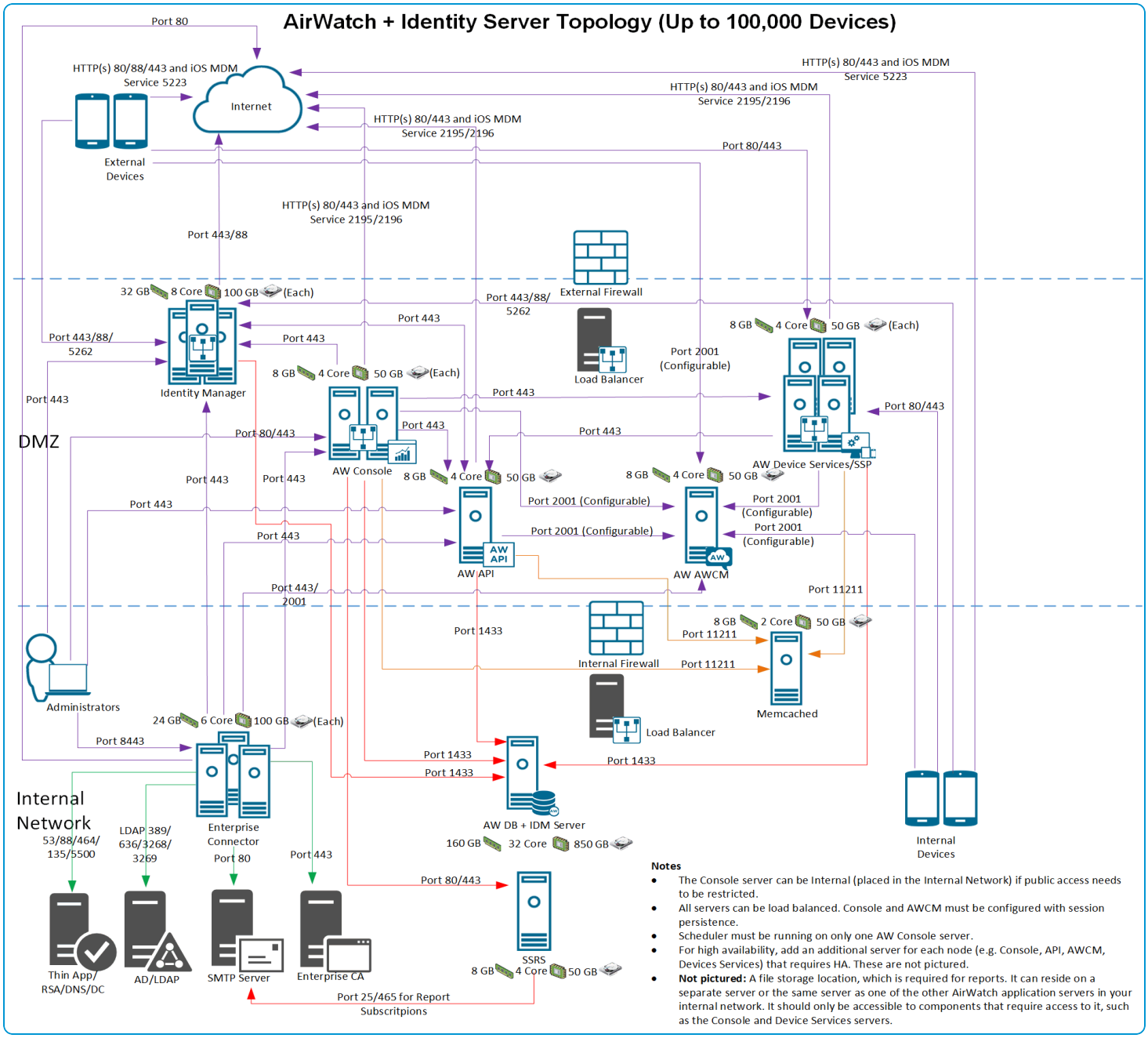
Server		Up to 100,000 Devices
Database server	CPU/Cores	2x 8-core
	RAM (GB)	128
	DB Size (GB)	750
	Trans Log Size (GB) (Log backups every 15 minutes)	400
	Temp DB (GB)	300
	Avg IOPS (DB & Temp DB)	2,000
	Peak IOPS (DB & Temp DB)	6,000
UEM console (dedicated)		2 load-balanced application servers, each with: 8 GB RAM, 4 CPU Cores, and 50 GB storage
API Server (dedicated)**		1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage
Device Services (dedicated)		4 load-balanced application servers, each with: 8 GB RAM, 4 CPU Cores, and 50 GB storage

Server	Up to 100,000 Devices
AWCM Server (dedicated)	1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage **Note :** If your Workspace ONE UEM deployment manages a majority of devices that require AWCM (Android, Windows Desktop, and Rugged devices), you must deploy additional resources. Each AWCM server must have 8 CPU and 8GB RAM per 40,000 devices and active connections. For example, 120,000 Android Devices requires 3 servers with 8CPU and 8GB RAM each.
Reporting Server (SSRS)	1 reporting server with 4 CPU cores, 8 GB RAM, and 50 GB storage
VMware Identity Manager Service	See VMware Identity Manager Service Hardware Sizing
VMware Enterprise Systems Connector	See VMware Enterprise Systems Connector Server Hardware Sizing
SEG Proxy Server	See Secure Email Gateway Server Hardware Sizing
VMware Tunnel	See VMware Tunnel Server Hardware Sizing
Email Notification Service	See Email Notification Service Hardware Sizing
Content Gateway	See Content Gateway Hardware Sizing
Workspace ONE Intelligence	See Workspace ONE Intelligence on page 30
Adaptiva	See Adaptiva on page 30

** If your API server is standalone then the network requirements for the API server is to ensure connectivity to the database and various cloud messaging platforms (APNS, GCM, WNS) over ports 80, 443, 2195, and 2196. All other Workspace ONE UEM services (Console, Device Services, SEG, VMware Tunnel) must be enabled to communicate to the API server over HTTPS (443).

Important: For application servers, a 64-bit dual core Intel processor is required.

Server Sizing Topology (Up to 100,000 Devices)



On-Premises Architecture Hardware Assumptions

The following are assumptions that help you determine if you must adjust the hardware requirements shown in the sizing tables based on the hardware needs of your environment.

General Assumptions

- High Availability is easily accomplished in Workspace ONE UEM but affects your requirements. Contact Workspace ONE Support if you need further assistance, since every deployment is unique and has its own requirements.
- Support for TLS 1.0, 1.1, and 1.2 is provided.
- Sizing estimates include allocation for 1 GB of cumulative app storage. Increase the server disk space and DB disk space to account for increased storage (for example, a 5 GB app deployment requires an extra 4 GB disk space for the database and application servers).
- Sizing estimates include allocation for 1 GB of cumulative content storage for the VMware Content Locker. Increase the server disk space to account for increased storage (for example, 5 GB of content requires an extra 4 GB disk space for the application servers).
- Servers must be set up in English. AirWatch must be set up on an English operating system.

Database Server Hardware Assumptions

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

- You can install the Workspace ONE UEM database on physical or virtualized hardware.
    - If installing on virtualized hardware, ensure you are following the VMware and Microsoft best practices for SQL deployments. Also ensure I/O requirements can be met and the overall virtual architecture supports Workspace ONE UEM requirements.
- If AirWatch is to be installed on a shared database server, Workspace ONE UEM must be given its own instance with earmarked resources as defined in the On-Premises Architecture Sizing for up to 5,000 and 25,000 Devices on page 14.

Other AirWatch Components

The following sections show the hardware assumptions for various Workspace ONE UEM components. They are listed here to give you an idea of what you will need to configure them based on the needs of your deployment. Each component has a separate guide, available at docs.vmware.com, that you can reference for additional requirements and information.

VMware Identity Manager Service Hardware Sizing

The following assumptions are made regarding server hardware used to host the VMware Identity Manager Service. For sizing above the highest amount, contact Workspace ONE Support.

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
CPU cores	3 load-balanced servers with 2 CPU cores	3 load-balanced servers with 4 CPU cores	3 load-balanced servers with 8 CPU cores	3 load-balanced servers with 8 CPU cores
RAM	6 GB each	8 GB each	16 GB each	32 GB each
Hard Disk Space	100 GB each	100 GB each	100 GB each	100 GB each

Database Sizing Increase

When you deploy the VMware Identity Manager Service, you must increase the size of your Workspace ONE UEM database.

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
CPU cores	+2 CPU cores	+4 CPU cores	+8 CPU cores	+8 CPU cores
RAM	+4 GB each	+8 GB each	+16 GB each	+32 GB each
Hard Disk Space	+50 GB each	+50 GB each	+100 GB each	+100 GB each

An Intel processor is required. CPU Cores should each be 2.0 GHz or higher.

VMware Enterprise Systems Connector Server Hardware Sizing

The following assumptions are made regarding server hardware used to host the VMware Enterprise Systems Connector. For sizing above the highest amount, contact Workspace ONE Support.

Hardware Sizing

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
ACC Requirements				
CPU Cores	2 CPU cores	2 load-balanced servers with 2 CPU cores	2 load-balanced servers with 2 CPU cores	3 load-balanced servers with 2 CPU cores
RAM	4 GB	4 GB each	4 GB each	8 GB each
Disk Space	50 GB	50 GB each	50 GB each	50 GB each
The VMware Identity Manager Connector component has the following additional requirements. If you are installing both the ACC and VMware Identity Manager Connector components, add these requirements to the ACC requirements.				
VMware Identity Manager Connector Requirements				
CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores	2 load-balanced servers with 4 CPU Cores
RAM	6 GB each	8 GB each	16 GB each	16 GB each
Disk Space	50 GB each	50 GB each	50 GB each	50 GB each

Notes:

- VMware Enterprise Systems Connector traffic is automatically load-balanced by the AWCM component. It does not require a separate load balancer. Multiple VMware Enterprise Systems Connectors in the same organization group that connect to the same AWCM server for high availability can all expect to receive traffic (a live-live configuration). How traffic is routed is determined by AWCM and depends on the current load.
- CPU Cores should each be 2.0 GHz or higher. An Intel processor is required.
- Disk Space requirements include: 1 GB disk space for the VMware Enterprise Systems Connector application, Windows OS, and .NET runtime. Additional disk space is allocated for logging.

Secure Email Gateway Server Hardware Sizing

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

Classic Platform

SEG	CPU Core	RAM	Notes
SEG without content transformation	2	4 GB	Per 4,000 devices, up to a maximum of 16,000 devices (8 CPU/16 GB RAM) per application server
SEG with content transformation (Attachment handling, hyperlinks security, tagging, etc.)	2	4 GB	Per 500 devices (250 devices per core), up to a maximum of 2,000 devices (8 CPU/16 GB RAM) per application server Performance varies based on the size and quantity of transforms. These numbers reflect a deployment with a high number of content transforms. Sizing estimates vary based on actual email and attachment usage

Notes for both SEG deployment types:

- An Intel processor is required. CPU Cores should each be 2.0 GHz or higher.
- The minimum requirements for a single SEG server are 2 CPU cores and 4 GB of RAM.
- IIS App Pool Maximum Worker Processes should be configured as (# of CPU Cores / 2).
- 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.
- 5 GB Disk Space needed per SEG and dependent software (IIS). This does not include system monitoring tools or additional server applications.

V2 Platform

SEG	CPU Core	RAM	Notes
SEG without content transformation	2	4 GB	Per 8,000 devices, up to a maximum of 32,000 devices (8 CPU/ 16 GB RAM) per application server.
SEG with content transformation (Attachment handling, hyperlinks security, tagging etc.)	2	4 GB	Per 4,000 devices (2,000 devices per core) per application server, up to a maximum of 16,000 devices (8 CPU/16 GB RAM) Performance varies based on the size and quantity of transforms. These numbers reflect a deployment with a high number of content transforms. Sizing estimates vary based on actual email and attachment usage.

Notes for both SEG deployments types:

- An Intel processor is required. CPU Cores should each be 2.0 GHz or higher.
- The minimum requirements for a single SEG server are 2 CPU cores and 4 GB of RAM.
- 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.
- 5 GB Disk Space needed per SEG and dependent software. This does not include system monitoring tools or additional server applications.

VMware Tunnel and Unified Content Gateway (Tunnel) Hardware Sizing

The following assumptions are made regarding server hardware used to host the VMware Tunnel. For sizing above the highest amount, contact Workspace ONE Support.

Hardware Sizing

Use the table to determine the sizing requirements for your deployment. Each column represents the requirements for a deployment up to that number of devices. The columns are not cumulative – each column contains the exact requirements for the listed number of devices.

Number of Devices	Up to 5,000	5,000 to 10,000	10,000 to 40,000	40,000 to 100,000
CPU Cores	1 server with 2 CPU Cores*	2 load-balanced servers with 2 CPU Cores each	2 load-balanced servers with 4 CPU Cores each	4 load-balanced servers with 4 CPU Cores each
RAM (GB)	4	4 each	8 each	16 each
Hard Disk Space (GB)	10 GB for distro (Linux only) 400 MB for installer ~10 GB for log file space**			

*It is possible to deploy only a single VMware Tunnel server as part of a smaller deployment. However, consider deploying at least 2 load-balanced servers with 2 CPU Cores each regardless of number of devices for uptime and performance purposes.

**About 10 GB is for a typical deployment. Log file size should be scaled based on your log usage and requirements for storing logs.

AirWatch Content Gateway and Unified Access Gateway (Content Gateway) Hardware Sizing

The following assumptions are made regarding server hardware used to host the AirWatch Content Gateway. For sizing above the highest amount, contact Workspace ONE Support. Consider deploying Content Gateway on a separate server from the VMware Tunnel, as both have different network and system requirements. If your deployment requires that Content Gateway be installed on the same server as VMware Tunnel, reference the Unified Access Gateway documentation at https://docs.vmware.com/en/Unified-Access-Gateway/index.html.

Hardware Sizing

Use the table to determine the sizing requirements for your deployment. Each column represents the requirements for a deployment up to that number of devices. The columns are not cumulative – each column contains the exact requirements for the listed number of devices.

Requirement	CPU Cores	RAM (GB)	Disk Space	Notes
VM or Physical Server (64-bit)	2 CPU Core (2.0+ GHz)* *An Intel processor is required.	2 GB+	5 GB	The requirements listed here support basic data query. You may require additional server space if your use case involves the transmission of large encrypted files from a content repository.
Sizing Recommendations				
Number of Devices	**Up to 5,000**	**5,000 to 10,000**	**10,000 to 40,000**	**40,000 to 100,000**
CPU Cores	1 server with 2 CPU Cores*	2 load-balanced servers with 2 CPU Cores each	2 load-balanced servers with 4 CPU Cores each	4 load-balanced servers with 4 CPU Cores each
RAM (GB)	4	4 each	8 each	16 each
Hard Disk Space (GB)	10 GB for distro (Linux only) 400 MB for installer ~10 GB for log file space**			

*It is possible to deploy only a single AirWatch Content Gateway server as part of a smaller deployment. However, consider deploying at least 2 load-balanced servers with 2 CPU Cores each regardless of number of devices for uptime and performance purposes.

**About 10 GB is for a typical deployment. Log file size should be scaled based on your log usage and requirements for storing logs.

Email Notification Service Hardware Sizing

The following assumptions are made regarding server hardware used to host the Email Notification Service (ENS) application.

Hardware Sizing - Classic

CPU Core	RAM	Hard Disk Storage	Notes
2 (Intel processor)	4 GB	10 GB	Per 20,000 users.

Hardware Sizing - V2

ENS Server	CPU Core	RAM	Hard Disk Storage	Notes
App Server	2 (2 GHz Intel processor)	16 GB	50 GB	Up to 100,000 users.
Database Server	2 (2 GHz Intel processor)	16 GB	50 GB	Up to 100,000 users.

Reports Storage Requirement

To use the new reports framework, which generates reports with greater reliability and faster download times, you must set up reports storage.

Workspace ONE Intelligence

	5000 Devices	25,000 Devices	50,000 Devices	100,000 Devices
Servers	1	1	1	1
CPUs	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)	2 (2 GHz Intel processor)
Memory	4GB	8GB	8GB	16GB
Storage	25GB	25GB	25GB	25GB

Adaptiva

Component	Requirement
Operating system	Windows Server 2008+
Processor	Xeon Processor, single quad core (2 GHz Intel processor)
Memory allocation	• 0 to 5,000 clients - 2048 MB • 5,001 to 10,000 clients - 3072 MB • 10,001 to 19,999 clients - 5120 MB • 20,000 to 49,999 clients - 6144 MB • 50,000+ - 8192 MB

Memcached

Component	0-300k devices	300k+ devices
CPU Cores(2 GHz Intel processor)	2	2
RAM	8 GB	16 GB

Reports Storage Requirements

To deploy the reports storage solution, ensure that your server meets the requirements.

Note: If you are already using File Storage, then Report Storage is available, but not required to run your deployment. If you configure Reports Storage alongside File Storage, the report files will prioritize report storage over file storage.

Create the Shared Folder on a Server in your Internal Network

- Report storage can reside on a separate server or the same server as one of the other Workspace ONE UEM application servers in your internal network. Ensure only the components that require access to the server can access the report storage server, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid an authentication failure. If the Device Services or Console servers are not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure Reports Storage at the Global Organization Group

Configure reports storage settings at the Global organization group level in the UEM console.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for report storage.
- Give the local user read/write/modify permissions to the file share that is being used for the Report Storage Path.

  If you give the user modify permission, Workspace ONE UEM automatically deletes old reports from the storage. If you do not give the user modify permissions, consider monitoring report storage to prevent running out of space.
- Configure the Report Storage Impersonation User in Workspace ONE UEM with the local user.

You can also use a domain service account instead of a local user account.

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use reports storage. Ensure that the reports storage location has enough space to accommodate the reports you intend to use.

For storing reports, your storage requirements depend on the number of devices, the daily number of reports, and the frequency with which you purge them. As a starting point, plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Also apply this sizing to your Console server if you enable caching.

File Storage Requirements

To set up local file storage, you must meet the following requirements.

Important: File Storage is required for Windows 10 Software Distribution.

Create the Shared Folder on a Server in your Internal Network

- File storage can reside on a separate server or the same server as one of the other AirWatch application servers in your internal network. It is only accessible to components that require access to it, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid the authentication failure. If the Device Services server or Console server is not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure the Network Requirements

- **If using Samba/SMB** – TCP: 445, 137, 139. UDP: 137, 138
- **If using NFS** – TCP and UDP: 111 and 2049

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use file storage. The file storage location should have enough space to accommodate the internal apps, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal apps or content, then a best practice is to size the Device Services server for 120 percent of the cumulative size of all the apps/content you need to publish.
- For storing reports, your storage requirements depend on the number of devices, the daily amount of reports, and the frequency with which you purge them. As a starting point, you should plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Apply this sizing to your Console server as well if you enable caching.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for File Storage.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure the File Storage Impersonation User in AirWatch with the local user.

You can also use a domain service account instead of a local user account.

Configure File Storage at the Global Organization Group

Configure file storage settings at the Global organization group level in the UEM Console.

Chapter 4:
Software Requirements

On-Premises Architecture Software Requirements

Ensure you meet the following software requirements for each of your application servers and your database server. You can find the software requirements for the various Workspace ONE UEM components, such as VMware Enterprise Systems Connector, Tunnel, and SEG, in their applicable guides, available at docs.vmware.com.

Application Server Software Requirements

Ensure that you meet the following software requirements for the application servers:

- Internet Explorer 9+ installed on all application servers
- Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016
- 64-bit Java (JRE 1.8) server needed for the server on which AWCM is installed. The Java installer is packaged with the Workspace ONE UEM installer and installs automatically if it is not already present.
- 64-bit Java (JRE 1.8) installed on all app servers. The Java installer is packaged with the Workspace ONE UEM installer and installs automatically if it is not already present.
- .NET Framework 4.6.2. The .NET Framework 4.6.2 installer is packaged with the Workspace ONE UEM installer and installs automatically if it is not already present.
- PowerShell version 3.0+ if you are deploying the PowerShell MEM-direct model for email. To verify your version, open PowerShell and run the command `$PSVersionTable`. More details on this and other email models are available in the **Workspace ONE UEM Mobile Email Management Guide**, available at docs.vmware.com.
- Microsoft SQL Server 2012 Native Client 11.3.6538.0 to run the database installer. If you do not want to install SQL Server 2012 Native Client, run the database installer from another UEM server (or a jump server) where Microsoft SQL Server 2012 Native Client 11.3.6538.0 can install.
- If you use Windows for SQL authentication, you must join application servers that talk to the database to the Windows user's domain. The Active Directory service account must have administrator-level permissions.

Database Server Software Requirements

- SQL Server 2012, SQL Server 2014, or SQL Server 2016 with Client Tools (SQL Management Studio, Reporting Services, Integration Services, SQL Server Agent, latest service packs). Ensure the SQL Servers are 64-bit (OS and SQL Server).

  Workspace ONE UEM does not support Express, Workgroup, or Web editions of SQL Server. These editions do not support all the features used in the Workspace ONE UEM application. Currently only Standard and Enterprise Editions are supported.
- Microsoft SQL Server 2012 Native Client 11.3.6538.0 is required to run the database installer. If you do not want to install Microsoft SQL Server 2012 Native Client 11.3.6538.0 on to your database server, then run the database installer from another AirWatch server or a jump server where Microsoft SQL Server 2012 Native Client 11.3.6538.0 can be installed.
- .NET 4.6.2 is required to run the database installer. If you do not want to install .NET on to your database server, then run the database installer from another Workspace ONE UEM server or a jump server where .NET can be installed.

- Ensure the SQL Server Agent Windows service is set to Automatic or Automatic (Delayed) as the Start type for the service. If set to Manual, it has to be manually started before database installation.
- You must have the access and knowledge required to create, back up, and restore a database.

When the database installer runs, it automatically updates your SQL Server with the latest versions of:

- ODBC Driver 13 for SQL Server 64-bit
- Command Line Utilities 13 for SQL Server 64-bit

Workspace ONE UEM Database Performance Recommendations

Use the following Workspace ONE UEM database performance recommendations, which are based on scalability tests performed by Workspace ONE UEM.

Recommendation	Description
TempDB Configuration	The number of tempDB files must match the number of CPU cores when the core is less than or equal to 8 cores. Beyond 8 cores, the number of files must be the closest multiple of 4 that is less than or equal to the number of cores (e.g. 10 cores will need 8 tempDBs, 12 cores will need 12 tempDBs, 13 cores will need 12 tempDBs, 16 cores will need 16 tempDBs.) File size, growth rate, and the location need to be the same for all tempDB files.
Memory Allocation	Eighty percent of the server memory should be allocated to SQL. The remaining 20% must be freed up to run the OS.
Cost Threshold for Parallelism and Maximum Degree of Parallelism	Cost Threshold for Parallelism is the cost needed for a query to be qualified to use more than a single CPU thread. Maximum Degree of Parallelism is the maximum number of threads that can be used per query. The following are recommended values for these parameters: • Cost Threshold of Parallelism: 50 • Max Degree of Parallelism: 2 and reduce to 1 in case of high server utilization.
Trace Flag	The following trace flags must be set to 1 at Global. 1117 (https://msdn.microsoft.com/en-us/library/ms188396.aspx) 1118 (https://msdn.microsoft.com/en-us/library/ms188396.aspx) 1236 (https://support.microsoft.com/en-us/kb/2926217) 8048 (https://blogs.msdn.microsoft.com/psssql/2015/03/02/running-sql-server-on-machines-with-more-than-8-cpus-per-numa-node-may-need-trace-flag-8048/)
Hyperthreading	If the database is running on a physical server, hyperthreading must be disabled on the database to ensure best performance. If it is on a VM, then having hypertherading enabled on the ESX host will not have any performance impact, but hyperthreading must be disabled on the Windows host level.
Optimize for Ad hoc Workloads	Enable Optimize for Ad hoc Workloads under SQL server properties. This is recommended in order to free memory from the server. Refer to the following article for more information: https://msdn.microsoft.com/en-us/library/cc645587(v=sql.120).aspx.

Recommendation	Description
Lock Escalation	Disable Lock Escalation for “interrogator.scheduler” table by running the “alter table interrogator.scheduler set (lock_escalation = {Disable})” command. This is recommended as the scheduler table has very high rate of updates/inserts. There is a high contention on this table with the use of GCM, and disabling lock escalation helps improve performance. However, the drawback is that more memory is consumed. Refer to the following article for more information: https://technet.microsoft.com/en-us/library/ms184286(v=sql.105).aspx.

For device deployments above 300,000 devices , ensure that the Database is partitioned. To enable this please run the installer from an elevated command prompt with the following flag: `Name_Of_Database_installer.exe /V"AWINSTALLPARTITIONEDDATABASE=1"`.

For example: `AirWatch_DB_9.1_GA_Setup.exe /V"AWINSTALLPARTITIONEDDATABASE=1"`.

Important: This command requires SQL Enterprise. If you are running this command on a Workspace ONE UEM Database, you must run the installer with the flag for each upgrade from then on. If you do not, an error displays.

Chapter 5:
Network Requirements

On-premises Architecture Network Requirements

The Workspace ONE UEM console and Device Services servers must communicate with several internal and external endpoints for functionality. End-user devices must also reach certain endpoints for access to apps and services.

For configuring the ports listed below, all traffic is uni-directional (outbound) from the source component to the destination component.

	Source Component	Destination Component	Protocol	Port	Notes
Console Server					
	UEM console Hostname	discovery.awmdm.com	HTTPS	443	Optional, for AutoDiscovery
	UEM console Hostname	awcp.air-watch.com	HTTPS	443	Optional, for APNs Certificate
	UEM console Hostname	gem.awmdm.com	HTTPS	443	Workspace ONE UEM Analytics in myAirWatch
	UEM console Hostname	appwrap04.awmdm.com	HTTPS	443	Workspace ONE UEM Cloud iOS App Wrapping Service
	UEM console Hostname	gateway.push.apple.com (17.0.0.0/8)	TCP	2195	Apple iOS and macOS only
	UEM console Hostname	feedback.push.apple.com (17.0.0.0/8)	TCP	2196	Apple iOS and macOS only
	UEM console Hostname	appwrapandroid.awmdm.com	HTTPS	443	Workspace ONE UEM Cloud Android App Wrapping Service
	UEM console Hostname	android.googleapis.com	HTTPS	443	Android only
	UEM console Hostname	play.google.com	HTTPS	443	Android only
	UEM console Hostname	android.clients.google.com	TCP	80	Android App Management only
	UEM console Hostname	fonts.googleapis.com	HTTP/HTTPS	80 or 443	For fonts used in the UEM console
	UEM console Hostname	inference.location.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging for Windows devices
	UEM console Hostname	*notify.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging for Windows devices

	Source Component	Destination Component	Protocol	Port	Notes
	UEM console Hostname	next-services.apps.microsoft.com	HTTP/HTTPS	80 or 443	For App Management, Windows 8 /RT only
	UEM console Hostname	*.windowsphone.com	HTTP/HTTPS	80 or 443	For App Management, Windows Phone 8 only
	UEM console Hostname	login.live.com	HTTPS	443	For Cloud Messaging for Windows devices
	UEM console Hostname	login.windows.net/{TenantName}	HTTPS	443	Windows 10 only, where {TenantName} is the domain name of your tenant in Azure
	UEM console Hostname	graph.windows.net	HTTPS	443	Windows 10 only
	UEM console Hostname	has.spserv.microsoft.com	HTTPS	443	Windows 10 only, for health attestation
	UEM console Hostname	*virtualearth.net	HTTP/HTTPS	80 or 443	For location services Bing Maps integration
	UEM console Hostname	BES Server	HTTPS	443	Blackberry only
	UEM console Hostname	**Apple iTunes** itunes.apple.com *.mzstatic.com *.phobos.apple.com *.phobos.apple.com.edgesuite.net	HTTP	80	Apple iOS and macOS only
	UEM console Hostname	gateway.celltrust.net (162.42.205.0/24)	HTTPS	443	Only requires the use of 443 when using SMS integration
	UEM console Hostname	SSL Cert CRL* (Example: ocsp.verisign.com)	HTTP/HTTPS	80 or 443	Optional, if Console is publicly accessible

	Source Component	Destination Component	Protocol	Port	Notes
	UEM console Hostname	CRL: http://crl3.digicert.com/sha2-assured-cs-g1.crl	HTTP	80	Supports code-signing verification of Workspace ONE UEM code post-install.
	UEM console Hostname	All Workspace ONE UEM Servers	HTTPS	443	
	UEM console Hostname	AWCM server	HTTPS	2001	AWCM may be installed on your Device Services server.
	UEM console Hostname	Workspace ONE UEM API server (if standalone)	HTTPS	443	Set up network traffic from the Console server to the API server if the API component is not installed on the Console server. The API component may be installed on your Device Services server.
	UEM console Hostname	File Storage (if not set up on Console server)	SMB or NFS	Samba/SMB: TCP: 445, 137, 139. UDP: 137, 138 NFS: TCP and UDP: 111 and 2049	Required for reports. For more information see Reports Storage Requirement on page 30.
	UEM console Hostname	SQL SSRS Reporting	HTTP	80	
	UEM console Hostname	Workspace ONE UEM Database server	SQL	1433	
	UEM console Hostname	Exchange Server	HTTP/HTTPS	80 or 443	For PowerShell integration, if not using VMware Enterprise Systems Connector
	UEM console Hostname	Active Directory domain controller	LDAP(S)	389 or 636 or 3268 or 3269	For LDAP integration

	Source Component	Destination Component	Protocol	Port	Notes
	UEM console Hostname	SMTP Mail Relay	SMTP	25 or 465	For SMTP integration
	UEM console Hostname	Internal PKI	HTTPS/ DCOM	443 (HTTPS) or 135 or 1025-5000 or 49152-65535 (DCOM)	For PKI integration
	Console Admin APIs				
	Admin Browser	VMware Identity Manager Service	HTTPS	443	Astro APIs
	Admin Browser	UEM console Hostname	HTTPS	443	Console Access
	Admin Browser	API Server Hostname	HTTPS	443	Astro APIs
	API Server (If Standalone)				
	API Server Hostname	Workspace ONE UEM Database server	SQL	1433	
	API Server Hostname	AWCM server	HTTPS	2001	If AWCM is hosted on device services, then direct to the Device Services server.
	API Server Hostname	Active Directory domain controller	LDAP(S)	389 or 636 or 3268 or 3269	Only required if you are integrating with VMware Identity Manager without the use of VMware Enterprise Systems Connector.
	API Server Hostname	android.googleapis.com play.google.com	HTTP/HTTPS	80 or 443	For Cloud Messaging for Android devices.
	API Server Hostname	inference.location.live.net *notify.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging for Windows devices.
	API Server Hostname	gateway.push.apple.com (17.0.0.0/8) feedback.push.apple.com (17.0.0.0/8)	TCP	2195, 2196	For Apple iOS and macOS cloud messaging.

	Source Component	Destination Component	Protocol	Port	Notes
Console Admin APIs					
	VMware Identity Manager Service	API Server Hostname	HTTPS	443	Auth Token Request
	API Server Hostname	VMware Identity Manager Service	HTTPS	443	Astro APIs
Device Services Server					
	Device Services Hostname	discovery.awmdm.com	HTTPS	443	Optional – For auto discovery functionality
	Device Services Hostname	gateway.push.apple.com	TCP	2195	Apple only
	Device Services Hostname	feedback.push.apple.com	TCP	2196	Apple only
	Device Services Hostname	android.googleapis.com	HTTP/HTTPS	80 and 443	Android only
	Device Services Hostname	play.google.com	HTTPS	443	Android only
	Device Services Hostname	android.clients.google.com	TCP	80	Android app management only
	Device Services Hostname	awcp.air-watch.com	HTTPS	443	Optional, for APNs Certificate
	Device Services Hostname	inference.location.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging for Windows devices
	Device Services Hostname	*notify.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging for Windows devices
	Device Services Hostname	*.windowsphone.com	HTTP	80	For App Management, Windows Phone 8 only
	Device Services Hostname	next-services.apps.microsoft.com	HTTP/HTTPS	80 or 443	For App Management, Windows 8/RT only
	Device Services Hostname	login.live.com	HTTPS	443	For Cloud Messaging for Windows devices

	Source Component	Destination Component	Protocol	Port	Notes
	Device Services Hostname	login.windows.net/{TenantName}	HTTPS	443	Windows 10 only. Where {TenantName} is the domain name of your tenant in Azure.
	Device Services Hostname	graph.windows.net	HTTPS	443	Windows 10 only
	Device Services Hostname	has.spserv.microsoft.com	HTTPS	443	Windows 10 only for health attestation
	Device Services Hostname	**Apple iTunes** itunes.apple.com *.mzstatic.com *.phobos.apple.com *.phobos.apple.com.edgesuite.net	HTTP	80	Apple only
	Device Services Hostname	SSL Cert CRL* (Example: ocsp.verisign.com)	HTTP/HTTPS	80 or 443	
	Device Services Hostname	CRL: http://crl3.digicert.com/sha2-assured-cs-g1.crl	HTTP	80	For various services to function properly
	Device Services Hostname	All Workspace ONE UEM Servers	HTTPS	443	
	Device Services Hostname	AWCM (if standalone)	HTTPS	2001	Set up network traffic from the Device Services server to the AWCM server if the AWCM component is not installed on the Device Services server.

	Source Component	Destination Component	Protocol	Port	Notes
	Device Services Hostname	Workspace ONE UEM API server (if standalone)	HTTPS	443	Set up network traffic from the Device Services server to the API server if the API component is not installed on the Device Services server.
	Device Services Hostname	File Storage (dedicated server or set up on an internal application server)	SMB or NFS	Samba/SMB: TCP: 445, 137, 139. UDP: 137, 138 NFS: TCP and UDP: 111 and 2049	Required for reports. For more information see Reports Storage Requirement on page 30.
	Device Services Hostname	Database Server	SQL	1433	
	Device Services Hostname	Exchange Server	HTTP/HTTPS	80 or 443	For PowerShell integration, if not using VMware Enterprise Systems Connector
	Device Services Hostname	Active Directory domain controller	LDAP(S)	389 or 636 or 3268 or 3269	[OPTIONAL] if you don't use VMware Enterprise Systems Connector
	Device Services Hostname	SMTP Mail Relay	SMTP	25 or 465	[OPTIONAL] if you do not use VMware Enterprise Systems Connector
	Device Services Hostname	Internal PKI	HTTPS/ DCOM	443 (HTTPS) or 135 or 1025-5000 or 49152-65535 (DCOM)	[OPTIONAL] if you do not use VMware Enterprise Systems Connector

	Source Component	Destination Component	Protocol	Port	Notes
	Device Services Hostname	appwrap04.awmdm.com	HTTPS	443	AirWatch Cloud iOS App Wrapping Service
	Device Services Hostname	appwrapandroid.awmdm.com	HTTPS	443	AirWatch Cloud Android App Wrapping Service
	VMware Identity Manager Service				
	Load Balancer	VMware Identity Manager service	HTTPS	443	
	VMware Identity Manager service	VMware Identity Manager service	HTTPS	443	
	Browsers	VMware Identity Manager service	HTTPS	443	
	VMware Identity Manager service	vapp-updates.vmware.com	HTTPS	443	Access to the upgrade server
	Browsers	VMware Identity Manager service	HTTPS	8443	Administrator Port
	VMware Identity Manager service	SMTP	SMTP	25	Port to relay outbound mail
	VMware Identity Manager service	Active Directory	LDAP, LDAPS, MSFT-GC, MSFT-GC-SSL	389, 636, 3268, 3269	Default values are listed. These ports are configurable.
	VMware Identity Manager service	VMware ThinApp repository	TCP	445	Access to the ThinApp repository
	VMware Identity Manager service	RSA SecurID system	UDP	5500	Default value is listed. This port is configurable.
	VMware Identity Manager service	DNS server	TCP/UDP	53	Every VMware Identity Manager server must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
	VMware Identity Manager service	Domain controller	TCP/UDP	88,464,135	
	VMware Identity Manager service	VMware Identity Manager service	TCP	9300-9400	Audit needs

	Source Component	Destination Component	Protocol	Port	Notes
	VMware Identity Manager service	VMware Identity Manager service	TCP	54328	Audit needs
	VMware Identity Manager service	VMware Identity Database	TCP	1433, 5432, 1521	Microsoft SQL default port is 1433. The PostgreSQL default port is 5432. The Oracle default port is 1521.
	VMware Identity Manager service	View server		443	Access to View server.
	VMware Identity Manager service	Citrix Integration Broker server	TCP	80, 443	Connection to the Citrix Integration Broker. Port option depends on whether a certificate is installed on the Integration Broker server.
	VMware Identity Manager service	Workspace ONE UEM REST API	HTTPS	443	For device compliance checking and for the Enterprise System Connector Workspace ONE UEM Cloud Connector password authentication method, if that is used.
	VMware Identity Manager service	Cloud-hosted KCD	UDP	88	Port used for Kerberos traffic from the identity manager to the hosted cloud KDC service.

	Source Component	Destination Component	Protocol	Port	Notes
	Adaptiva Server	AW Cloud Connector	UDP	34320	Port used for Adaptiva SDK library to send and receive messages to/from Adaptiva Server.
	iOS mobile device	Cloud-hosted KCD	UDP	88	Port used for Kerberos traffic from the iOS device to the hosted cloud KDC service.
	iOS mobile device	VMware Identity Manager service	TCP/UDP	88	Port used for Kerberos traffic from iOS device to the built-in KDC
	iOS mobile device	VMware Identity Manager service	UDP	88	Port used for Kerberos traffic from iOS device to the hosted cloud KDC service.
	iOS mobile device	VMware Identity Manager service	HTTPS/TCP	443	Port used for Kerberos traffic from iOS device to the hosted cloud KDC service.
	Android mobile device	Workspace ONE UEM HTTPS proxy service	TCP	5262	Workspace ONE UEM Tunnel client routes traffic to the HTTPS proxy for Android devices.
	Browser	VMware Identity Manager service	HTTP	80	Required
	VMware Identity Manager service	Ehcache		40002	
	VMware Identity Manager service	RabbitMQ		4269, 5700, and 25672	
	VMware Identity Manager service	Elasticsearch		9200, 9300, 443, 8443, 80	
	VMware Identity Manager service	Android SSO		5262	

	Source Component	Destination Component	Protocol	Port	Notes
	VMware Identity Manager service	Browsers	HTTPS	6443	For certificate authentication configured in a VMware Identity Manager on premises DMZ deployment.
	Console Admin APIs				
	UEM console Hostname	VMware Identity Manager Service	HTTPS	443	Astro APIs
	Reports Server				
	SSRS Server (Reports Server)	SMTP Mail Relay	SMTP	25 or 465	For reports subscriptions
	End-User Devices				
	Devices (Internet/Wi-Fi)	Device Services Hostname	HTTP/HTTPS	80 or 443	Best practice: use HTTPS 443 for additional security.
	Devices (Internet/Wi-Fi)	SEG Hostname	HTTPS	443	
	Devices (Internet/Wi-Fi)	VMware Tunnel Hostname	HTTPS	443, 2020	For Browser access
	Devices (Internet/Wi-Fi)	#-courier.push.apple.com (17.0.0.0/8)	TCP	5223 and 443	Apple only. '#' is a random number from 0 to 200.
	Devices (Internet/Wi-Fi)	phobos.apple.com ocsp.apple.com ax.itunes.apple.com	HTTP/HTTPS	80 or 443	Apple only
	Devices (Internet/Wi-Fi)	mtalk.google.com	TCP	5228	For Cloud Messaging, Android only
	Devices (Internet/Wi-Fi)	play.google.com	HTTPS	443	For App Management, Android only
	Devices (Internet/Wi-Fi)	*.notify.windows.com	HTTPS	443	For Cloud Messaging, Windows 10
	Devices (Internet/Wi-Fi)	inference.location.live.net	HTTP/HTTPS	80 or 443	Retrieve device location, Windows 10

	Source Component	Destination Component	Protocol	Port	Notes
	Devices (Internet/Wi-Fi)	*.notify.live.net	HTTP/HTTPS	80 or 443	For Cloud Messaging. Windows Phone 10
	Devices (Internet/Wi-Fi)	wns.windows.com	HTTPS	443	Windows Push Notification Service
	Devices (Internet/Wi-Fi)	has.spserv.microsoft.com	HTTPS	443	Health Attestation Services, Windows 10
	Devices (Internet/Wi-Fi)	microsoft.com/store/apps	HTTPS	443	Public app store access
	Devices (Internet/Wi-Fi)	bspmts.mp.microsoft.com	HTTPS	443	Business store portal app access
	Devices (Internet/Wi-Fi)	ekop.intel.com/ekcertservice	HTTPS	443	For Intel firmware TPM. Authorize this URL if you are filtering Internet access for client devices. This is needed for signed certificates for Secure Boot.
	Devices (Internet/Wi-Fi)	ekcert.spserv.microsoft.com	HTTPS	443	For Qualcomm firmware TPM. Authorize this URL if you are filtering Internet access for client devices. This is needed for signed certificates for Secure Boot.
	Devices (Internet/Wi-Fi)	*login.live.com	HTTP/HTTPS	80 or 443	Request WNS Channel, Windows 10
	Devices (Internet/Wi-Fi)	*.windowsphone.com	HTTP/HTTPS	80 or 443	Windows Phone 8
	Devices (Internet/Wi-Fi)	has.spserv.microsoft.com	HTTPS	443	Windows 10 only for health attestation
	Devices (Internet/Wi-Fi)	Public SSL Cert CRL (Example: ocsp.verisign.com)	HTTP/HTTPS	80 and 443	

	Source Component	Destination Component	Protocol	Port	Notes
	Devices (Internet/Wi-Fi)	AWCM Server	HTTP/HTTPS	2001	Windows Rugged, Android, macOS, Windows 7, and Windows Desktop devices with Workspace ONE UEM Protection Agent only. Windows Desktop devices using the Workspace ONE UEM Protection Agent use the AWCM for real-time notifications.

Chapter 6:
Monitoring Guidelines

On-Premises Architecture Monitoring Overview

Monitoring your Workspace ONE UEM 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 Workspace ONE Support.

Hardware Load Capacity Recommendations

Hardware	Monitoring	Recommendation
CPU	CPU load-hour	Alerting at high-load (for example, 90% load is a warning and 95% load is critical)
RAM	Free memory	Alerting at low free memory (for example, 10% free is a warning and 5% free is critical)
Hard Disk	Free hard disk space	Alerting at low hard disk space (for example, 10% free is a warning and 5% free is critical)

Archive Workspace ONE UEM Logs

Workspace ONE UEM-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 Workspace ONE UEM directory structure. Automatic monitoring of these files is not required, but consider consulting these files if issues arise.

For more information about collecting logs, see the **VMware Workspace ONE UEM Logging Guide**, available at my.air-watch.com.

Perform a 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 official health check test for your load balancer(s) to test connectivity to the Console, Device Services, Device Management, and Self-Service Portal endpoints.

1. Configure the following in your load balancer(s), depending on the application server(s) being load-balanced:
   - **Console** – GET to https://<host>/airwatch/awhealth/v1
   - **Device Services** – GET to https://<host>/deviceservices/awhealth/v1
   - **Device Management** – GET to https://<host>/devicemanagement/awhealth/v1
   - **Self-Service Portal** – GET to https://<host>/mydevice/awhealth/v1

2. Add your load balancer IP address – or addresses if multiple – in the Workspace ONE UEM console under **System Settings > Admin > Monitoring**.

   Configure this page to determine which tools can monitor whether the application server(s) are up. These can include the Admin Console, Device Services, Device Management, and Self-Service Portal. By default any load balancer or monitoring tool can perform this monitoring. For security purposes you can control this monitoring by IP address.

   For example, you can set up a load balancer to detect if a given application server is up. The Admin Monitoring settings page lets you whitelist certain IP addresses that can access this page. By default, any IP address is allowed if no IP addresses are defined.

3. Restart the application pools.

When you test the health check endpoints you should receive a 200 response from the HTTP GET request and a JSON response with the Workspace ONE UEM version. If you receive a 403 response for the Console or Device Services endpoint ensure you restart the app pools after entering the IP address in the Workspace ONE UEM console.

Workspace ONE UEM URL Endpoints for Monitoring

The listed URL endpoints for the various Workspace ONE UEM components can be monitored to ensure a functioning Workspace ONE UEM environment. The endpoints and expected status codes are listed below.

These endpoints are **not** official health checks, but simply endpoints you can monitor to ensure connectivity.

Device Services

Since most typical on-premises 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 Enrollment	/DeviceManagement/enrollment	HTTP 200
App Catalog	/DeviceManagement/appcatalog?uid=0	HTTP 200
Device Services AWCM	/AWCM/Status	HTTP 200
Device Services WinMo Tracker	/DeviceServices/tracker.aspx?id=0	HTTP 302

Console

Description	URL Endpoint	Status code
Web Console	/AirWatch/login	HTTP 200

Secure Email Gateway

Description	URL Endpoint	Status code
ActiveSync Connectivity	/Microsoft-Server-Activesync	HTTP/1.1 401

Secure Email Gateway v2

Description	URL Endpoint	Status code
Service Availability	/	HTTP 200

VMware Tunnel – Proxy Component

Description	URL Endpoint	Status code
HTTPS	https://<TUNNEL_URL>:<HTTPS_Port>	HTTP 407

VMware Tunnel – Per-App VPN Component

Description	URL Endpoint	Status code
Telnet	https://<TUNNEL_URL>:<HTTPS_Port>	Successful Connection

Content Gateway

Description	URL Endpoint	Status code
Content	https://<Content_Gateway_URL>/content/systeminfo	HTTP 403

This endpoint currently only works for the Content Gateway for Windows. If you want to enable monitoring of this endpoint, you will need to enable the following value in the web.config file, which is disabled by default for security considerations: `<add key="enableSystemInfo" value="true" />`.

Remote File Storage

Description	URL Endpoint	Status code
RFS	https://<RFSURL>:<port>/tokens/awhealth	HTTP 200
RFS	https://<RFSURL>:<port>/files/awhealth	HTTP 200
CRE	https://<CREURL>:<port>/tokens/awhealth	Ensure there is no certificate trust error.

Remote Management

Description	URL Endpoint	Status code
RMS	https://<RMS_URL>/health	HTTP 200

Load Balancers

Componen	URL Endpoint	Status coc
VIDM Service (PC)	/SAAS/API/1.0/REST/system/health/heartbeat	HTTP 200

Componen	URL Endpoint	Status coc
VIDM Service (Android)	Certproxy - :526/system/health	HTTP 401
VIDM Service (iOS)	kdc - Telnet 88	Connectio n
VIDM Connector	/hc/API/1.0/REST/system/health/allOK	HTTP 200
Integratio n Broker	IB/API/RestServiceImpl.svc/ibhealthcheck	HTTP 200
Integratio n Broker (XenApp 7.X)	/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenapversion =Version7x	HTTP 200
Integratio n Broker (XenApp 6.X)	/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenapversion =Version75orLater	HTTP 200

Monitor the Workspace ONE UEM Database

Monitor the Workspace ONE UEM database to ensure a fully-functioning, healthy on-premises Workspace ONE UEM environment. The table listed here provides several recommendations for monitoring on the Workspace ONE UEM 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%.
Waiting Tasks	Waiting tasks in the SQL activity monitor must be under 10 on average. Ideally waiting tasks should be between 0 and 2 when compared to 20,000 batch requests per second.
Index Rebuild	Monitor for fragmentation between 10% and 29%. Reorganize with an update of statistics. Indexes with fragmentation greater than 29% should be rebuilt.
Page Life Expectancy	Page Life Expectancy is an indication of whether the database server has memory pressure. The expected number is over 1,000 (seconds). If it is low, this is a first indicator of memory pressure. This may not be an issue if: • The PLE is increasing over time. If it is increasing, but is still less than 1,000, then that is a sign of a memory pressure. • After an index maintenance job, the PLE can be low. This needs to be monitored for a few hours to see if it goes up.

Monitor	Description
Index Fragmentation Level	A high fragmentation level means data retrieval becomes less efficient and reduces database performance. Run the defragmentation job on a nightly basis. The script below shows the fragmentation level (in percent) against all the tables. The recommended fragmentation level is less than 30% when the page size is more than 1,000. `SELECT OBJECT_NAME(object_id), index_id, index_type_desc, index_level, avg_fragmentation_in_percent, avg_Page_space_used_in_percent, page_count FROM sys.dm_db_index_physical_stats(DB_ID(N'AirWatch'), null, null, null, 'SAMPLED') ORDER BY avg_fragmentation_in_percent DESC` If the database is highly fragmented, it is recommended that you perform an index reorganize or rebuild.
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, Workspace ONE UEM 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 Queuing	Monitor Disk Queuing on all Data and Log Drives for 'AirWatch' and 'tempdb' Databases. Check Disk Queue Length via **Task Manager > Performance > Resource Monitor > Dist Tab > Storage**. It should average between 2 and 4. It could increase or decrease, but on average it should be between those values.

Health Checks

Synthetic transactions are the strongest indicator of a healthy Workspace ONE UEM 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 **Workspace ONE UEM console**.
2. Log in using credentials.
3. Navigate to **Hub > Reports & Analytics > Reports > List View**.
4. Run a report.
5. Log out.

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

Chapter 7:
Maintenance

On-Premises Architecture Maintenance Guidelines

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

Workspace ONE UEM Database

Workspace ONE UEM Database Regular database maintenance must be performed. Maintenance standards vary per company. Check with your local database team for best practices. The following table provides Workspace ONE UEM database maintenance guidelines.

Task	Frequency	Description	Responsible Party
Transaction Log Backups	Nightly	Keeps high percentage of free space in the log file.	Customer DBA
Workspace ONE UEM Purge Job	Nightly	Removes expired session data provided by Workspace ONE UEM.	Workspace ONE UEM Built-In Function
Index Rebuild	Nightly	Routine index maintenance, especially after purge job.	Customer DBA
Daily Differential Backup	Nightly	Creates a back up file of database changes since the previous full back up.	Customer DBA
Weekly Full Backup	Weekly	Creates a back up file of the entire database. Full backups can be retained per your 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 use 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 the log file.	Customer DBA
Resize Transaction Log	As Needed	This prevents VLFs and keeps enough free space in the log file.	Customer DBA

Workspace ONE UEM Logs

Over time, it may be necessary to archive or purge old Workspace ONE UEM log files to conserve disk space. If logging is set to verbose on Workspace ONE UEM services or Web sites, archiving or purging can occur more frequently. Hard disk space can be monitored, as noted. If disk space becomes low, Workspace ONE UEM recommends archiving or purging old log files.

The following DOS script can be used to delete Workspace ONE UEM 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

Workspace ONE UEM recommends that auto-update functionality is turned off and manual updates are performed every 2–4 weeks or per your policy.

Chapter 8:
High Availability

On-Premises Architecture High Availability Overview

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

High Availability Support for Workspace ONE UEM Components

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 time.

High availability is achieved by using load balancing and session persistence. See On-Premises Architecture Monitoring Overview on page 52 for information on health checks on the servers. The following table outlines both for each Workspace ONE UEM component.

Contact Workspace ONE Support if you have specific questions or concerns about your specific deployment.

Application Modules	Load Balancing Supported?	Recommended Session Persistence	Recommended Timeout Value
Console	Yes*	Source IP-based persistence	60 minutes
Device Services	Yes	Source IP-based persistence	20 minutes
Workspace ONE UEM Cloud Messaging	Yes	Persistence based on parameter **awcmsessionid** in either the URI or HTTP Header. For more information, see https://support.air-watch.com/articles/115001666028	N/A
VMware Tunnel (Per-App Tunnel)	Yes	Source IP-based persistence**	30 minutes
VMware Tunnel (Proxy)	Yes	Source IP-based persistence	30 minutes
Secure Email Gateway (Classic and V2)	Yes	None***	N/A
Content Gateway	Yes	None	N/A
Unified Access Gateway	Yes	Source IP-based persistence	30 minutes
Remote File Storage	Yes	None	N/A
VMware Identity Manager	Yes	Source IP / SSL session / cookie-based persistence	60 minutes

Application Modules	Load Balancing Supported?	Recommended Session Persistence	Recommended Timeout Value
VMware Enterprise Systems Connector	N/A (see **Note**)	N/A	N/A
VMware Identity Manager Inbound Connector (SecureID Auth)	Yes	Source IP / SSL session / cookie-based persistence	60 minutes
API (SOAP and REST)	Yes	Source IP-based persistence	Idle persistence timeout should be less than the policy retrieval interval to ensure optimal load balancing
Workspace ONE Intelligence	N/A	N/A	N/A
Memcached	N/A	N/A	N/A
Adaptiva	N/A	N/A	N/A
ENS	N/A	N/A	N/A
*The Scheduler and Directory Sync services must be active on only **one** console server. All other services and endpoints of the EUC console can be load-balanced in an active-active configuration.			
**Persistence is not required if the short-lived TCP connections are not interrupted while they are active.			
***Persistence is not required for SEG Classic or V2, but without persistence there may be delays in email flow for newly-enrolled devices. To speed up email flow, consider using SEG V2 and clustering the SEG V2 servers.			

Note: The AWCM component automatically load balances traffic from the VMware Enterprise Systems Connector. It does not require a separate load balancer because there are no incoming connections. To accommodate extra users as part of your sizing requirements you can deploy multiple VMware Enterprise Systems Connectors, which are all load balanced by AWCM.

On-Premises Architecture Load Balancer Considerations

Consider the following when setting up load balancing for Workspace ONE UEM components deployed on premises.

- You can configure load balancers with an algorithm of your choosing. Workspace ONE UEM supports simple algorithms such as Round Robins and more sophisticated ones such as Least Connections.

- The following 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 Workspace ONE UEM.

    If the **Enrollment Session Timeout** values are modified in **AirWatchConsole Settings**, then you must set the **Persistence Timeout** values to the same value.
  - **UEM console:** Session persistence timeout of one hour is required based on the default configuration of Workspace ONE UEM.

    If the **Idle Session Timeout** values are modified in the **AirWatchConsole Settings**, then you must set the **Persistence Timeout** values to the same value.
  - **Secure Email Gateway:** Session persistence timeout value for the Secure Email Gateway must be the same as the persistence timeout value for your Exchange ActiveSync Servers based on recommendations from the Mail Solution vendor.
  - **Mail (EAS) Servers:** Follow the recommendations from your load balancer and mail environment vendors to configure the load balancer in front of one or more EAS servers when using one or more SEGs. In general, Workspace ONE UEM does not recommend using IP-based persistence when using one or more SEGs.
- Workspace ONE UEM recommends load balancers to redirect all HTTP requests to HTTPS.

High Availability for Workspace ONE UEM Database Servers

All critical data and configurations for Workspace ONE UEM are stored in the database and this is the data tier of the solution. Workspace ONE UEM 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.

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

Workspace ONE UEM supports failover clustering to achieve high availability of your database servers.

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

AlwaysOn

The SQL Server AlwaysOn capability combines failover clustering with database mirroring and log shipping. AlwaysOn allows for multiple read copies of your database and a single copy for read-write operations.

For more information about AlwaysOn functionality, see https://msdn.microsoft.com/en-us/library/ff877884.aspx.

If you have the bandwidth to support the traffic generated by Workspace ONE UEM, the Workspace ONE UEM database supports AlwaysOn. The following AlwaysOn functionality has been tested for support:

- Database in an Availability Group
- Availability Group failover

- Secondary Replica promotion to Primary
- Synchronous Replication

For more information about deploying AlwaysOn, see **Database Server Prerequisites** in the **Workspace ONE UEM Installation Guide**, available on docs.vmware.com.

Disaster Recovery

Workspace ONE UEM components can be deployed to accommodate most of the typical disaster recovery scenarios. A robust back up policy for application servers and database servers can restore a Workspace ONE UEM environment in another location with minimal steps.

You can configure disaster recovery for your Workspace ONE UEM solution using whatever procedures and methods meet your DR policies. Workspace ONE UEM has no dependency upon your DR configuration, but Workspace ONE UEM strongly recommends you have some type of failover for DR scenarios. Because 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 require assistance with disaster recovery, contact Workspace ONE Support.

Chapter 9:
Reference Material

List of Workspace ONE UEM Services

The following is a list of Workspace ONE UEM services with descriptions.

Service Name	Service Description
AirWatch Agent Builder Services	Service that generates a CAB file that is available for download from the UEM console.
AirWatch Alert Adapter	The Alert Adapter processes data from Workspace ONE UEM to generate alerts.
AirWatch Alert Delivery Service	Takes alerts from the adapter and delivers them to end users.
AirWatch Background Processor Service	Batch processing for legacy SSRS reports.
AirWatch Batch Processing Service	This service extracts user information from Bulk Import Spreadsheets and puts the data in the Database.
VMware Enterprise Systems Connector	Enables integration with your back-end enterprise resources.
AirWatch Cloud Messaging Service	This service allows device to establish a persistent connection to Workspace ONE UEM. 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 Directory Sync Service	Service used to process directory sync jobs. This was moved from the Scheduler to this new service.
AirWatch EAS Integration Service	Processes mail requests routed through the Workspace ONE UEM Secure Email Gateway.
AirWatch Email Notification Service	This service listens for and sends APNs notifications for the iOS version of AirWatch Inbox.
AirWatch Entity Change Queue Monitor	This service monitors the event log MSMQ and sends the outbound event logs.

Service Name	Service Description
AirWatch GEM Inventory Service	AirWatch GEM Inventory Service communicate instance-specific information to a GEM installation.
AirWatch Integration Service	The Bulk Import Service writes to this queue. Integration Service then reads from this queue.
AirWatch Interrogator Queue Monitor	Processes samples from devices that have been stored in various queues, and writes those samples to the database.
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 Rugged 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 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 Smart Group Service	Consolidates processing of Smart Groups into one service.
AirWatch SMS Service	The messaging service is used by the Web Console to send messages to devices.
VMware Tunnel	Adds Proxy to all your internal resources.
Tunnel Server	Tunnel Server service maintains open connections for communication to Windows Rugged devices.

List of Message Queues

The following is a list of Workspace ONE UEM message queues and descriptions.

Message Queues	Description
apnsoutbound	iOS Outbound APNS Messages

Message Queues	Description
awadminbatchqueue	Workspace ONE UEM Admin Batch Queue
awapplicationeventsample	Application Analytics for iOS Content Locker
awapplicationfeedback	Used for Managed Application feedback samples.
awapplicationlistsample	iOS Application List Samples (From Device)
awappscantpiqueue	App Scan requests to Third-Party Apps
awappwithupdatesqueue	VPP applications auto update
awautodiscovery	Used for auto discovery messages
awbackgroundjobsreports	Batch processing for legacy SSRS reports
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	Workspace ONE UEM Compliance Device Queue
awdepbatchqueue	Separate queue to process DEP syncs and assign profile requests
awdevicecapabilitysample	Workspace ONE UEM Device Capability Sample
awdevicecomplianceattributequeue	TrustPoint integration
awdevicecustomattributelistsample	List of device custom attributes, used primarily by rugged devices (Android, QNX, WinMo, Mac, PCs)
awdevicepolicyrulecompliance evaluationqueue	Handles compliance rule level evaluations on a device context.
awdevicepolicyrulecompliancequeue	Handles compliance rule level evaluations on a device context.
awdevicesampledata	Used for initializing devices for compliance
awdiskencryptionsample	Workspace ONE UEM Disk Encryption Sample
aweventlog	Keeps various events related to device / system activities
awexternaldirectorybatchqueue	Queue for user authentication and directory sync for VMware Identity Manager
awfetchappupdatesqueue	VPP applications auto update
awgpscoordinatesample	Android/BlackBerry/WinMo GPS Coordinate Samples (From Device)
awgpsextendedcoordinatessample	Android/BlackBerry/WinMo Extended GPS Coordinate Samples (From Device)
awintegrationservice	This queue is for handling Web Sense certificate requests asynchronously.
awlogmanagerxml	WinMo LogManager XML Samples (From Device)

Message Queues	Description
awmanagedlicenselistsample	Windows Phone 10 application and license status
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)
awmetricssample	New Product Provisioning
awmobiledatausagesample	Workspace ONE UEM Mobile Data Usage Sample
awnetworkadaptersample	Android/BlackBerry/WinMo Network Adapter Samples (From Device)
awnetworkwlansample	Android/BlackBerry/WinMo Network WLAN Samples (From Device)
awnonmobiledatausagesample	Workspace ONE UEM Non Mobile Data Usage Sample
awoutboundeventlog	Workspace ONE UEM 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 Sample (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
awsmartgrouppublish	Smart Group Publish 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 VMware Tunnel through AWCM

Message Queues	Description
awtunnel	WinMo Tunnel Server (From Tunnel Server)
awupdatelistsample	Microsoft EMM: Handles messages related to Windows Updates Revisions
awuserbatchqueue	Workspace ONE UEM User Batch Queue
awusergroupsbatchqueue	Separate queue to process user group actions (sync user attributes, add missing users)
awvppbulkdeployment	Separate Queue to process Users for VPP bulk registration of users and licenses
awvpplicensesyncqueue	Queue to process the VPP apps for a license sync
awwnsnotification	Windows Notification Service (WNS) Notifications
c2dmoutbound	Android Outbound C2DM Messages
fastlaneapnsoutbound	Admin initiated iOS and GCM Outbound APNs Messages
gcmoutbound	Android Google Cloud Messaging Outbound
sensorchangequeue	Sensor Change Queue
syncdirectoryadminattributesqueue syncdirectoryuserattributesqueue syncdirectorygroupsqueue	Queues for the directory sync service. One queue for each job.
workflow-devicecommands	Workflow – Device Commands

VMware Enterprise Systems Connector Error Codes

The following VMware Enterprise Systems Connector error codes apply only to infrastructure errors. Errors within service operations are not included in the table. For example, if VMware Enterprise Systems Connector has a problem reaching your Active Directory when trying to authenticate a user, an error displays in the system Event Log for Workspace ONE UEM, as well as in the log file, but it would not have an error code number.

Error Codes	Error Type	Error Message	Followed by Exception?
6000	Startup	Cannot read configuration	Yes
6001	Startup	AccIdentifier is missing	No
6002	Startup	AwIdentifier is missing	No
6003	Startup	AwcmUrl is invalid: {AwcmUrl}	Yes
6004	Startup	Unable to load the certificate with thumbprint	Possibly
6005	Startup	Configuration specifies to use a proxy, but no proxy address is provided	No
6006	Startup	Invalid proxyAddress	Yes
6007	Startup	Cannot decrypt the proxy password using the VMware Enterprise Systems Connector certificate	Yes

Error Codes	Error Type	Error Message	Followed by Exception?
6008	Startup	Error while starting listener tasks	Yes
6020	Shutdown	All listener thread have terminated; killing application	No
6021	Shutdown	Attempt to stop background tasks timed out; killing application	No
6022	Shutdown	Error when canceling background tasks	Yes
6030	Update	Update check delay was interrupted by an exception	Yes
6031	Update	Unable to check for update with {AutoUpdateUrl}	Yes
6032	Update	Failed to write the update file	Yes
6033	Update	Unable to verify the update file signature	Yes
6034	Update	Update file was signed by an unexpected certificate: {InfoAboutSigningCert}	No
6035	Update	Unable to rename the update file to remove the .untrusted extension	Yes
6036	Update	Error while checking for or performing update; cannot ensure the service is up-to-date.	Yes
6037	Update	Cannot delete old file: {FilePath}	No
	Update	Cannot delete old folder: {FolderPath}	No
6038	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
6039	Update	Error unloading old AppDomain {Name}	Yes
	Update	It appears that we ran the same version after update	No

Error Codes	Error Type	Error Message	Followed by Exception?
6040	Update	Update check is bypassed. VMware Enterprise Systems Connector is configured to bypass its check for updates; THIS CONFIGURATION IS UNSUPPORTED! It is important to keep VMware Enterprise Systems Connector up-to-date! Please remove the 'bypassUpdate' attribute from the .config file ASAP.	No
	Update	Update check failed to complete. VMware Enterprise Systems 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.	No
	Update	This version is out-of-date. VMware Enterprise Systems 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 VMware Enterprise Systems Connector 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.	No
	Update	This version is out-of-date. VMware Enterprise Systems 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 Console reported an error; you must update VMware Enterprise Systems Connector manually. {ErrorMessageFromConsole} Please obtain a new installer through the Workspace ONE UEM Web Console and upgrade as soon as possible.	No
6041	Update	Unable to determine installed .NET framework version	Yes
		VMware Enterprise Systems Connector can emit some Client messages during the update process with {ServiceType:Op} as Workspace ONE UEM.CloudConnector.DiagnosticService.IComponentUpdater:Check	

Error Codes	Error Type	Error Message	Followed by Exception?
6060	Runtime	VMware Enterprise Systems Connector 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
6061	Runtime	Failed to process a received message	Yes
6062	Runtime	Cannot read request: ({ExceptionType}) {ExceptionMessage}	Yes
	Runtime	Cannot create service instance: ({ExceptionType}) {ExceptionMessage}	Yes
	Runtime	Exception from service operation: ({ExceptionType}) {ExceptionMessage}	Yes
6063	Runtime	Reply task terminated with exception	Yes
6064	Runtime	Reply resulted in {NumberNot1} results from AWCM	No
6065	Runtime	Reply resulted in a {AwcmMessageTypeNotSuccess} result from AWCM	No
6066	Runtime	Error processing service result.	Yes
6080	Client	Error reading VMware Enterprise Systems Connector service timeouts from config file	Yes
6081	Client	Error invoking {ServiceType:Op} via AWCM({UpdateUrl}): Timeout after {Timeout} seconds	No
6082	Client	Error reaching AWCM({UpdateUrl}) to invoke {ServiceType:Op}: {Reason}	Yes
6083	Client	Received a Failure message from AWCM: {ErrorMessage}	No
6084	Client	Response from VMware Enterprise Systems Connector is not authenticated.	No
6085	Client	Response came from wrong VMware Enterprise Systems Connector! Expected: {TargetAppUri}; Actual: {ResponseOriginAppUri}	No
6086	Client	Received an error response to {ServiceType:Op}: {ErrorMessage}	No
6087	Client	Unable to decrypt or deserialize response to {ServiceType:Op}	Yes
6088	Client	Received an invalid message response to {ServiceType:Op}	No

VMware Tunnel – Proxy Component Error Codes

The following sections list out the error codes or messages for the VMware Tunnel Proxy component. You can use these error codes and message to better monitor your Workspace ONE UEM deployment.

Code	Name	Meaning
0	UNKNOWN	Unknown error. A runtime exception while processing the request
1	MISSING_HEADER	Headers are missing. This can include headers such as "Proxy-Authorization". **Possible Cause:** The request was stripped in transit or a bad request was sent from the app. **Possible Solution:** Check all hops between the device and VMware Tunnel to see if another network component (e.g. proxy, VPN) stripped the header.
2	WRONG_ENCODING	Proxy-Authorization header value is not Base64 encoded. **Possible Cause:** The request was stripped in transit or a bad request was sent from the app. **Possible Solution:** Check all hops between the device and VMware Tunnel to see if another network component (e.g. proxy, VPN) stripped the header.
3	TOKENS_DONT_MATCH	Client identification tokens in Proxy-Authorization header do not follow *alg:%s;uid:%s;bundleid:%s* format. ID_FORMAT should contain encryption algorithm, uid and bundleID in a specific format. One or more of these is not present. **Possible Cause:** The request was stripped in transit or a bad request was sent from the app. **Possible Solution:** Check all hops between the device and VMware Tunnel.
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 **Possible Solution:** Check all hops for a stripped certificate.
6	SINGLE_SIGNER	Error thrown if there are multiple signers found in the certificate chain. The request is expected to be signed by only one entity. **Possible Cause:** A bad certificate. **Possible Solution:** Create another certificate with a single signer.
7	SINGLE_SIGNER_CERT	Error thrown if there are multiple certificates for signers. The VMware Tunnel expects only one signer. The request signer should sign it with only one certificate. **Possible Cause:** A bad certificate. **Possible Solution:** Create another certificate with a single signer.
8	INVALID_SIGN	The signer information could not be verified. **Possible Solution:** Import the signer into the trusted certificate store on the server.

Code	Name	Meaning
9	UNTRUSTED_ISSUER	The certificate used for signing wasn't issued by Device-Root of the given OG. **Possible Cause:** Workspace ONE UEM device root is different for enrolled OG and the OG on which VMware Tunnel is configured. **Possible Solutions:** (1) Override the Workspace ONE UEM device root certificate and regenerate the VMware Tunnel certificate. (2) Export the Workspace ONE UEM certificate from the Console or reinstall the VMware Tunnel.
10	MISSING_SIGN_TIME	The signing time attribute which is used to determine potential replay attack is missing in the signature **Possible Cause:** A bad certificate. **Possible Solution:** Determine which certificate is bad in a request log. Create a correct certificate (if the cert is not a Workspace ONE UEM certificate). Re-run the VMware Tunnel installer.
11	POTENTIAL_REPLAY	There is more than a 15 minute interval between signature creation by the requester (AW Browser, Wrapping, etc) and verification by VMware Tunnel
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 VMware Tunnel. Any method other than the "CONNECT" request is sent to the VMware Tunnel and is rejected. **Possible Cause:** An invalid request. **Possible Solution:** Check all hops for what changed with the request at each hop.
13	DATA_UNAVAILABLE	The requester's (AW Browser, Wrapping, etc) related data is not available with VMware Tunnel even after making an API call. No data available for Udid: #####, BundleId: ####. **Possible Cause:** VMware Tunnel does not have device details. **Possible Solutions:** Check the VMware Tunnel to API connection. Restart the VMware Tunnel service.
14	INVALID_THUMBPRINT	The thumbprint of the certificate used by the requester (AW Browser, Wrapping, etc) for signing and the one expected by VMware Tunnel is different. Invalid SHA-1 thumbprint. Udid: ####, BundleId: ####. VMware Tunnel expected: XYZ, Found:ABC **Possible Cause:** Occurs only when device is re-enrolled. **Possible Solutions:** Re-install the Client (AWB, Wrapped App). Check the VMware Tunnel to AWCM connection. Restart VMware Tunnel Service.
15	NOT_COMPLIANT	The device making the request is not compliant (Must be in compliance states of 'Compliant' or 'Not Available'). **Possible Cause:** VMware Tunnel expected: X,Y, Found: Z **Possible Solution:** Check the compliance status in the Device Dashboard.

Code	Name	Meaning
16	NOT_MANAGED	The device is not managed by Workspace ONE UEM. **Possible Cause:** The device is not enrolled. **Possible Solution:** Enroll the device.
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). **Possible Solution:** Identify the invalid certificate.
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 (Classic Platform) Error Codes

The following sections list out the error codes or messages for the Secure Email Gateway (Classic Platform). Use these error codes and message to better monitor your Workspace ONE UEM deployment.

For SEG V2 error codes, see the Workspace ONE UEM Logging Guide, available at https://resources.air-watch.com/view/25j372vpkr24kpp9sd4h/en.

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} . Id: {1}
SEG-11006	Integration Service	Server / Network	AirWatchServiceException encountered while executing {0} . ErrorCode: {1}, Message: {2}
SEG-11007	Integration Service	Server / Network	CallContextException encountered while while executing {0} . 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. 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. HttpException - Status: '{0}', ExMessage: '{1}'
SEG-12014	Gateway Module	Authentication	Client certificate is not valid. 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.

Error Code ID	Component	Area	Message
SEG-12028	Gateway Module	Server / Network	WebException encountered while '{0}'(descriptor) '{1}' (commDirectionText). WebExStatus: '{2}', RequestTid: '{3}', Status Code: '{4}', Status Description: '{5}', ExMessage: '{6}'
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. 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

Error Code ID	Component	Area	Message
SEG-14007	SEG Setup	Setup Validation	The email server's name is empty
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}