Recommended Architecture

for on-premises deployments

VMware Workspace ONE UEM 1907

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction to Workspace ONE UEM Recommended Architecture

1

The Recommended Architecture Guide covers supported topologies, hardware requirements, sizing, and network requirements for deployment of Workspace ONE UEM powered by AirWatch components, guidelines for high availability, suggestions for monitoring your Workspace ONE UEM solution, and more.

This documentation 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.

Every on-premesis deployment of Workspace ONE UEM is unique and poses distinct requirements. This documentation 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 can provide guidance for your specific deployment. Contact VMware for more details.

Workspace ONE UEM Topology

2

The Workspace ONE™ UEM powered by AirWatch software suite is composed of multiple components that work in conjunction to provide a complete mobile device solution.

Understand these components and their operation to deploy them correctly in your instance of Workspace ONE UEM. Not all components are present in every deployment. Consult your Workspace ONE UEM representative and docs.vmware.com for additional information.

This chapter includes the following topics:

Workspace ONE UEM Components

Each Workspace ONE UEM component has a section below with a short summary of their role within the Workspace ONE UEM powered by 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.

Device Services

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

- Device enrollment.
- Application provisioning.
- Delivering device commands and receiving device data.

Device Services also hosts the Self-Service Portal, which device users access (through a Web browser) to monitor and manage their devices in Workspace ONE UEM.

AirWatch Cloud Messaging (AWCM)

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

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

AWCM simplifies device management by offering the following benefits:

- Secure communication to your back-end infrastructure through the VMware AirWatch Cloud Connector.
- Real-time communication with Workspace ONE UEM Windows Intelligent Hub.
- Removing the need for third-party IDs.
- Workspace ONE UEM console commands delivered directly to Android and Windows Rugged devices.
- Remote commands such as device wipe and device lock delivered to macOS devices.
- Increased functionality of internal Wi-fi only devices using push notifications in certain circumstances.

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

API (Application Program Interface)

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 want to start Workspace ONE UEM functionality and use the information stored in their Workspace ONE UEM environment.

By default, the AirWatch API is installed on both CN and DS application servers. It is configured to point to the CN by default.

When developing any new applications, VMware 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 Workspace ONE UEM database, proper sizing of the database server is crucial to a successful deployment.

For more information on system configurations, see the **VMware AirWatch Installation Guide**, available on docs.vmware.com, or contact Workspace ONE Support.

VMware Workspace ONE Access

VMware Workspace ONE Access extends your infrastructure to provide a seamless single sign-on (SSO) experience to web, mobile, software-as-a-service (SaaS), and legacy applications.

VMware Workspace ONE Access provides:

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

For more information on configuring VMware Workspace ONE Access, see the VMware Workspace ONE Access guide, available on docs.vmware.com.

VMware AirWatch Cloud Connector

VMware AirWatch Cloud Connector provides organizations the ability to integrate Workspace ONE UEM and Workspace ONE Access with their back-end enterprise systems. VMware AirWatch Cloud Connector runs in the internal network in outbound connection mode to transmit secure requests from Workspace ONE UEM and Workspace ONE Access to critical enterprise infrastructure components. This allows organizations to harness the benefits of Workspace ONE UEM Mobile Device Management (MDM) and Workspace ONE Access and their existing LDAP, certificate authority, email, and other internal systems, all without inbound port 443 opened.

VMware AirWatch Cloud 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)
- Third-party Certificate Services (on-premesis only)
- Lotus Domino Web Service (HTTPS)
- Syslog (Event log data)

Additional information about VMware AirWatch Cloud Connector requirements, setup, and installation can be found in the AirWatch Cloud Connector documentation.

Workspace ONE AccessConnector

The Workspace ONE Access connector is an on-premesis component of Workspace ONE Access that provides directory integration, user authentication, and integration with resources such as Horizon 7. The connector is deployed in outbound connection mode and, for most use cases, does not require inbound port 443 to be opened. It communicates with the Workspace ONE Access service through a Websocket-based communication channel.

Workspace ONE Access Connector supports optional services such as:

- Horizon
- RSA Secure ID and Adaptive Auth
- Citrix Farms

Additional information about Workspace ONE Access Connector requirements, setup, and installation can be found in the Workspace ONE Access Connector documentation.

VMware AirWatch AirWatch Secure Email Gateway (V2)

Enterprises using certain types of email servers, such as Exchange 2010 or Lotus Traveler, can use the **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.

Workspace ONE UEM 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 Workspace ONE UEM 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.

Beginning with the 1907 release, SEG Classic is no longer available on new deployments. Beginning with Unified Access Gateway 3.6 the SEGv2 image is included in the UAG appliance.

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 9 and higher devices using the VMware Tunnel.

Additional information about VMware 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 Workspace ONE Content, 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 are immediately reflected in the Workspace ONE Content, and users are 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 Workspace ONE Content allows you to provide 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** documentation, available on docs.vmware.com.

AirWatch Email Notification Service (Classic and V2)

The Email Notification Service (ENS) adds push notification support to Exchange on iOS and Android devices.

On iOS, this means the VMware Boxer email app can get notifications using 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 might 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 V2 supports notification services on managed Android devices 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. The Reports feature provides faster, easier access to critical business intelligence data than normal Workspace ONE UEM reports. 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 **Workspace ONE UEM Mobile Application Management (MAM) Guide**, which includes configuration and installation, from docs.vmware.com.

Memcached

As deployments begin to scale over 1,000 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 must be made to the database. After caching is configured, the Workspace ONE UEM components 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 then store the value on the cache server for future use.

For more information on configuring Memcached, see the **Memcached Integration** guide, available on docs.vmware.com. If the Memcached setting is not available, reach out to VMware support for assistance.

Airlift

VMware Workspace ONE AirLift is a server-side connector that simplifies and speeds the customers journey to modern management. Workspace ONE AirLift bridges administrative frameworks between Microsoft System Center Configuration Manager (ConfigMgr) and Workspace ONE UEM.

This bridge allows the customer to focus on moving co-management workloads and applications to the appropriate platform without redefining device and group memberships. Workspace ONE AirLift provides seamless adoption of co-management benefits and eases the transition on a collection by collection basis addressed toward particular use cases.

For more information on configuring Airlift, see the **Airlift Integration** guide, available on docs.vmware.com. If the Memcached setting is not available, contact VMware support for assistance.

Dell Factory Provisioning

In partnership with Dell Configuration Services, Workspace ONE UEM supports creating provisioning packages to install applications and configurations on your Dell Windows 10 devices before they leave the factory.

Dell Provisioning for VMware Workspace ONE requires on-premesis customers to install the Dell Provisioning for VMware Workspace ONE service onto a standalone application server. To set up and configure Factory Provisioning, see the **Workspace ONE UEM Windows Desktop Guide**, available at docs.vmware.com.

To use Dell Provisioning for VMware Workspace ONE, you must participate in Dell Configuration Services. For more information, see https://www.dell.com/en-us/work/learn/system-configuration.

Workspace ONE UEM on-premesis Deployment Model

Workspace ONE UEM can be deployed on-premesis in various configurations to suit diverse business requirements. When deployed within a network infrastructure, Workspace ONE UEM can adhere to strict corporate security policies by storing all data on site. In addition, Workspace ONE UEM has been designed to run on virtual environments, which creates seamless deployments on several different setups.

The primary difference between deployment sizes (by number of devices) is how Workspace ONE UEM components 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 VMware support to discuss the possible server combinations that best suit your needs. For more information on hardware sizing, see Chapter 3 on-premesis Recommended Architecture Hardware Sizing Overview.

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. Consult your Workspace ONE UEM representative for information about supported technologies, 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.workspaceone.com/articles/115001665868.

Standard Deployment Model

In a standard Workspace ONE UEM deployment, you use multiple servers for the various components. 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.

While these components are combined in some 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 Chapter 3 on-premesis Recommended Architecture Hardware Sizing Overview. Contact Workspace ONE UEM and schedule a consultation to discuss the appropriate server configuration for your on-premesis deployment.

Cross-Datacenter Latency

There are many server configurations you can apply to your particular network setup, each with distinct requirements and benefits. In setting up your network, server latency can be a critical factor in network performance.

If you deploy servers in an active-active cross-datacenter configuration, the latency between those servers should not exceed 5 milliseconds. Longer latency times can create adverse effects on the performance of some services and increase webpage loading times.

For detailed configurations based on deployment sizing, see Chapter 3 on-premesis Recommended Architecture Hardware Sizing Overview.

For an overview of an on-premesis deployment model, see Workspace ONE UEM on-premesis Deployment Model.

on-premesis Recommended Architecture Hardware Sizing Overview

3

Sizing for a Workspace ONE UEM environment begins with an initial assessment of critical factors to provide a clear view of system use.

When determining the required hardware specifications for 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 might 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. Workspace ONE UEM continually conducts performance testing to validate sizing requirements and as such the figures listed in this section might change over time.

This chapter includes the following topics:

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 UEM 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 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 Workspace ONE UEM 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 Workspace ONE UEM 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
VMware Workspace ONE Access		See VMware Workspace ONE Access Hardware Sizing	
VMware AirWatch Cloud Connector		See VMware AirWatch Cloud Connector Server Hardware Sizing	
Connector		See Workspace ONE AccessConnector	
SEG Proxy Server		See Secure Email Gateway Server Hardware Sizing	
VMware Tunnel		See VMware Tunnel and Unified Content Gateway (Tunnel) Hardware Sizing	
Email Notification Service		See Email Notification Service Hardware Sizing	

	Up to 5,000 Devices	Up to 25,000 Devices
Content Gateway	See AirWatch Content Gateway and Unified Access Gateway (Content Gateway) Hardware Sizing	
Workspace ONE Intelligence	See Workspace ONE Intelligence Connector	
Adaptiva	See Adaptiva	
Memcached	See Memcached	
Airlift	See VMware Workspace ONE Airlift	
Dell Factory Provisioning	See Dell Factory Provisioning	

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

Figure 3-1. Server Sizing Topology (Up to 5,000 Devices)

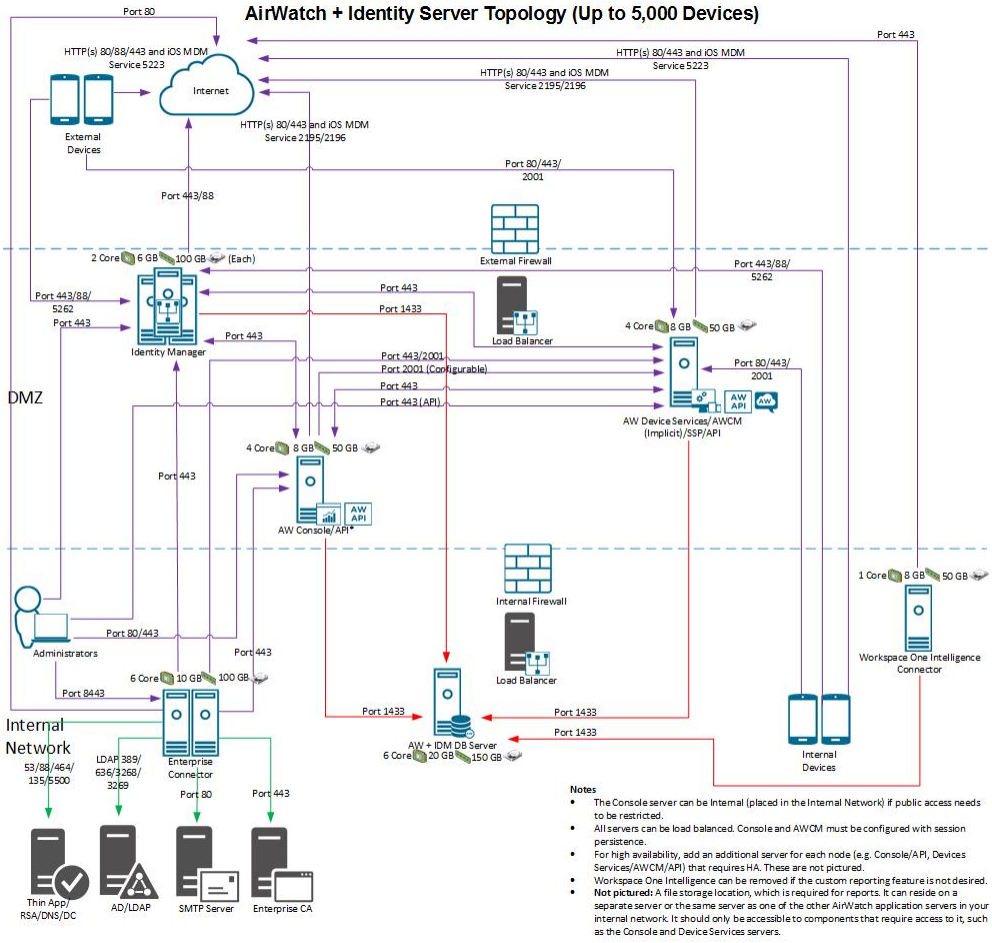
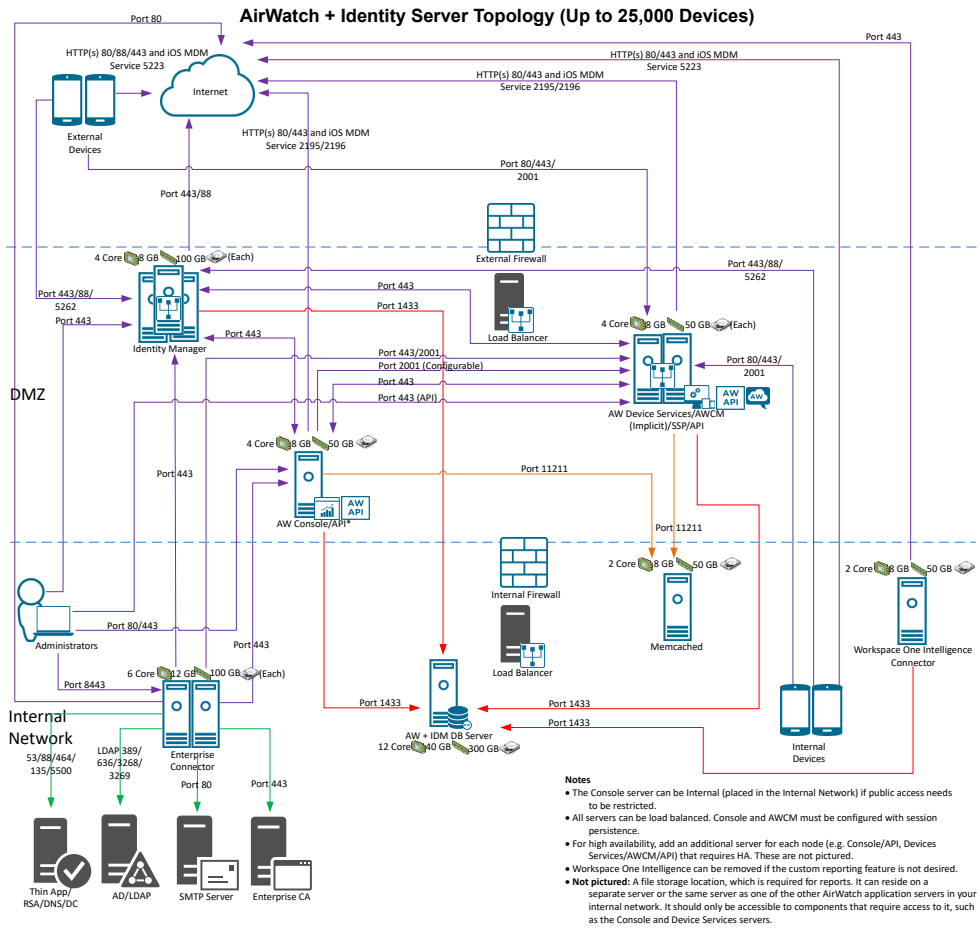


Figure 3-2. Server Sizing Topology (Up to 25,000 Devices)



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 UEM 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.

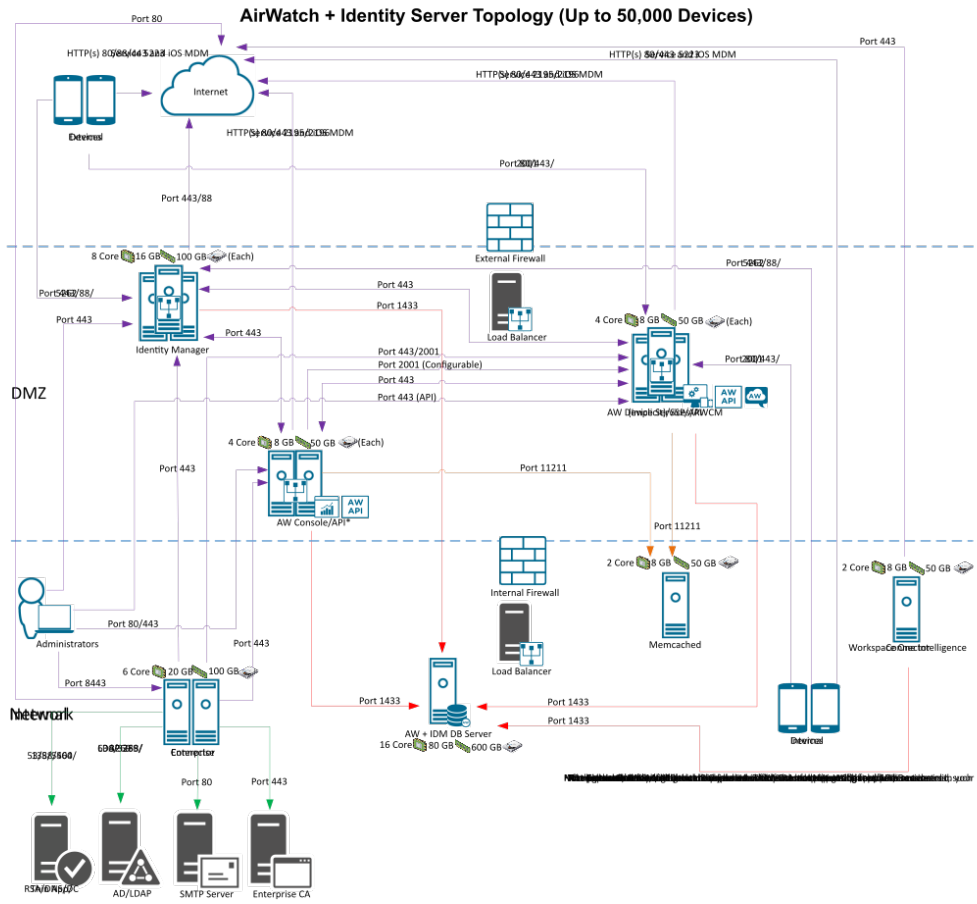
- The file storage requirement for reports may affect the amount of hard disk space needed on the Console and Device Services servers, depending on whether you enable caching. See Reports Storage Requirements for more information.

Server		Up to 50,000 Devices
Database server	CPU/Cores	8-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
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
AWCM Server (Dedicated with 40K+ Windows 10 or Android devices)		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 Workspace ONE Access		See VMware Workspace ONE Access Hardware Sizing
VMware Enterprise Systems Connector		See VMware AirWatch Cloud Connector Server Hardware Sizing
Workspace ONE Access Connector		See Workspace ONE AccessConnector
VMware AirWatch Cloud Connector		See VMware AirWatch Cloud Connector Server Hardware Sizing
SEG Proxy Server		See Secure Email Gateway Server Hardware Sizing
VMware Tunnel		See VMware Tunnel and Unified Content Gateway (Tunnel) Hardware Sizing
Email Notification Service		See Email Notification Service Hardware Sizing
Workspace ONE Intelligence		See Workspace ONE Intelligence Connector
Adaptiva		See Adaptiva
Memcached		See Memcached

Server	Up to 50,000 Devices
Airlift	See VMware Workspace ONE Airlift
Dell Factory Provisioning	See Dell Factory Provisioning

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

Figure 3-3. Server Sizing Topology (Up to 50,000 Devices)



Workspace ONE UEM API Endpoint Installation

Because 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 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 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 Workspace ONE UEM Installation

documentation, which includes this task as part of the post-installation process. Using the API endpoint on the Device Services server might increase the sizing requirements for the server. These requirements depend on how you use the APIs, with heavy use resulting in different sizing numbers. Because 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 reinstall 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 more than 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 UEM if you require extra assistance.

Additional notes to consider:

- If your deployment uses a shared database, you must ensure that the database optimizations in this guide do not adversely affect the other running DB instances. If you cannot ensure this, use a dedicated DB server.
- 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 for more information.

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

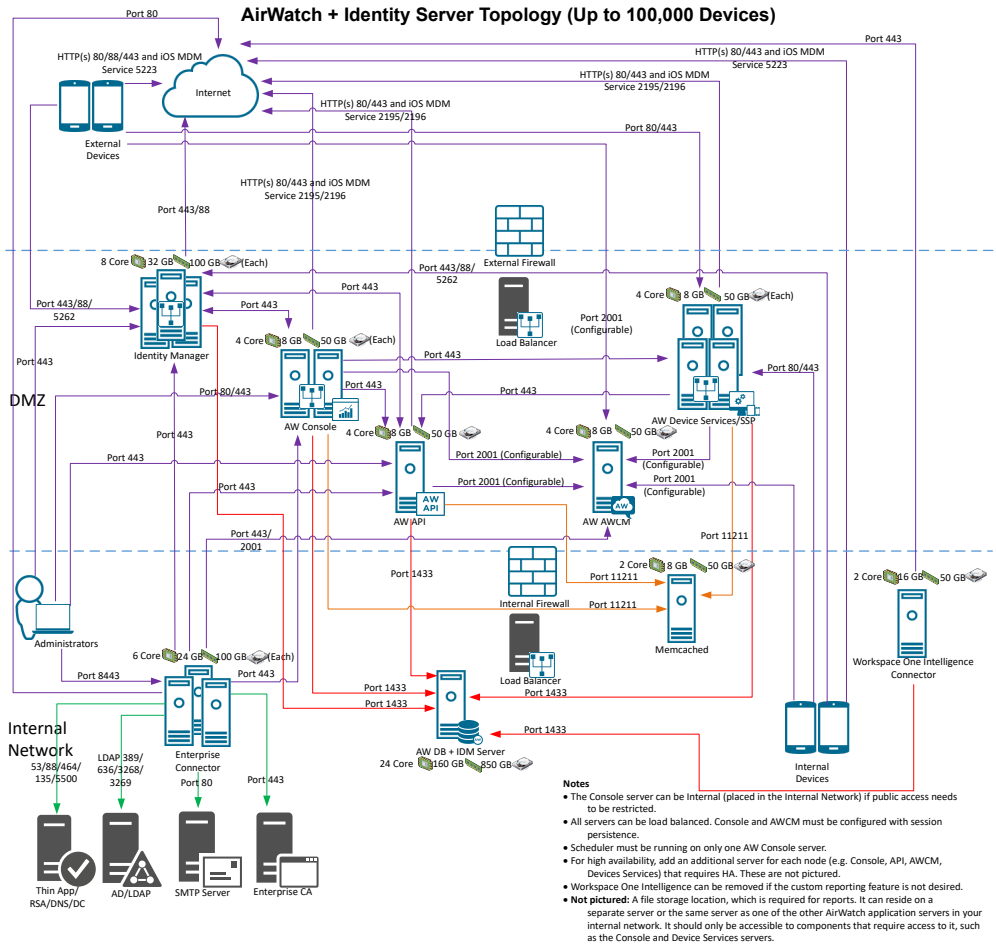
Server		Up to 100,000 Devices
Database server	CPU Cores	16 cores
	RAM (GB)	128
	DB Size (GB)	750

Server		Up to 100,000 Devices
	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
AWCM Server (dedicated)		1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage
AWCM Server (Dedicated with 40K+ Windows 10 or Android devices)		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 Workspace ONE Access		See VMware Workspace ONE Access Hardware Sizing
Workspace ONE Access Connector		See Workspace ONE UEM Components
VMware AirWatch Cloud Connector		See VMware AirWatch Cloud Connector Server Hardware Sizing
SEG Proxy Server		See Secure Email Gateway Server Hardware Sizing
VMware Tunnel		See VMware Tunnel and Unified Content Gateway (Tunnel) Hardware Sizing
Email Notification Service		See Email Notification Service Hardware Sizing
Content Gateway		See AirWatch Content Gateway and Unified Access Gateway (Content Gateway) Hardware Sizing
Workspace ONE Intelligence		See Workspace ONE Intelligence Connector
Adaptiva		See Adaptiva
Memcached		See Memcached
Airlift		See VMware Workspace ONE Airlift
Dell Factory Provisioning		See Dell Factory Provisioning

** 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.

Figure 3-4. Server Sizing Topology (Up to 100,000 Devices)



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

Configure your servers, connectors, and other components for on-premesis Workspace ONE UEM deployments of between 50,000 and 100,000 Rugged 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. Due to special sizing and configuration challenges, contact Workspace ONE UEM for help setting up a Rugged deployment of this size.

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 for more information.

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

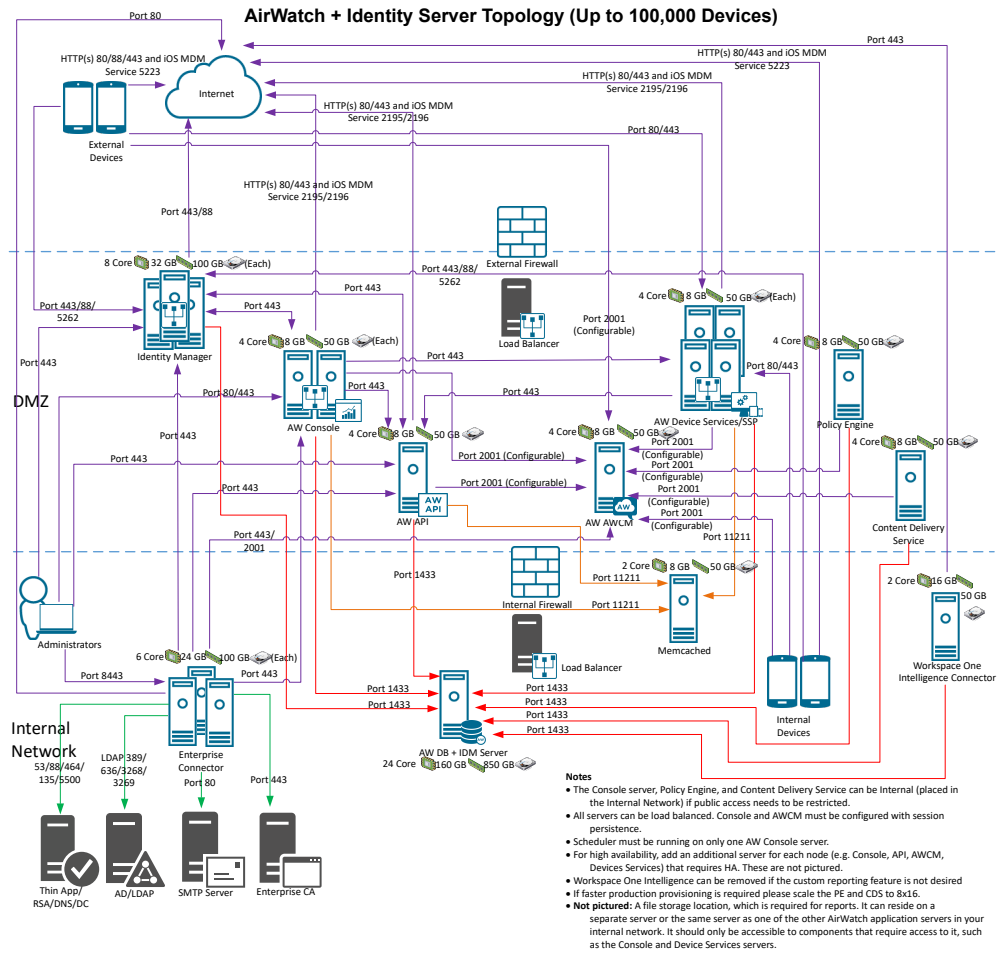
Server		**Up to 100,000 Devices**
Database server	CPU Cores	16 cores
	RAM (GB)	128
	DB Size (GB)	750
	Trans Log Size (GB) (Log backups every 15 minutes)	400
	Temp DB (GB)	300
	Avg IOPS (DB & Temp DB)	2,000
	Peak IOPS (DB & Temp DB)	6,000
UEM console (dedicated)		2 load-balanced application servers, each 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
AWCM Server (dedicated)		1 application server with 4 CPU cores, 8 GB RAM, and 50 GB storage 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.

Server	Up to 100,000 Devices
VMware Workspace ONE Access	See VMware Workspace ONE Access Hardware Sizing
Policy Engine	1 policy engine server with 4 CPU cores, 8 GB RAM, and 50 GB storage
Content Delivery Service	1 CDS server with with 4 CPU cores, 8 GB RAM, and 50 GB storage
Workspace ONE Access Connector	See Workspace ONE AccessConnector
VMware AirWatch Cloud Connector	See VMware AirWatch Cloud Connector Server Hardware Sizing
SEG Proxy Server	See Secure Email Gateway Server Hardware Sizing
VMware Tunnel	See VMware Tunnel and Unified Content Gateway (Tunnel) Hardware Sizing
Email Notification Service	See Email Notification Service Hardware Sizing
Content Gateway	See AirWatch Content Gateway and Unified Access Gateway (Content Gateway) Hardware Sizing
Workspace ONE Intelligence	See Workspace ONE Intelligence Connector
Adaptiva	See Adaptiva
Memcached	See Memcached
Airlift	See VMware Workspace ONE Airlift
Dell Factory Provisioning	See Dell Factory Provisioning

** 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.

Figure 3-5. Server Sizing Topology (up to 100,000 Rugged devices)



on-premesis 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.

Additional requirements for the components listed below can be found in their respective sections. View the sizing tables at On-Premises Architecture Sizing for up to 5,000 and 25,000 Devices, On-Premises Architecture Sizing for up to 50,000 Devices, or On-Premises Architecture Sizing for up to 100,000 Devices.

General Assumptions

- High Availability is easily accomplished in Workspace ONE UEM but affects your requirements. Contact Workspace ONE UEM 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. Workspace ONE UEM 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.
- Workspace ONE UEM and Workspace ONE Access are implemented on a standalone DB.

Other Workspace ONE UEM 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 Workspace ONE Access Hardware Sizing

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

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 VMware Workspace ONE Access, 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 AirWatch Cloud Connector Server Hardware Sizing

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

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 servers with 2 CPU cores	2 servers with 2 CPU cores	3 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

Notes:

- Multiple VMware AirWatch Cloud 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 AirWatch Cloud Connector application, Windows OS, and .NET runtime. Additional disk space is allocated for logging.

Workspace ONE Access Hardware Sizing

The Workspace ONE Access Connector component has the following additional requirements. If you are installing both the ACC and Workspace ONE Access components, add these requirements to the ACC requirements.

Number of Users	1,000 to 10,000	10,000 to 25,000	25,000 to 50,000	50,000 to 100,000
Workspace ONE Access 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:

- 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 Workspace ONE Access 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.

Concurrent Connections	Up to 6,000	6,000 to 10,000	10,000 to 50,000	50,000 to 100,000	100,000 to 150,000	150,000 to 200,000
Max with Transformation enabled	4000	6000	35000	70000	100000	140000
UAG Sizing	4GB RAM / 2vCPU	4GB RAM / 2 vCPU	16GB RAM / 4vCPU	16GB RAM / 4vCPU	32GM RAM / 8vCPU	32GM RAM / 8vCPU
Number of UAG Appliances**	2*	3	5	8	6	9

Notes for SEG deployments:

- * It is possible to deploy only a single UAG Appliance as part of a smaller deployment. However, VMware recommends deploying at least 2 load-balanced appliances.
- ** Numbr of UAG Appliances include HA n+1
- 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 UEM.

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 UEM. 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

Requirement	CPU Cores	RAM (GB)	Disk Space	Notes
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

Table 3-1.

CPU Cores	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. For instructions on enabling reports storage in the Workspace ONE UEM Console, see Reports Storage Requirements.

Workspace ONE Intelligence Connector

	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

Dell Factory Provisioning

Factory Provisioning hardware requirements are not necessarily related to the number of devices in your organization. The hardware requirements correlate to the number of concurrent provisioning packages that you request. These hardware requirements assume a maximum package size of 25 GB and a maximum of 3 concurrent packages requested at a time.

Dell Factory Provisioning Service should be installed on a standalone server meeting these requirements.

Table 3-2. Dell Factory Provisioning Service Server Requirements

Component	3 Packages (25 GB)
Servers	1
CPUs	2 (2 GHz Intel processor)
Memory	6GB (Windows Server)
Storage	100GB

VMware Workspace ONE Airlift

Table 3-3. Workspace ONE Airlift Server Requirements

Component	Requirement
Servers	1
CPUs	2 (2 Ghz Intel processor)
Memory	4GB
Storage	1GB disk space for the Airlift application, operating system, and .NET core runtime. Consider allocating 5GB of disk space.

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 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 can 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

Separate the managed content from the Workspace ONE UEM database by storing it in a dedicated File Storage. To set up a file storage, you must determine the location and storage capacity for your file storage, configure the network requirements, and create an impersonation account.

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 Workspace ONE UEM 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 supply the domain during service account configuration in the format <domain \username>. Domain Trust can also be established to avoid authentication failure.

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 in the domain of the shared storage directory.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure File Storage Impersonation User in Workspace ONE UEM with the domain account in the format <domain\username>.
- If the shared storage directory is not on a domain, create an identical local user and password on the server being used for File Storage, Console, and Device Services server. In this case, supply the local user account in the format <username>.

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.

on-premesis Architecture Software Requirements

4

Workspace ONE UEM powered by AirWatch has software requirements that provide the foundation necessary for a proper configuration and efficient workflow.

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 SP1, Windows Server 2012 R2, or Windows Server 2016
  - For Windows Server 2008 R2, ensure that your Windows installation includes KB2999226 and KB2533623 to avoid errors when you launch a .NET Core application.
  - For Windows Server 2012 R2, ensure that your Windows installation includes KB2999226 to avoid errors when you launch a .NET Core application.
- 64-bit Java (8u241) 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 (8u241) installed on all application servers. The Java installer is packaged with the Workspace ONE UEM installer and installs if it is not already present.
- .NET Framework 4.8. The .NET Framework 4.8 installer is packaged with the Workspace ONE UEM installer and installs automatically if it is not already present. .NET 4.7 and 4.7.1 are also supported.
- .NET CORE 2.2.6
- 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, SQL Server 2016, or SQL Server 2017 with Client Tools (SQL Management Studio, 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.
- Set SQL max memory to be 80% of total memory available.
- Enable locking pages in memory to prevent Windows from swapping the SQL service out of memory.
- Choosing to cycle the error log and agent error log each day prevents individual log files from becoming too large and unmanageable.
- Enable instant file initialization (IFI). To enable IFI, grant the policy to the Windows service account and restart the SQL Server service.
- .NET 4.6.2 is required to run the database installer, .NET 4.7 and 4.7.1 are also supported. 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 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

This chapter includes the following topics:

Workspace ONE UEM Database Performance Recommendations

Workspace ONE UEM powered by AirWatch provides a database of performance recommendations based on scalability tests performed by the Workspace ONE UEM team.

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 need 8 tempDBs, 12 cores need 12 tempDBs, 13 cores need 12 tempDBs, 16 cores need 16 tempDBs.) File size, growth rate, and the location must be the same for all tempDB files.
Memory Allocation	80% 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 if there is 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/)
Trace Flag - SQL Server 2016	See https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-traceontrace- flags-transact-sql/view=sql-server-2017
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 doesn't 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 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.
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.
Autogrowth	For Production and Temp DBs, set Autogrowth to 128MB and max size to Unlimited.

For device deployments above 150,000 devices, ensure that the Database is partitioned. You can 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.

on-premesis Architecture Network Requirements

5

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 applications and services.

For the ports listed below, all traffic is uni-directional (outbound) from the source component to the destination component. Workspace ONE UEM supports IPv6 protocol for all ports and components.

Console Server Ports

Source Component	Destination Component	Protocol	Port	Notes+
UEM console Hostname	discovery.awmdm.com	HTTPS	443	Optional, for AutoDiscovery
UEM console Hostname	signing.awmdm.com	HTTPS	443	Mandatory for Workspace ONE Baselines. Optional, for AutoDiscovery
UEM console Hostname	awcp.air-watch.com	HTTPS	443	Optional, for APNs Certificate. Proxy Connections not supported.
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	appwrapandroid.awmdm.com	TCP	443	Android only
UEM console Hostname	fcm.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.

Source Component	Destination Component	Protocol	Port	Notes+
UEM console Hostname	fcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; DPC Communication
UEM console Hostname	android.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
UEM console Hostname	*gvt2.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
UEM console hostname	*gvt3.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
UEM console hostname	cri.pki.goog	CRL	443, 80	certificate validation
UEM console hostname	ocsp.pki.goog	CRL	443, 80	certificate validation
UEM console Hostname	pki.google.com	TCP	443	Android only. Certificate revocation.
UEM console Hostname	clients1.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	clients2.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	clients3.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	clients4.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	clients5.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	clients6.google.com	TCP	443	Android only. Google backend services.
UEM console Hostname	android.com	TCP TCP, UDP	443 5228-5230	Android only
UEM console Hostname	*.googleapis.com	TCP	443	Android only. Google APIs, Play Store APIs.
UEM console Hostname	accounts.google.com	TCP	443	Android only. Authentication.
UEM console Hostname	play.google.com	TCP TCP, UDP	443 5228-5230	Android only
UEM console Hostname	android.clients.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
UEM console Hostname	fonts.googleapis.com	HTTP/ HTTPS	80 or 443	For fonts used in the UEM console
UEM console Hostname	google-analytics.com	TCP TCP, UDP	443 5228-5230	

Source Component	Destination Component	Protocol	Port	Notes+
UEM console Hostname	googleusercontent.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
UEM console Hostname	gstatic.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
UEM console Hostname	*.gvt1.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
UEM console Hostname	*.ggpht.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
UEM console Hostname	dl.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
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
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	**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	mdmenrollment.apple.com	TCP	443	Apple iOS, tvOS, and macOS only
UEM Console Hostname	api.push.apple.com	HTTPS	443	Apple iOS and macOS only

Source Component	Destination Component	Protocol	Port	Notes+
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
UEM console Hostname	CRL: http://crl3.digicert.com/sha2-assured-cs-g1.crl http://crl4.digicert.com/sha2-assured-cs-g1.crl	HTTP	80	Supports code-signing verification of Workspace ONE UEM code post-installation.
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 on-premesis Architecture Hardware Assumptions.
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
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
UEM console Hostname	Memcached	TCP	1211	Memcached outbound communications

Console Server Admin API Ports

Source Component	Destination Component	Protocol	Port	Notes
Admin Browser	VMware Workspace ONE Access	HTTPS	443	Astro APIs
Admin Browser	UEM console Hostname	HTTPS	443	Console Access
Admin Browser	API Server Hostname	HTTPS	443	Astro APIs

API Server Ports (if standalone)

Source Component	Destination Component	Protocol	Port	Notes
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 Workspace ONE Access without the use of VMware Enterprise Systems Connector.
API Server Hostname	vmwarebaselines.com	HTTPS	443	AWS-hosted VMware Policy Catalog Service. Mandatory for Workspace ONE Baselines.
API Server Hostname	android.googleapis.com play.google.com	HTTP/ HTTPS	80 or 443	For Cloud Messaging for Android devices.
API Server Hostname	appwrapandroid.awmdm.com	HTTPS	443	Workspace ONE UEM Cloud Android App Wrapping Service
API Server Hostname	appwrapandroid.awmdm.com	TCP	443	Android only
API Server Hostname	gcm-http.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
API Server Hostname	gcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.
API Server Hostname	fcm.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.
API Server Hostname	fcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; DPC Communication

Source Component	Destination Component	Protocol	Port	Notes
API Server Hostname	android.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
API Server Hostname	pki.google.com	TCP	443	Android only. Certificate revocation.
API Server Hostname	clients1.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	clients2.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	clients3.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	clients4.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	clients5.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	clients6.google.com	TCP	443	Android only. Google backend services.
API Server Hostname	android.com	TCP TCP, UDP	443 5228-5230	Android only
API Server Hostname	*.googleapis.com	TCP	443	Android only. Google APIs, Play Store APIs.
API Server Hostname	accounts.google.com	TCP	443	Android only. Authentication.
API Server Hostname	play.google.com	TCP TCP, UDP	443 5228-5230	Android only
API Server Hostname	android.clients.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
API Server Hostname	fonts.googleapis.com	HTTP/ HTTPS	80 or 443	For fonts used in the UEM console
API Server Hostname	google-analytics.com	TCP TCP, UDP	443 5228-5230	
API Server Hostname	googleusercontent.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
API Server Hostname	gstatic.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
API Server Hostname	*.gvt1.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
API Server Hostname	*.ggpht.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.

Source Component	Destination Component	Protocol	Port	Notes
API Server Hostname	dl.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
API Server Hostname	*gvt2.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
API Server Hostname	*gvt3.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
API Server Hostname	cri.pki.goog	CRL	443, 80	certificate validation
API Server Hostname	ocsp.pki.goog	CRL	443, 80	certificate validation
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, 2197	For Apple iOS and macOS cloud messaging. Proxy Connections not supported.
API Server Hostname	mdmenrollment.apple.com	TCP	443	Apple iOS, tvOS, and macOS only
API Server Hostname	api.push.apple.com	HTTPS	443	For Apple iOS and macOS cloud messaging. Proxy Connections not supported
API Server Hostname	Memcached	TCP	1211	Memcached outboung communications

Workspace ONE Access Admin API Ports

Source Component	Destination Component	Protocol	Port	Notes
Workspace ONE Access Service	API Server Hostname	HTTPS	443	Auth Token Request
API Server Hostname	VMware Workspace ONE Access	HTTPS	443	Astro APIs

Device Services Server Ports

Source Component	Destination Component	Protocol	Port	Notes
Device Services Hostname	discovery.awmdm.com	HTTPS	443	Optional – For auto discovery functionality
Device Services Hostname	signing.awmdm.com	HTTPS	443	Optional – For auto discovery functionality
Device Services Hostname	gateway.push.apple.com	TCP	2195	Apple only

Source Component	Destination Component	Protocol	Port	Notes
Device Services Hostname	feedback.push.apple.com	TCP	2196	Apple only
Device Services Hostname	www.google.com	HTTPS	443	Google devices running Android 8.0+
Device Services Hostname	appwrapandroid.awmdm.com	HTTPS	443	Workspace ONE UEM Cloud Android App Wrapping Service
Device Services Hostname	appwrapandroid.awmdm.com	TCP	443	Android only
Device Services Hostname	gcm-http.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
Device Services Hostname	gcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.
Device Services Hostname	fcm.googleapis.com	TCP	443, 5228-5230	Android only; Firebase Cloud Messaging. Proxy Connections not supported.
Device Services Hostname	fcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; DPC Communication
Device Services Hostname	android.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
Device Services Hostname	pki.google.com	TCP	443	Android only. Certificate revocation.
Device Services Hostname	clients1.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	clients2.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	clients3.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	clients4.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	clients5.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	clients6.google.com	TCP	443	Android only. Google backend services.
Device Services Hostname	android.com	TCP TCP, UDP	443 5228-5230	Android only
Device Services Hostname	*.googleapis.com	TCP	443	Android only. Google APIs, Play Store APIs.
Device Services Hostname	accounts.google.com	TCP	443	Android only. Authentication.
Device Services Hostname	play.google.com	TCP TCP, UDP	443 5228-5230	Android only

Source Component	Destination Component	Protocol	Port	Notes
Device Services Hostname	android.clients.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Device Services Hostname	fonts.googleapis.com	HTTP/ HTTPS	80 or 443	For fonts used in the UEM console
Device Services Hostname	google-analytics.com	TCP TCP, UDP	443 5228-5230	
Device Services Hostname	googleusercontent.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
Device Services Hostname	gstatic.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
Device Services Hostname	*.gvt1.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Device Services Hostname	*gvt2.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
Device Services Hostname	*gvt3.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
Device Services Hostname	cri.pki.goog	CRL	443, 80	certificate validation
Device Services Hostname	ocsp.pki.goog	CRL	443, 80	certificate validation
Device Services Hostname	*.ggpht.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Device Services Hostname	dl.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
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. Proxy Connections not supported.
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

Source Component	Destination Component	Protocol	Port	Notes
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
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	mdmenrollment.apple.com	TCP	443	Apple iOS, tvOS, and macOS only
Device Services Hostname	api.push.apple.com	HTTPS	443	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://crl4.digicert.com/sha2-assured-cs-g1.crl	HTTP	80	Supports code-signing verification of Workspace ONE UEM code post-installation.
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.
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.

Source Component	Destination Component	Protocol	Port	Notes
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 on-premesis Architecture Hardware Assumptions.
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
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
Device Services Hostname	Memcached	TCP	1211	Memcached outbound communications

VMware Workspace ONE Access Ports

Source Component	Destination Component	Protocol	Port	Notes
Load Balancer	VMware Workspace ONE Access	HTTPS	443	
Workspace ONE Accessservice	VMware Workspace ONE Access	HTTPS	443	
Browsers	VMware Workspace ONE Access	HTTPS	443	
Workspace ONE Access service	vapp-updates.vmware.com	HTTPS	443	Access to the upgrade server
Browsers	VMware Workspace ONE Access	HTTPS	8443	Administrator Port

Source Component	Destination Component	Protocol	Port	Notes
Workspace ONE Access service	SMTP	SMTP	25	Port to relay outbound mail
Workspace ONE Access service	Active Directory	LDAP, LDAPS, MSFT-GC, MSFT-GC-SSL	389, 636, 3268, 3269	Default values are listed. These ports are configurable.
Workspace ONE Access service	VMware ThinApp repository	TCP	445	Access to the ThinApp repository
Workspace ONE Access service	RSA SecurID system	UDP	5500	Default value is listed. This port is configurable.
Workspace ONE Access service	DNS server	TCP/UDP	53	Every Workspace ONE Access server must have access to the DNS server on port 53 and allow incoming SSH traffic on port 22.
Workspace ONE Accessservice	Domain controller	TCP/UDP	88,464,135	
Workspace ONE Access service	VMware Workspace ONE Access	TCP	9300-9400	Audit needs
Workspace ONE Access service	VMware Workspace ONE Access	TCP	54328	Audit needs
Workspace ONE Access service	Workspace ONE Access Database	TCP	1433, 5432, 1521	Microsoft SQL default port is 1433. The PostgreSQL default port is 5432. The Oracle default port is 1521.
Workspace ONE Accessservice	View server		443	Access to View server.
Workspace ONE Access 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.
Workspace ONE Accessservice	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.
Workspace ONE Access service	Cloud-hosted KCD	UDP	88	Port used for Kerberos traffic from the Workspace ONE Access to the hosted cloud KDC service.
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.

Source Component	Destination Component	Protocol	Port	Notes
iOS mobile device	VMware Workspace ONE Access	TCP/UDP	88	Port used for Kerberos traffic from iOS device to the built-in KDC
iOS mobile device	VMware Workspace ONE Access	UDP	88	Port used for Kerberos traffic from iOS device to the hosted cloud KDC service.
iOS mobile device	VMware Workspace ONE Access	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 Workspace ONE Access	HTTP	80	Required
Workspace ONE Access service	Ehcache		40002	
Workspace ONE Accessservice	RabbitMQ		4269, 5700, and 25672	
Workspace ONE Accessservice	Elasticsearch		9200, 9300, 443, 8443, 80	
Workspace ONE Access service	Android SSO		5262	
Workspace ONE Access service	Browsers	HTTPS	6443	For certificate authentication configured in a Workspace ONE Access on premises DMZ deployment.

VMware Workspace ONE Access Admin API Ports

Source Component	Destination Component	Protocol	Port	Notes
UEM console Hostname	VMware Workspace ONE Access	HTTPS	443	Astro APIs

End-User Device Ports

Source Component	Destination Component	Protocol	Port	Notes
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.

Source Component	Destination Component	Protocol	Port	Notes
Devices (Internet/Wi-Fi)	*.push.apple.com	TCP	443, 80, 5223, 2197	Push notifications
Devices (Internet/Wi-Fi)	gdmf.apple.com	TCP	443	MDM server to identify which software updates are available to devices that use managed software updates.
Devices (Internet/Wi-Fi)	deviceenrollment.apple.com	TCP	443	DEP provisional enrollment.
Devices (Internet/Wi-Fi)	deviceservices-external.apple.com	TCP	443	
Devices (Internet/Wi-Fi)	identity.apple.com	TCP	443	APNs certificate request portal.
Devices (Internet/Wi-Fi)	iprofiles.apple.com	TCP	443	Hosts enrollment profiles used when devices enroll in Apple School Manager or Apple Business Manager through Device Enrollment
Devices (Internet/Wi-Fi)	mdmenrollment.apple.com	TCP	443	MDM servers to upload enrollment profiles used by clients enrolling through Device Enrollment in Apple School Manager or Apple Business Manager, and to look up devices and accounts.
Devices (Internet/Wi-Fi)	vpp.itunes.apple.com	TCP	443	MDM servers to perform operations related to Apps and Books, like assigning or revoking licenses on a device.
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. Proxy Connections not supported.
Devices (Internet/Wi-Fi)	play.google.com	HTTPS	443	For App Management, Android only
Devices (Internet/Wi-Fi)	appwrapandroid.awmdm.com	HTTPS	443	Workspace ONE UEM Cloud Android App Wrapping Service
Devices (Internet/Wi-Fi)	appwrapandroid.awmdm.com	TCP	443	Android only
Devices (Internet/Wi-Fi)	gcm-http.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
Devices (Internet/Wi-Fi)	gcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.

Source Component	Destination Component	Protocol	Port	Notes
Devices (Internet/Wi-Fi)	fcm.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; Firebase Cloud Messaging. Proxy Connections not supported.
Devices (Internet/Wi-Fi)	fcm-xmpp.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only; DPC Communication
Devices (Internet/Wi-Fi)	android.googleapis.com	TCP	443, 5228-5230, 5235, 5236	Android only
Devices (Internet/Wi-Fi)	pki.google.com	TCP	443	Android only. Certificate revocation.
Devices (Internet/Wi-Fi)	clients1.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	clients2.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	clients3.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	clients4.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	clients5.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	clients6.google.com	TCP	443	Android only. Google backend services.
Devices (Internet/Wi-Fi)	android.com	TCP TCP, UDP	443 5228-5230	Android only
Devices (Internet/Wi-Fi)	www.google.com	TCP	443	
Devices (Internet/Wi-Fi)	*.googleapis.com	TCP	443	Android only. Google APIs, Play Store APIs.
Devices (Internet/Wi-Fi)	accounts.google.com	TCP	443	Android only. Authentication.
Devices (Internet/Wi-Fi)	play.google.com	TCP TCP, UDP	443 5228-5230	Android only
Devices (Internet/Wi-Fi)	android.clients.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Devices (Internet/Wi-Fi)	fonts.googleapis.com	HTTP/ HTTPS	80 or 443	For fonts used in the UEM console
Devices (Internet/Wi-Fi)	google-analytics.com	TCP TCP, UDP	443 5228-5230	
Devices (Internet/Wi-Fi)	googleusercontent.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).

Source Component	Destination Component	Protocol	Port	Notes
Devices (Internet/Wi-Fi)	gstatic.com	TCP TCP, UDP	443 5228-5230	Android only. User Generated Content (e.g. app icons in the store).
Devices (Internet/Wi-Fi)	*.gvt1.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Devices (Internet/Wi-Fi)	*gvt2.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
Devices (Internet/Wi-Fi)	*gvt3.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
Devices (Internet/Wi-Fi)	dl-ssl.google.com	TCP,UDP	443, 5228-5230	Download apps and updates, Play Store APIs
Devices (Internet/Wi-Fi)	*.ggpht.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
Devices (Internet/Wi-Fi)	dl.google.com	TCP TCP, UDP	443 5228-5230	Android only. Download apps and updates, Play Store APIs.
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
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

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

On-Premises Advanced Configurations

6

Some large deployments of Workspace ONE UEM require additional configuration. This section lists various advanced Workspace ONE UEM configurations, and the additional considerations that must be made for a successful implementation.

High Frequency Certificate Generation with CICO

In a CICO environment, certificates last hours instead of weeks or months, leading to a significant number of certificates being generated and revoked. Not only does this increase the load on the Workspace ONE UEM platform but also on the back-end Certificate Authority infrastructure.

Configure your Workspace ONE UEM deployment to control CA proliferation in three ways:

1 Use the built-in CA (SCEP). If you select a different CA, vetting the back-end CA infrastructure becomes key to the success of this configuration.

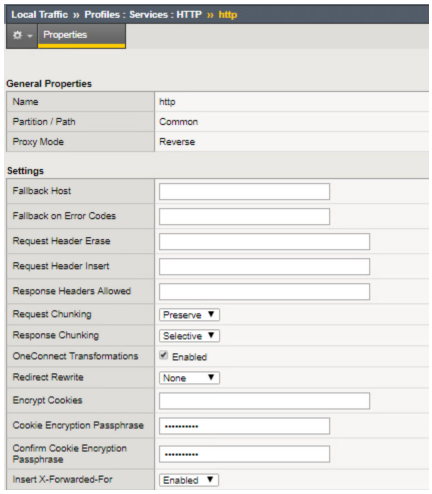
2 Increase the feature flag value for stored private key generation. The impact of this configuration is an increase of memory use equivalent to 100MB per 100,000 certificates. VMware recommends setting this value to the number of certificates you might expect to generate in one day. To update this value, contact VMware Support.

3 Lower the validity period and the renewal period of the certificates. VMware recommends that validity and renewal values consider business-specific requirements such as maximum shift length. Recommended values are somewhere between 12 and 24 hours. This prevents the CRL from expanding indefinitely.

Public IP Address Forwarding

On-premises customers using Load Balancers for Devices Services must also configure the load balancers to set the XFF header with Client's Source IP. In the Load Balancer Configuration for your Directory Services Server, set Insert-X-Forwarded-For to Enable.

Figure 6-1. Public IP Address Forwarding



Unsupported CIS Benchmarks

Industry standards and best practices include the incorporation of CIS Benchmarks into your network infrastructure. However, some platforms and applications might not fully integrate with select controls. The Workspace ONE UEM Architecture as describe in this guide, has been validated for all CIS Benchmarks, except the ones listed in the Unsupported CIS Benchmarks table. These CIS Benchmarks cannot be enabled on any device with VMware software installed.

Note Deploying against one of the listed benchmarks could result in loss of data or functionality.

Table 6-1. Unsupported CIS Benchmarks

	Section	Recommendation	Title	Description
Level 1 - IIS 10				
	1	1.1	Basic Configurations	Basic web server-level recommendations
	1	2.3	Ensure that web content is on non-system partition	Web resources published through IIS are mapped, via Virtual Directories, to physical locations on disk. It is recommended to map all Virtual Directories to a non-system disk volume.
	2	3.10	Ensure 'forms authentication' require SSL	Forms-basedauthentication can pass credentials across the network in clear text. It is therefore imperative that the traffic between client and server be encrypted using SSL, especially in cases where the site is publicly accessible. It is recommended that communications with any portion of a site using Form Authentication is encrypted using SSL. **Note** Due to identified security vulnerabilities, SSL is no longer considered to provide adequate protection for sensitive information.

Table 6-1. Unsupported CIS Benchmarks (continued)

	Section	Recommendation	Title	Description
	4	4.7	Ensure Unlisted File Extensions are not allowed	The 'FileExtensions' Request Filter allows administrators to define specific extensions their web server(s) allow and disallow. The property 'allowUnlisted' covers all other file extensions not explicitly allowed or denied. Often times, extensions such as '.config', '.bat', '.exe', to name a few, should never be served. The 'AllowExtensions' and 'DenyExtensions' options are the UrlScan equivalents. It is recommended that all extensions be unallowed at the most global level possible, with only those necessary being allowed.
Level 2 - IIS 10				
	4	4.4	Ensure non-ASCII characters in URLs are not allowed.	This feature is used to allow or reject all requests to IIS that contain non-ASCII characters. When using this feature, Request Filtering denies the request if high-bit characters are present in the URL. the UrlScan equivalent is 'AllowHighBitCharacters'. It is recommended that requests containing non-ASCII characters are rejected, where possible.

For more information on CIS Benchmarks, see http://www.cisecurity.org.

on-premesis Architecture Monitoring

7

Monitoring your Workspace ONE UEM solution is an important part of ensuring it operates effectively. Many tools and software packages exist to help you. 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 following section 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,contact VMware 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)

This chapter includes the following topics:

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.workspaceone.com.

Perform a Health Check for Load Balancers

Performing regular health checks for your load balancers helps verify connectivity. If there is no connectivity, then the server is listed as down and any subsequent requests are sent 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
- **MDM API** – GET to https://<host>/api/mdm/hc
- **System API** – GET to https://<host>/api/system/hc
- **MEM API** – GET to https://<host>/api/mem/hc
- **MAM API** – GET to https://<host>/api/mam/hc

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.

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

Table 7-1. 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/Statistics	HTTP 200
Device Services WinMo Tracker	/DeviceServices/tracker.aspx?id=0	HTTP 302

Table 7-2. Console

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

Table 7-3. API

Description	URL Endpoint	Status code
API Help Page	/api/help/#!/apis	HTTP 200

Table 7-4. Secure Email Gateway v2

Description	URL Endpoint	Status code
Service Availability	/	HTTP 200
ActiveSync Connectivity	/Microsoft-Server-ActiveSync /health	HTTP 401 HTTP 200

Table 7-5. VMware Tunnel (Unified Access Gateway) – Proxy Component (Basic and TLS Port Sharing)

Description	URL Endpoint	Status code	Default Port
HTTPS	https://<TUNNEL_PROXY_SERVER>:<PORT>	HTTP 407	2020
HTTPS	https://<TUNNEL_PROXY_RELAY_SERVER>:<RELAY_PORT>	HTTP 407	2020
HTTPS	https://<TUNNEL_PROXY_ENDPOINT_SERVER>:<ENDPOINT_PORT>	HTTP 407	2010

Table 7-6. VMware Tunnel (Unified Access Gateway) – Per-App VPN Component (Basic and TLS Port Sharing)

Description	URL Endpoint	Status code	Default Port
TCP	TUNNEL_SERVER:PORT	Successful Connection	8443

Table 7-7. Content Gateway (Unified Access Gateway) - Basic

Description	URL Endpoint	Status code	Port
HTTPS	https://<Content_SERVER>:<PORT>/Content/awhealth	HTTP 403	443
HTTPS	https://<Content_RELAY_SERVER>:<PORT>/Content/awhealth	HTTP 403	443
HTTPS	https://<Content_ENDPOINT_SERVER>:<PORT>/Content/awhealth	HTTP 403	443

Table 7-8. Content Gateway (Unified Access Gateway) - TLS Port Sharing

Description	URL Endpoint	Status code	
HTTPS	https://<Content_SERVER>:<PORT>/Content/awhealth	HTTP 403	10443
HTTPS	https://<Content_RELAY_SERVER>:<PORT>/Content/awhealth	HTTP 403	10443
HTTPS	https://<Content_ENDPOINT_SERVER>:<PORT>/Content/awhealth	HTTP 403	10443

Change the scheme from https to http when SSL offloading is used for Content Gateway.

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" />.

Table 7-9. 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.

Table 7-10. Remote Management

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

Table 7-11. Workspace ONE Access

Component	URL Endpoint	Status code
Workspace ONE Access Service (PC)	/SAAS/API/1.0/REST/system/health/heartbeat	HTTP 200
Workspace ONE Access Service (Android)	Certproxy - :5262/system/health	HTTP 401
Workspace ONE Access Service (iOS)	kdc - Telnet 88	Connection
Workspace ONE Access Connector	/hc/API/1.0/REST/system/health/allOK	HTTP 200
Integration Broker	IB/API/RestServiceImpl.svc/ibhealthcheck	HTTP 200
Integration Broker (XenApp 7.X)	/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenapversion=Version7x	HTTP 200
Integration Broker (XenApp 6.X)	/IB/API/RestServiceImpl.svc/hznxenapp/admin/xenfarminfo?computerName=&xenapversion=Version75orLater	HTTP 200

Table 7-12. Dell Factory Provisioning

Description	URL Endpoint	Status code
Dell FPS	/hc	HTTP 200

Monitor the Workspace ONE UEM Database

Monitor the Workspace ONE UEM database to ensure a fully-functioning, healthy, on-premesis 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 Maintenance	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.

on-premesis Architecture Maintenance Guidelines

Workspace ONE UEM powered by AirWatch describes some of the maintenance tasks to perform for your on-premesis deployment to keep it healthy and functioning properly.

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	Hourly (frequency should be adjusted based on server workload)	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 Maintenance	Nightly	Reorganize or rebuild based on fragmentation percentage, 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

Task	Frequency	Description	Responsible Party
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

Archive Workspace ONE UEM Logs

Over time, it might 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 websites, 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.

on-premesis Architecture High Availability

8

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.

This chapter includes the following topics:

High Availability Support for Workspace ONE UEM Components

You can setup your Workspace ONE UEM compenents for high-availability support through load balancing and session persistence. Laarn more about the individual recommended component settings through Workspace ONE UEM powered by AirWatch.

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 Chapter 7 on-premesis Architecture Monitoring for information on health checks on the servers. The following table outlines both for each Workspace ONE UEM component.

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

Application Modules	Load Balancing Supported?	Recommended Session Persistence	Recommended Timeout Value
Console	Yes*	Source IP-based persistence or cookie-based persistence	60 minutes
Device Services	Yes	Source IP-based persistence	20 minutes

Application Modules	Load Balancing Supported?	Recommended Session Persistence	Recommended Timeout Value
VMware AirWatch Cloud Messaging (Implicit)	Yes	Persistence based on parameter **awcmsessionid** in either the URI or HTTP Header.	N/A
VMware AirWatch Cloud Messaging (Explicit)	Yes	N/A	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 (V2)	Yes	None**	Variable**
Content Gateway	Yes	None	N/A
Unified Access Gateway	Yes	Source IP-based persistence	30 minutes
Remote File Storage	Yes	None	N/A
Workspace ONE Access	Yes	Source IP / SSL session / cookie-based persistence	60 minutes
AirWatch Cloud Connector	N/A (see **Note**)	N/A	N/A
Workspace ONE Access Connector	N/A	N/A	N/A
Workspace ONE Access 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	Yes	N/A	N/A
Memcached	N/A	N/A	N/A
Adaptiva	N/A	N/A	N/A
ENS V1	N/A	N/A	N/A
ENS V2	Yes	N/A	N/A
Airlift	N/A	N/A	N/A
Dell Factory Provisioning	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 for SEG Classic or V2, but without persistence there might be delays in email flow for newly enrolled devices. To speed up email flow, consider using SEG V2 and clustering the SEG V2 servers.

Device Services requires persistence as noted unless your deployment of Workspace ONE UEM 9.4 and above includes Memcached. In this configuration persistence is not required on the /deviceservices endpoint, which can be achieved with Layer 7 routing. Other Device Services endpoints such as /devicemanagement or /mydevice still require Source-based IP persistence.

Note To accommodate extra users as part of your sizing requirements you can deploy multiple VMware AirWatch Cloud Connectors, which are all served 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 Robin 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 **Workspace ONE UEMConsole 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 **UEMConsole 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.
  - Dell Factory Provisioning: No persistence is required. The Factory Provisioning service is stateless and can be loadbalanced.
- 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.

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 the Workspace ONE UEM Installation Guide.

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, however, 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 from Workspace ONE UEM with disaster recovery, contact Workspace ONE Support.

List of Workspace ONE UEM Services

9

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

Service	Description
AirWatch API Workflow	This service processes device commands from REST API.
AirWatch Background Processor Service	This service is used for asynchronous execution of long running jobs.
AirWatch Batch Processing Service	This service processes batch requests from the AirWatch system.
AirWatch Cloud Messaging Service	This service runs a message queueing server which transfers messages to and from devices and AirWatch servers.
AirWatch Compliance Service	This service handles compliance rule level evaluations and take actions on the scheduler level.
AirWatch Content Delivery Service	This service is responsible for pushing staging and provisioning content to relay servers.
AirWatch DataPlatform Service	This service is responsible for pushing data to the Intelligence platform.
AirWatch Device Scheduler	This service is responsible for orchestrating scheduled jobs across the console and devices.
AirWath Directory Sync Service	This service synchronizes uses and user groups from external user stores.
AirWatch Entity Change Queue Monitor	This service monitors the event log queue and send outbound event logs.
AirWatch Entity Reconcile Service	This service handles reconcile and sync for entities linked to smart groups.
AirWatch Eventlog Processor Service	This service monitors the event log queue, enriches them, and posts to the Intelligence platform.
AirWatch GEM Inventory Service	This service communicates instance specific information to the GEM.
AirWatch Integration Service	This service is used to integrate AirWatch with third party applications.
AirWatch Interrogator Service	This service reads device sample information from the queues and writes the information to the database.
AirWatch MEG Queue Service	This service reads and processes mobile email gateway requests from the message queues.
AirWatch Messaging Service	This service sends messages to the respective device cloud services (ex. APNS, GCM, FCM, etc).
AirWatch Outbound Queue Monitor Service	This service subscribes for outbound event notifications.

Service	Description
AirWatch Policy Engine	This service is used to determine product and product set applicability and compliance for devices, and if needed, project jobs are sent to the device to install/uninstall profiles, files, actions, and applications.
AirWatch Provisioning Package Service	This service is responsible for generating PPKG packages for the factory provisioning flow.
AirWatch Smart Group Service	This service is responsible for smart group device map updates.
AirWatch SMS Service	This service is used by AirWatch to send SMS messages to devices.
AirWatch Tunnel Service	This service manages tunnel configuration for devices and servers such as traffic rules and outbound configurations.

This chapter includes the following topics:

List of Message Queues

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

Queue Name	Description
APNSOutbound	iOS Outbound APNS Messages
AWAdminBatchQueue	Administration Group Batch Processing
AwAdminPasswordNotificationQueue	Password Expiration Management for Local Basic Admins
AWAppleCareGsxIntegration	AppleCare Model Information Request
AWApplicationEventSample	Application Analytics for iOS Content Locker
AWApplicationFeedback	Used for Managed Application feedback samples
AWApplicationListSample	iOS Application List Samples (From Device)
AWApplicationReport	Handles report messages sent by the device SDK
AWAppScanTpiQueue	App Scan requests to Third Party Apps
AWAppWithUpdatesQueue	VPP Applications Auto Update
AWAsyncExportQueue	Async exports of Telecom data from console
AWAutoDiscovery	Used for auto discovery messages
AWAvailableOsUpdatesListSample	Process the available OS Updates Samples for Devices
AWBaselineSample	Baseline sample information from devices (in 1909, but not used)
AwBackgroundJobsReports	Batch processing for legacy SSRS reports.
AWBiosSample	Dell BIOS Samples
AWBluetoothInformationSample	Android/WinMo Bluetooth Samples (From Device)

Queue Name	Description
AWCallLogSample	Android/WinMo Call Log Samples (From Device)
AWCellInformationSample	Android/WinMo Cellular Information Samples (From Device)
AWCellSignalQualitySample	Android/WinMo Cell Signal Quality Samples (From Device)
AWCellTowerInformationSample	Android/WinMo Cell Tower Information Samples (From Device)
AWCertificateListSample	iOS Certificate List Samples (From Device)
AWCMOutbound	AWCM Outbound Messages [For Rugged]
AWComplianceDeviceQueue	Real Time Device Compliance for enrollment and reenrollment flows
AWComplianceServiceQueue	Queue for standalone Compliance service
AWContentBatchQueue	Multi-file delete support for content
AWDepBatchQueue	Process DEP sync and assign profile requests
AWDeviceCapabilitySample	Android Device Capability Samples (From Device)
AWDeviceComplianceAttributeQueue	TrustPoint Integration
AWDeviceCustomAttributeListSample	List of device custom attributes, used primarily by rugged devices (Android, QNX, WinMo, Mac, PCs)
AWDevicePolicyRuleComplianceEvaluationQueue	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
AwDeviceSensorQueue	Stores Windows 10 Custom Samples before sending to AWS
AWDeviceSyncQueue	Generic MDM Queue
AWDiskEncryptionSample	Disk Encryption Samples (From Device)
AWEasSample	Generic MDM Queue
AWEfotaSample	Samsung Efota Samples
AWEventActionSample	Event Actions Samples (From Device)
AWEventLog	Keeps various events related to device/system activities
AwEventLogProcessor	Stores event logs messages before being sent to Elastic Search (Inactive)
AWExternalDirectoryBatchQueue	Queue for User Authentication and Directory Sync for vIDM
AWFetchAppUpdatesQueue	VPP Applications Auto Update
AWGPSCoordinateSample	Android/WinMo GPS Coordiante Samples (From Device)
AWGPSExtendedCoordinateSample	Android/WinMo Extended GPS Coordinate Samples (From Device)
AWHealthAttestationSample	Queue Health Attestation Sample
AWInstalledApplicationListSample	Installed Application List Sample (Inactive)
AWIntegrationService	This queue is for handling Web Sense certificate requests asynchronously.
AWIntegrationServiceGenericQueue	Queue Compliance State for Windows 10 Devices
AWInventoryCheckinCommandQueue	GEM Inventory Service
AWLocalBasicUserSyncQueue	Used for triggering a local basic user sync at regular intervals (inactive)

Queue Name	Description
AWLogManagerXml	WinMo LogManager XML Samples (From Device)
AWManagedLicenseListSample	Windows [Phone] 10 Application and License Status
AWManagedMediaListSample	Managed Media List Sample (Managed Books)
AWMegPayloads	MEG Payload Samples (from API)
AWMemorySample	Android/WinMo Memory Samples (From Device)
AWMetricsSample	New Product Provisioning
AWMobileDataUsageSample	Android/iOS [Non-]Mobile Data Usage Samples
AWNetworkAdapterSample	Android/WinMo Network Adapter Samples (From Device)
AWNetworkWLANSample	Android/WinMo Network WLAN Samples (From Device)
AWOemUpdateSample	Process the status of the OemUpdate(s) for Devices
AwOEMProvisioningQueue	Device information for Windows OEM reprovisioning (in 1909, but not used)
AwOemUpdateSampleSummaryQueue	DELL OemUpdate Samples Summary
AWOsUpdateStatustListSample	Process the status of the OS Updates for Devices
AWOutboundEventLog	Outbound queues for the "Outbound Event Notification" feature
AWPatchApplicationListSample	Application List for Unmanaged Devices
AWPolicyListSample	New Product Provisioning
AWPolicyProductListSample	New Product provisioning
AWPowerSample	Android/WinMo Power Samples (From Device)
AWPrinterNotification	Common MSMQ to send notifications to Zebra and Toshiba Print Servers
AWProfileListSample	iOS Configuration Profile List Samples (From Device)
AwProvisioningPackageServiceQueue	Cleans up the PPKG from the storage location (CDN)
AWProvisioningProfileSample	iOS Provisioning Profile Samples (From Device)
AWPublishQueue	iOS Bulk Profile Publish (From Console)
AWRestrictionsListSample	iOS Restrictions List Samples (From Device)
AWRosterSyncQueue	Queues an event for making a roster sync call to Apple API when an admin requests this on-demand from the console.
AWScheduleOsUpdateResultListSample	Process the results of the ‘Install OS Updates’ Command
AWSecurityInformationSample	iOS Security Information Samples (From Device)
AWSEGCompliance	Compliance Information for SEG
AWSegFastCompliance	MEM High Priority Compliance Commands
AWSelectiveApplicationListSample	Application Sample Query for iOS 7+ Devices
AWSmartGroupEvent	Data for Monitoring User Group Change Events
AWSmartGroupPublish	Smart Group Publish Events
AWSMSLogSample	Android/WinMo SMS Log Samples (From Device)
AWSWindowsInformationSample	Windows Information Sample (Windows 8 Devices only)

Queue Name	Description
AWSystemSample	Android/iOS/WinMo Device/System Information Samples (From Device)
AWToMagOutboundQueue	Queues message to be sent to MAG via AWCM
AWUpdateListSample	Microsoft EMM: Handles messages related to Windows Updates Revisions
AWUserBatchQueue	User Batch Processing Information
AWUserDataSample	OneDrive Integration for User Data Recovery and Migration (Inactive)
AWUserGroupsBatchQueue	Process User Group actions (sync user attributes, add missing users)
AWUserListSample	Used for saving user list sample changes.
AWVMInstanceSample	OS X VMware Flex Integration – Flex VM Status Reported from OS
AWVppBulkDeployment	Process Users for VPP bulk registration of users and licenses
AWVppLicensePreAssignmentQueue	Queues an event for making a license preassignment call to Apple API when an admin requests this on-demand from the console.
AWVppLicenseSyncQueue	Queue to process the VPP apps for license sync
AwWindows10KioskQueue	Kiosk profile publishing
AwWindowsPpkgPackagingQueue	Export applications from WS1 into the PPKG format
AwWindowsSecurityInformationSample	Windows 10 DeviceGuard / Security Information Sample (Inactive)
awwindowsupdatequeue	Windows 10 (Microsoft EMM)
AWWindowsWmiSample	Windows device queue for WMI samples
AWWnsNotification	Windows Notification Service (WNS) Notifications
AWWorkflowEvent	Process all workflow events
C2DMOutbound	Android Outbound C2DM Messages
FastLaneAPNSOutbound	iOS Outbound APNS Messages
FastLaneWnsOutbound	Critical WNS Outbound Messages
GCMOutbound	Android Google Cloud Messaging Outbound
SyncDirectoryAdminAttributesQueue	Queues for the Directory Sync Service
SyncDirectoryGroupsQueue	Queues for the Directory Sync Service
SyncDirectoryUserAttributesQueue	Queues for the Directory Sync Service
WorkFlow-DeviceCommands	API Workflow

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 and in the log file, but it does 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
6008	Startup	Error while starting listener tasks	Yes
6020	Shutdown	All listener threads 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 that 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; 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! 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 might be out-of-date; THIS CONFIGURATION IS UNSUPPORTED! 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. 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	

Error Codes	Error Type	Error Message	Followed by Exception?
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} 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	
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

Error Codes	Error Type	Error Message	Followed by Exception?
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

Proxy Component Error Codes

The following sections list out the error codes or messages for the 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

Code	Name	Meaning
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.
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.

Code	Name	Meaning
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.
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