

Workspace ONE Assist

VMware Workspace ONE UEM

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

<https://docs.vmware.com/>

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

Copyright © 2021 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** Workspace ONE Assist 4
- 2** General and Hardware Requirements for Workspace ONE Assist 10
- 3** Network and Security Requirements 16
- 4** Supported Platforms 25
- 5** Install Workspace ONE Assist to an On-Premises Environment 34
- 6** Configure Assist Admin User Access 57
- 7** Configure End-User Devices 62
- 8** Start an Assist Session 75
- 9** Troubleshooting Workspace ONE Assist 97

Workspace ONE Assist

1

VMware Workspace ONE Assist, together with Workspace ONE UEM powered by AirWatch, enables you to remotely access and troubleshoot devices in real time. Workspace ONE Assist is privacy-friendly. End users can accept, pause, and end a remote session at any time for privacy reasons.

The Workspace ONE Assist client also has additional support tools and device information available. The combination of remote control and information allows you to troubleshoot any issues on devices quickly and accurately.

Workspace ONE Assist is already configured for Workspace ONE UEM SaaS customers who have purchased the upgrade. For the most up-to-date information about the licenses and purchases of Workspace ONE products, see the knowledge base article, [Locating Workspace ONE license information in Customer Connect](#).

Workspace ONE Assist requires devices to have the Workspace ONE Intelligent Hub and the Remote Management client installed.

Workspace ONE Assist Components

Workspace ONE Assist uses multiple components to facilitate the communication between admins and end-user devices. The core components are as follows.

Database

The database handles system and tenant configuration, operations, and logging such as the accrual of historical device enrollment data. The Workspace ONE Assist system is composed of eight databases.

- **ApAdmin** – Maintains all the system configurations, tenant (customer) configuration, management information, system administration data, and server instrumentation data. There is only one ApAdmin database for all tenants.
- **APOps (2)** – Maintains data required for the operations of the system such as device enrollment, Access Control List's (ACL), groups, users, zones, and so on. You have one template APOps database and one for the tenant with the GUID.
- **APReports (2)** – Contains historical data of device enrollment, session, audit, report views, and so on. You have one template APReports database and one for the tenant with a GUID.

- **APJournal (2)** – Contains aggregated information on the tenant necessary to construct various reports. You have one template APJournal database and one for the tenant with a GUID.
- **APPublic** – Contains pre-enrollment information on devices and multiple database jobs. There is only one APPublic database for all tenants.

Core Services

The Core Services component provides service discovery and auxiliary services for the Workspace ONE Assist solution through Web services and Windows services. These services include the following.

- **Management Entity (ME)** – Windows service that provides an in-memory datastore for admin and management Web service, which provides the operational end point to the system.
- **Service Coordinator (SVC)** – This Windows service is responsible for coordinating communication between various elements within the system. It provides the communication to the database and is responsible for the discovery of all other Remote Management Tool services. All Workspace ONE Assist Tool services register with this service. Service coordinator service is installed on an Application (App) Server.
- **Data Tier Proxy (DTP)** – This Windows service works with the Service Coordinator. It serves as the gateway for all services to reach the Service Coordinator service to communicate with Remote Management Tool databases. Data Tier Proxy service is installed on the App Server.
- **Data Access Proxy (DAP)** – This Web service is responsible for a proper communication of all Web services. It serves a similar purpose as the Data Tier Proxy service and is installed on the App server.

Portal Services

The Portal Services component handles the administrative and management services for Workspace ONE Assist. The Management Website is installed as part of the portal services component and consists of the following.

- **AetherPal Tool Controller Service (ACS)** – Acts as a gateway service that maintains a consistent socket connection between the RS web console and the Connection Proctor.
- **Management Web Site (ADM/ANC)** – IIS Service that hosts the RS web console for managing and remoting into devices. Anchor service responsible for mobile device registration. Also, it contains the System Admin Service (SAS) admin web portal for accessing and administering the tool and defining tenant and service configuration.
 - **T10 Interface** – The T10 Interface is part of the Management website and it defines an integration portal between Workspace ONE UEM and the Workspace ONE Assist server.
 - The T10 interface uses Representational State Transfer (REST) communication with a JavaScript Object Notation (JSON) payload. The T10 interface provides Workspace ONE UEM with the ability to make a mobile device eligibility call.
 - The T10 interface can also start a remote support session using the Workspace ONE Assist tool and delete the device from the Workspace ONE Assist system.

Application Services

Messaging Entity (MSG) – a core Windows service that provides the means for the Workspace ONE Assist tool to send out SMS messages to the device by way of API or direct communication. This communication is accomplished with a messaging gateway, such as Google Cloud Messaging (GCM), or any proprietary SMSC aggregator.

The remaining application services are installed by default but are not used by Workspace ONE Assist directly. As such, these services can be disabled if you prefer.

- **ZVC Services (ZVC)** – Windows service used for GuideMe feature. ZVC Service helps with versioning and authoring management. Workspace ONE Assist does not require this auxiliary service. After installation, these services can be disabled in Windows services.
- **KB Service (KB)** – Windows service used for GuideMe feature. This service help process content for delivery and publishing. This is an auxiliary service that is not required by the Workspace ONE Assist application for most use cases. Once installed, these services can be disabled in Windows services.

Connection Proctor

The Connection Proctor component uses the Windows Connection Proctor service to manage device connections to the Workspace ONE Assist server. The component also simultaneously handles multiple requests for sessions.

Supported Deployment Models

Workspace ONE Intelligent Hub and the platform-specific Workspace ONE Assist app must be installed on all devices. These two installs work together with Workspace ONE UEM to make it easy to use the console as the starting point for each support session.

Whether your Workspace ONE UEM deployment is part of an on-premises, dedicated SaaS, or shared SaaS environment, several Workspace ONE Assist deployment models are supported.

Note Prior to UEM console version 2101, if assist were enabled for a customer, all the iOS devices would enroll automatically for the entire customer. Therefore, enabling assist for specific organization groups (OG) was not possible. With console versions 2101 and later, the remote view can be enabled or disabled for iOS devices belonging to specific OGs.

Table 1-1. Single Customer

Workspace ONE UEM	Workspace ONE Assist
On-Premises	On-Premises
On-Premises (Multi-Environment)	Shared SaaS*
Shared SaaS	Shared SaaS
Dedicated SaaS	Shared SaaS

* In this scenario, multiple instances of Workspace ONE UEM (each for a single customer) communicate to a single Shared SaaS build of Workspace ONE Assist. See [Integrate Deployment Model, On-Prem UEM With SaaS Assist](#).

Table 1-2. Multi-Tenant Partner**

Workspace ONE UEM	Workspace ONE Assist
On-Premises	Shared SaaS
Shared SaaS	Shared SaaS
Dedicated SaaS	Shared SaaS

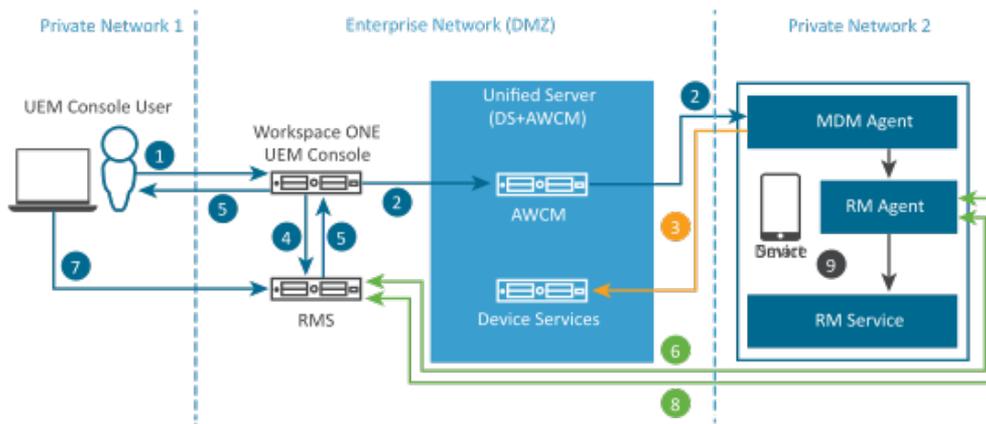
** In this scenario, multiple organization groups within Workspace ONE UEM (on-premises or SaaS) communicate to a single Shared SaaS build of Workspace ONE Assist.

Typical On-premises Deployment

Most administrators deploy the Workspace ONE Assist server in an enterprise network to facilitate the communication between the various components. The typical deployment scenarios are summarized in this section. For simplicity, deployment with High Availability or multiple nodes with Active or Passive configuration details is not provided here.

Standard (Single Server) Deployment

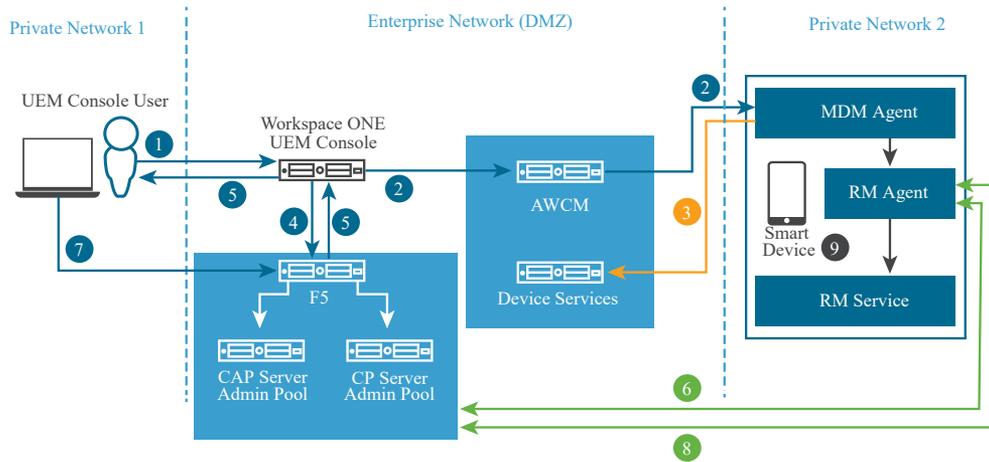
This sample diagram is a typical deployment without the use of a load balancer.



- | | |
|--|------------------------------|
| 1. Queue Remote Control Command. | 6. Request Session URL. |
| 2. Queuing Command to Connect to Server. | 7. Admin Joins Session. |
| 3. Confirm Command. | 8. Device Joins Session. |
| 4. Create Session. | 9. Send Commands/Get Frames. |
| 5. Send Session URL. | |

Medium-sized Deployment

This diagram represents typical medium sized deployment where two servers are utilized. One server has Core, Application, and Portal services (CAP). Second server is the CP server. You can have more than one CP server. For more information, see [Load Balancer](#).



Workspace ONE Assist **CAP Servers** contain Core Services, Application Services, and Portal Services.

- | | |
|--|------------------------------|
| 1. Queue Remote Control Command. | 6. Request Session URL. |
| 2. Queuing Command to Connect to Server. | 7. Admin Joins Session. |
| 3. Confirm Command. | 8. Device Joins Session. |
| 4. Create Session. | 9. Send Commands/Get Frames. |
| 5. Send Session URL. | |

Load Balancer

A load balancer improves the workload distribution across multiple server resources and is valuable in high capacity, high availability environments. Consider a load balancer in your Workspace ONE Assist environment if your configuration features a separate CAP server and connection proctor server.

Integrate a Load Balanced to Your Deployment

SSL passthrough is required for all server configurations on the load balancer. To address persistence, you must configure the load balancer to use IP or SSL session persistence.

When you initially run the installer which creates the config.installer file, you are presented with the **Database Credentials** screen.

- 1 For multi-node solutions, you must enter the database server instance name or the database server instance IP address.

- 2 Run the database installation by itself even if you are installing other services on the same server.
- 3 The Workspace ONE Assist server requires a host record that points to the internal IP address of the VIP (also known as Virtual IP) for the load balanced pool.
- 4 Ensure that each [FQDN] record in the [ApAdmin].[dbo].[Server] table in the database points to the internal IP address of the VIP (also known as Virtual IP) for the load balanced pool.

Ensure that you delete the Default Website from IIS once the server is running. See [Domain Name Service](#) and also [Modify Database Record for Multi-Node Configuration](#).

General and Hardware Requirements for Workspace ONE Assist

2

Both SaaS and On-Premises customers must meet minimum requirements before using Workspace ONE Assist.

General Requirements

SaaS customers must meet only the general requirements listed here.

Requirements	Minimum
Supported Browsers for Admins	Latest version of Google Chrome, Firefox, Safari, or Edge. Only Chrome supports the File Manager feature.
Workspace ONE™ UEM version	Workspace ONE UEM 9.2 or later with the ARM add-on.

Hardware Requirements (for On-Premises Servers)

In addition to the general requirements, on-premises customers must also meet the hardware requirements.

Table 2-1. Workspace ONE Assist Server (On-Premises Server)

Hardware	Minimum
CPUs	2.4 GHz Processors, 4 Logical Processors, 2 CPUs, 2 Core 2x2 or 4 physical depending on machine type, virtual machine, or physical.
Memory	16 GB
Hard Drive IOPS	200
Hard Drive Space	100 GB for OS drive

Table 2-2. Workspace ONE Assist Database Server (for On-Premises Server)

Hardware	Minimum
CPUs	2.4 GHz Processors, 4 Logical Processors, 2 CPUs, 2 Core 2x2 or 4 physical depending on the machine type, virtual machine, or physical.
Memory	16 GB

Table 2-2. Workspace ONE Assist Database Server (for On-Premises Server) (continued)

Hardware	Minimum
Hard Drive IOPS	200
Hard Drive Space	200 GB for databases

Table 2-3. Bandwidth

Hardware	Minimum
Average Remote Session Requirement	1 MB/per minute (17 kbps)

On-Premises Hardware Scaling Requirements

Use the following requirements as a basis for creating an effective Workspace ONE Assist system that scales to your on-premises environment.

These requirements do not include network equipment such as load balancers or monitoring servers. All the arrangements presented here offer a high system availability in active and passive modes.

# Devices / # of Concurrent Remote Sessions / # of Concurrent Enrollments	Core Server (all in one)	DB Server	CP Server	CAP Server
Less than 1000 / Up to 50 sessions / 5 enrollments per sec	1 server (2 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012–2016 Express (if DB is on the same server).	1 server, optional (2 CPUs, 8 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012–2016 Express.	n/a	n/a
1000–10,000 / Up to 50 sessions / 5 enrollments per sec	1 server (2 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012–2016 Standard (if DB is on same server).	1 server, optional (2 CPUs, 8 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012–2016 Standard.	n/a	n/a
10,000–100,000 / Up to 50 sessions / 5 enrollments per sec	1 server (2 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI.	1 server, optional (2 CPUs, 16 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012–2016 Standard.	n/a	n/a

# Devices / # of Concurrent Remote Sessions / # of Concurrent Enrollments	Core Server (all in one)	DB Server	CP Server	CAP Server
100,000–500,000 / Up to 100 sessions / 20 enrollments per sec	n/a	SQL cluster (2 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/ GUI. * MS SQL 2012–2016 Standard.	2 servers (4 CPUs, 16 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI.	2 servers (4 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI.
500,000–1 million / Up to 200 sessions / 40 enrollments per sec	n/a	SQL cluster (4 CPUs, 32–64 GB RAM, 1 TB HDD): * Windows 2012 or 2016 w/ GUI. * MS SQL 2012–2016 Standard.	4 servers (8 CPUs, 16 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI.	4 servers (8 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI.

On-Premises Software Requirements

Ensure that you meet the following software requirements to run Workspace ONE Assist.

SaaS and On-Premises Device Software Requirements

For a full listing of platform-specific software requirements for devices, see [Chapter 4 Supported Platforms](#) and [Chapter 7 Configure End-User Devices](#).

On-Premises Installation Software Requirements

Table 2-4. Workspace ONE Assist Server

Requirement	Description
Operating System	Microsoft Windows Server 2019 (w/GUI), 2016 (w/GUI), or 2012 R2.
Software	Microsoft .NET Framework 4.7.2

Table 2-4. Workspace ONE Assist Server (continued)

Requirement	Description
Server Roles *	<ul style="list-style-type: none"> ■ Application Server. ■ Web Server IIS.
Features **	<ul style="list-style-type: none"> ■ .NET Framework 4.7 Features. <ul style="list-style-type: none"> ■ .NET Framework 4.7.2 ■ ASP .NET 4.7. ■ WCF Services. <ul style="list-style-type: none"> ■ HTTP Activation. ■ Message Queuing (MSMQ) Activation. ■ Named Pipe Activation. ■ TCP Activation and TCP Port Sharing. ■ Message Queuing Services. ■ Windows Process Activation Service. <ul style="list-style-type: none"> ■ Process Model. ■ .NET Environment 3.5. ■ Configuration APIs.

* For medium and multiple server deployments, these roles are not required on the Connection Proctor (CP) Servers. The ONLY software requirement on Connection Proctor (CP) servers is .NET Framework 4.7.2 or newer.

Table 2-5. Workspace ONE Assist Database

Requirement	Description
Operating System	<ul style="list-style-type: none"> ■ Microsoft Windows Server 2019, 2016, or 2012 R2.
Software	<ul style="list-style-type: none"> ■ MS SQL Server of any of the following versions. <ul style="list-style-type: none"> ■ 2012 Standard ■ 2014 Standard or Enterprise ■ 2016 Standard or Enterprise ■ 2017 Standard or Enterprise ■ Express 2012 or later (only for deployments with less than 2000 devices) ■ MS SQL Management Studio 17 (only when SQL Server Express 2012 or later is used). ■ Microsoft .Net Framework 4.7 ■ Microsoft SQL Server Management Objects (SMO) DLL

Database Settings Created Automatically During Installation

You must have a server admin account (or equivalent) for these elements to auto-create when you install Workspace ONE Assist.

Note Each of these elements are created on the Database Server automatically when the installer runs.

Server Roles	<ul style="list-style-type: none"> ■ Sysadmin. ■ Bulkadmin. ■ Dbcreator.
User Mapping	<ul style="list-style-type: none"> ■ Downer. ■ Dbbackupoperator. ■ SQLAgent dependent. ■ serverGroup dependent.
Users	<p>Apdbuser</p> <p>Server role: Db_creator.</p> <p>Database role: Db_owner for all aetherpal user databases. On MSDB, database role to create SQL jobs.</p> <p>[SQLAgentOperatorRole]</p> <p>[SQLAgentReaderRole]</p> <p>{SQLAgentUserRole}</p> <p>Apadminuser</p> <p>Server role: Db_creator, to create multitenant databases.</p> <p>Database role: Db_owner for all aetherpal user databases. On MSDB, database role to create SQL jobs.</p> <p>[SQLAgentOperatorRole]</p> <p>[SQLAgentReaderRole]</p> <p>{SQLAgentUserRole}</p>

Domain Name Service

Domain Name Service is optional for on-premises multiple server deployments of Workspace ONE Assist. Domain Name Service is NOT required on single-server deployments (App+Core+Portal+CP).

In multiple server deployments, the Workspace ONE Assist server requires a forward lookup zone and three DNS records within the forward lookup zone. These records enable devices to communicate properly with the components within the Workspace ONE Assist server. The forward lookup zone, the host record, and service records all must point to the Workspace ONE Assist server.

Requirement	Description
Forward Lookup Zone	<p>Create a forward lookup zone that points to your Workspace ONE Assist server.</p> <p>The forward lookup zone must be named.</p> <pre>controlplane.aetherpal.internal</pre>
Host (A) Record	<p>The Host (A) Record must be named the following.</p> <pre>admin</pre> <ul style="list-style-type: none"> ■ If the Workspace ONE Assist Server is behind a load balancer, then the Host (A) Record must point to the internal IP address of the VIP (also known as Virtual IP) for the load balanced pool. ■ If the Workspace ONE Assist server is not behind a load balancer, then the Host (A) Record must point to the Workspace ONE Assist Server IP address.
Service Coordinator Service Records	<ul style="list-style-type: none"> ■ Record type: SRV. ■ Domain: controlplane.aetherpal.internal ■ Service: _svc. ■ Protocol: _tcp. ■ Priority: 0 ■ Weight: 0 ■ Port number: 8870 ■ Host Offering this service: admin.controlplane.aetherpal.internal

Custom Lookup Zone

You can use a custom **Forward Lookup Zone** with the Domain Name Service in place of the prescribed zone above. Full instructions on entering a custom lookup zone are provided in steps 11 and 14 of the [Advanced \(Custom\) Installation of Workspace ONE Assist](#). See [Advanced \(Custom\) Installation of Workspace ONE Assist](#).

Network and Security Requirements

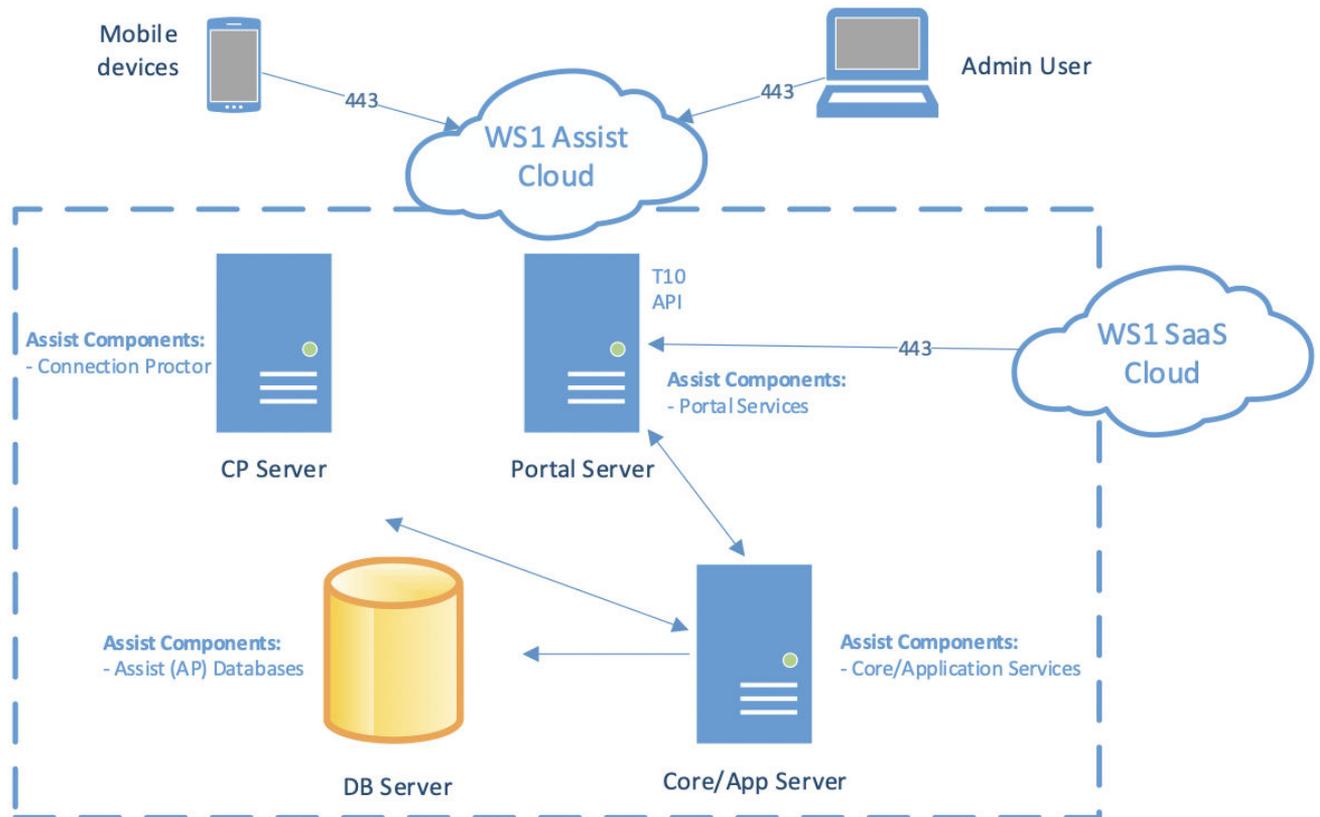
3

While configuring your network, you must take security measures into account whether you are in a SaaS or an on-premises environment.

SaaS Configurations

With a cloud-based implementation, the Workspace ONE Assist software is delivered as a service (SaaS). The integration between your Workspace ONE UEM SaaS tenant and your Workspace ONE Assist SaaS deployment is configured for you.

Figure 3-1. Workspace ONE Assist SaaS Deployment



If you want your Workspace ONE Assist to run in a SaaS configuration, you must whitelist the following fully qualified domain names (FQDNs) and IP addresses.

The FQDNs and IPs are region specific, so add these to your whitelist based on your location. The port is 443.

- US Portal Server - <https://rm01.awmdm.com> 52.207.131.208
 - US CP Server 01 rmsession01.awmdm.com 52.207.186.27
 - US CP Server 02 rmsession02.awmdm.com 34.195.109.57
 - US CP Server 03 rmsession03.awmdm.com 3.224.230.18
 - US CP Server 04 rmsession04.awmdm.com 52.200.22.165
 - US CP Server 05 rmsession05.awmdm.com 3.221.52.58
 - US CP Server 06 rmsession06.awmdm.com 18.211.168.20
- UK Portal Server <https://rmuk01.awmdm.com> 35.176.238.148
 - UK CP Server rmuksession01.awmdm.com 35.177.197.211
- Canada Portal Server <https://rmca01.awmdm.com> 52.60.162.133
 - Canada CP Server rmcasession01.awmdm.com 52.60.196.137
- Germany Portal Server - <https://rmde01.awmdm.com> 52.28.212.69
 - Germany CP Server - rmdesession01.awmdm.com 52.28.80.78
- Australia Portal Server <https://rmau01.awmdm.com> 52.62.156.193
 - Australia CP Server rmausession01.awmdm.com 13.55.186.162
- Japan Portal Server <https://rmjp01.awmdm.com> 52.193.23.235
 - Japan CP Server rmjpsession01.awmdm.com 52.199.112.44

For more information, please see the following knowledge base article, https://kb.vmware.com/s/article/82567?lang=en_US

SaaS and On-Prem Config: Additional Network Requirements to Enable Firebase Cloud Messaging (FCM)

You can configure the Android Assist agent to receive a Firebase Cloud Message (FCM) directly from the Assist server during the connection process. Together with Workspace ONE Intelligent Hub for notifications, this configuration improves the establishment speed and reliability of connections, thus minimizing request timeouts and improving the overall admin experience.

To receive FCM notifications, the following endpoints must be accessible on the end user devices.

Destination Host	Ports	Purpose
fcm.googleapis.com, fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (for example Find My Device, EMM Console <-> DPC communication, like pushing configs)

Note Workspace ONE Assist On-Premises customers with closed networks can continue to invoke Workspace ONE Assist agent through Workspace ONE Intelligent Hub/AWCM which is enabled by default. It also serves as a backup in case of FCM failures.

On-Prem Config: IP Address and Port Translation, Single-Server On-Prem Deployment

The Workspace ONE Assist server is required to have one static IPv4 address. This address must be accessible from the mobile device network and the network from which Workspace ONE UEM users access the Workspace ONE Assist web portal. This IP address is translated to the all-in-one server's Portal (web) services and Connection Proctor (CP) services.

By default, web services are bound to port 443 and 80 and CP services are bound to port 8443, however, your IT team can customize these ports. If Network Address Translation (NAT) is used, one public facing static IP address is required translated to the internal IP address of the Workspace ONE Assist server.

Port	Service
80 *	Assist Internal Services
443 *	Portal Services and T10 API
8443 *	Connection Proctor Service

* Customizable port address

On-Prem Config: IP Address and Port Translation, Medium and Multiple-Server On-Prem Deployment

Each Connection Proctor server must have its own static IPv4 address that is accessible from the device network and the user network that is translated to the CP service using port 443. The server hosting Workspace ONE Assist Web/Portal Services must also have its own static IP address that is accessible from the device network and Workspace ONE UEM user network. The portal services are bound to port 443 and 80, however, your IT team can customize these ports.

If network address translation (NAT) is used, the public facing IP addresses must be translated to the internal IP addresses of the servers accordingly.

Core and application components and corresponding services can be deployed on a public facing server or in a private zone. CP services and Portal services must be able to communicate with these core and application services over of a range of ports.

Port	Service
80*	Portal Services on Portal Server
443*	Portal Services and T10 API
443*	Connection Proctor Service on CP Server. In a multiple server deployment, the CP server can have port 443. Port 8443 is not necessary since the server has 443 available.
8865	Data Tier Proxy (DTP)
8866	Messaging Entity (MSG)
8867	Data Access Proxy (DAP)
8870	Service Coordinator (SVC)
12780	Connection Proctor (CP) from Management Entity (ME)
20879	Management Entity

* Customizable port address

Database services are deployed on the database server. The Workspace ONE Assist system connects to the database server using an IP address, hostname, or instance name. Typically, SQL database allows connections on port 1433.

On-Prem Config: Persistence for Multiple Server On-Prem Deployment

Workspace ONE Assist supports IP and SSL persistence. SSL persistence is required for connection proctor servers as the SSL termination must be made at the server level.

SSL persistence is also required for T10 service communication. An SSL certificate must be present on the T10 server since this communication cannot be offloaded.

On-Prem Config: Firewall Rules, Single-Server On-Prem Deployment

Firewall rules can be summarized based on the number of allocated IP addresses to the Workspace ONE Assist system.

Source	Destination	Protocol	Port	Direction	Rule
Device and User Networks / Internet	CP Server	TCP/TLS/SSL	8443	Inbound	Accept
Device and User Networks / Internet	Portal Server	TCP/HTTPS	443	Inbound	Accept
Workspace ONE portal server	Portal Server (T10 Interface)	TCP/HTTPS	443	Inbound	Accept
Workspace ONE Assist server	MS SQL Database Server	TCP	1433	Inbound	Accept

On-Prem Config: Firewall Rules, Multiple Server On-Prem Deployment

Source	Destination	Protocol	Port	Direction	Rule
Device and User Networks / Internet	CP Server	TCP/TLS/SSL	443 In a multiple server deployment, the CP server can use port 443. Port 8443 is not necessary since the server has 443 available.	Inbound	Accept
Device and User Networks / Internet	Portal Server	TCP/HTTPS	443	Inbound	Accept
Workspace ONE portal server	Portal Server (T10 Interface)	TCP/HTTPS	443	Inbound	Accept
CP Server and Portal Server	Core/App Server	TCP	8865, 8866, 8867, 8870	Inbound	Accept
Core/App Server	CP Server	TCP	12780	Inbound	Accept
Core/App Server	Database Server	TCP	1433	Inbound	Accept

On-Prem Config: Fully Qualified Domain Name and Site SSL/TLS Certificate, Single-Server On-Prem Deployment

The Workspace ONE Assist system requires one FQDN assigned to the static IP address which is used for Portal Services and for Connection Proctor services.

The Site SSL/TLS certificate has the following attributes in a single-server deployment:

- It is used for TLS/SSL bindings for Portal services.
- It is used in IIS for the Portal Services bound to port 443.
- It corresponds to the FQDN.
- It is used for the Connection Proctor Service bound to port 8443.
- It contains both public and private key pairs.

- It must be installed on the Workspace ONE Assist server's personal certificate store before the Workspace ONE Assist software is installed.

Obtain your SSL/TLS certificate from a well-known certificate authority such as Comodo, GoDaddy, and so on. If you prefer a self-signed certificate, then you must establish trust between the Assist Agent and the self-signed certificate.

Note For Android (Legacy) devices, self-signed certificates are only supported on Android 6.0 and earlier. The root and intermediate certificates/public key pair must be installed on mobile devices you intend to remote into. For Android devices, please see [Establish Trust for the Self-Signed SSL Certificate](#).

On-Prem Config: Fully Qualified Domain Name and Site SSL/TLS Certificate, Multiple Server On-Prem Deployment

One FQDN is assigned to the Portal server and one FQDN is assigned to each CP server deployed in the Assist system. If a single CP server is deployed, you must have 2 FQDNs. If 2 CP servers are deployed, then 3 FQDNs are required, and so on.

You can obtain a SAN or wildcard site SSL/TLS certificate used for TLS/SSL IIS bindings for the Portal Services. The same SAN or wildcard certificate can be used for the CP servers to bind the CP services. If you have a separate SSL/TLS certificate for each server, then each server must have its own certificate installed. The certificates must correspond to the FQDN assigned to the servers. The certificates must contain both private and public key pairs and they are installed on the server's local machine certificate store.

Obtain your SSL/TLS certificates from a well-known certificate authority such as Comodo, GoDaddy, and so on. If you prefer a self-signed certificate, then you must establish trust between the Assist Agent and the self-signed certificate.

Establish Trust for the Self-Signed SSL Certificate

To ensure security, you must obtain the SSL certificate issued by a trusted Certificate Authority (CA). Still, if you want to use a self-signed SSL certificate, you must establish trust between your Assist agent and the self-signed SSL certificate.

Note For Android (Legacy) devices, self-signed certificates are only supported on Android 6.0 and earlier. The root and intermediate certificates/public key pair must be installed on mobile devices you intend to remote into.

To establish trust for the self-signed SSL certificate, you must perform the following tasks:

- 1 Generate hash key from the RM console.
- 2 Update the self-signed certificate key value in the RM console.
- 3 Publish the SSL configuration to the devices from the Workspace ONE UEM console.

Generate hash key from the RM console

To allow the support for the Self-Signed SSL Certificate, two key value parameters must be passed to the Assist agent. For this, you must generate the hash key using the self-signed SSL root and intermediate certificate.

- 1 Open your browser and log into the AdminWebPortal using your credentials.
- 2 Click **ADMIN** from the top menu and then select **Client Configuration**.
- 3 From the Client Configuration drop-down menu, select **EMM AppConfig Assistant**.
- 4 For the **Base64 ssl certicate public key**, click **Choose file** and browse to the location where the Root.crt file is stored.
 - a Select the Root.crt file and click **Open**.
 - b Click **Generate Hash** on the RM console.
- 5 Click **Choose file** again and browse to the location where the Intermediate.crt file is stored.
 - a Select the Intermediate.crt file and click **Open**.
 - b Click **Generate Hash** on the RM console.
- 6 Click **Choose file** again and browse to the location where the End User Certificate (com.crt) is stored.
 - a Select the End User Certificate file and click **Open**.
 - b Click **Generate Hash** on the RM console.
- 7 Copy the generated hash key. This key is used as the input for the application configuration that is pushed from the Workspace ONE UEM console to the device while enrolling the device to the Assist server.

Update the Self-Signed certificate value in the RM console

After you generate the hash key, you must update the key value to True for the self-signed certificate in the RM console. This update enables the trust on the self-signed certificate.

- 1 For the **Trust self signed certificate**, click the **Edit** icon.
- 2 Change the key value from False to True and then click the **Update** icon.

Publish the SSL configuration from the Workspace ONE UEM console

To ensure the devices have the root and intermediate certificates, you must publish the SSL configuration to the devices from the Workspace ONE UEM console.

- 1 Open the browser and log into the Workspace ONE UEM console.
- 2 Navigate to **Devices > Profiles & Resources > Profiles** and select **Add**.
- 3 Select **Add Profile** and then select **Android**.
- 4 Configure the **General** settings. Enter the name and the groups to which the profile must be pushed.

- 5 Select the **Custom Settings** payload and then select **Configure**.
- 6 Enter the SSL configuration details in the custom settings field. The hash key that you generated previously from the RM console must be added as a parameter value to the configuration details.

```
<characteristic type="com.airwatch.android.androidwork.app:com.airwatch.rm.agent"
  uuid="c5f7a5a7-7fe5-4053-b736-f0023717e1eb" target="1" ><parm
  name="device.security.ssl.b64pubkeys" value="{ENTER SSL HASH HERE}"
  type="string" /><parm name="device.security.ssl.pinselfsignedcert" value="true"
  type="boolean" /></characteristic>
```

- 7 Select **Select & Publish**. The configuration details are pushed to all the devices enrolled to the Organization Group (OG).

Note

- The same configuration can also be done through the Profiles tab listed under Staging & Provisioning.
- After the configuration is pushed to the device, check the troubleshooting logs for successful initiation of remote management.

If not initiated, re-save the agent settings or uninstall and re-install the Assist agent and check for troubleshooting logs.

- This configuration works only with Intelligent Hub 19.03 or later. The parsing error seen in earlier versions of the Hub has been fixed in version 19.03.
 - The app configuration is currently supported for Android Enterprise enrolled devices.
-

On-Premises Deployments Across Public and Private Security Zones

Security zone configuration for Workspace ONE Assist depends upon whether your on-prem environment is composed of a single server or multiple servers.

Single-Server Deployments

The database component can be installed on a database server in the private zone while the rest of the components are installed on the all-in-one server in the public zone. You can deploy the all-in-one server either in the public or private zone but the all-in-one server **MUST** be accessible from the device network and the user network that uses the Workspace ONE Assist system.

Medium and Multiple Server Deployments

You can deploy Workspace ONE Assist servers across multiple security zones, such as DMZ/public and private. You can deploy all servers in a public zone or a private zone, depending on the network/security requirements. You can also deploy servers across any zone, provided the servers hosting Connection Proctor services and Portal Services are accessible from the device network and user network.

Typically, in multiple server deployments, components must be accessed by the device network and the user network. Because of this dependency, servers deployed in the Public zone include servers hosting Connection Proctor components and Portal services components. Servers deployed in private zones can include Application, Core, and Database components.

Based on hardware scaling, if the Core, Application, and Portal services components are deployed on the same server (CAP server), then this server must be deployed in a public zone. Connection Proctor servers are also deployed in the public zone. The database server is deployed in the private zone.

Supported Platforms

4

Workspace ONE Assist supports Remote Control for Android, macOS, Windows 10, and Windows Mobile devices. iOS devices are supported but only as far as the Remote View feature.

Android Devices

- Android devices managed by Workspace ONE Intelligent Hub 19.02 or later.
 - Download and install the latest version of the Workspace ONE Assist APK from the My Workspace ONE™ documentation repository (<https://my.workspaceone.com/>).
 - Android devices running Android 5.1 (Lollipop) or later support Remote View ONLY without a corresponding service application.
 - Android devices running Android 4.4 (Kit Kat) and later support full remote control with a corresponding OEM-specific service application installed. Download and install this OEM-specific service application by visiting the My Workspace ONE™ documentation repository (<https://my.workspaceone.com/>). Devices manufactured by Samsung, Sony, and Zebra (Android 11 and later only) support full remote control without a corresponding OEM-specific service application.
 - Samsung devices operating with a Work Profile in a BYOD or COPE enrollment require the Knox Service Plugin application (except those running Android 10 and later) to be installed after the Assist Agent is installed. For more information, see [How Do You Enable Remote Control with Samsung Knox Service Plugin](#).
 - On Samsung devices without the KNOX libraries, Workspace ONE Assist supports Remote View, File Manager, and Command Line client tools only. The Remote View functionality requires that the device end user allows screen sharing at the start of a session.
 - On devices running Android 9 and older, this is a one-time prompt.
 - On devices running Android 10 and later, this prompt must be accepted by the device end user at the start of each Assist session.

For details, see [Supported Features by Enrollment Type and Ownership, Android and Full Remote Control Support by Original Equipment Manufacturer \(OEM\) and Model, Android](#).

Windows 10 Devices

- Windows 10 devices running Windows 10 Anniversary Update (version 1607, code named Redstone 1) or later for Enterprise and Professional editions only.
- Windows 10 Enterprise Long-Term Servicing Channel (LTSC)
- Windows 10 in Kiosk Mode
- Microsoft .NET framework 4.6.2
- 64-bit OS required.
- Managed by Workspace ONE Intelligent Hub 1907 or later.
- Unmanaged Windows 10 devices enrolled with Registered Mode are also supported. For details on configuring registered mode, see the *Enrolling Windows 10 Devices into Workspace ONE UEM* topic of the *Windows Desktop Documentation*.
- Download and install the latest version of the Workspace ONE Assist agent (MSI file) from the My Workspace ONE™ documentation repository (<https://my.workspaceone.com/>).

iOS Devices

Managed iOS devices can only be viewed using Remote View, a feature in Workspace ONE Assist. iOS devices do not require a separate Assist app.

- iOS devices running version 12.2 or later.
- Managed by Workspace ONE Intelligent Hub 19.3 or later.
- On Workspace ONE UEM version prior to 2101, no configurations needed to enable Remote view on iOS devices
- On Workspace ONE UEM version 2101 or later, a privacy flag is introduced to enable or disable Remote View on iOS devices at an Organization Group (OG) level.

To configure the privacy flag, navigate to **Groups & Settings > All Settings > Devices & Users > General > Privacy**. On the Privacy screen, turn on or off the Remote Control flag for each ownership type. On existing Customer Organization Groups, this flag value remains the same as the previous value set prior to the 2101 upgrade. On new Customer Organization Groups, this flag is disabled by default. To enable Remote view, turn on the flag for the necessary ownership types.

macOS Devices

macOS devices can only be remotely controlled with the Share Screen client tool provided they are within these specifications and environments.

- Managed by Workspace ONE Intelligent Hub 1912 or later.
- Workspace ONE UEM 1912 or later.

- macOS devices running 10.13 (High Sierra) or later.
 - **Note** With regard to the permission prompts for the Remote View and Remote Control functions on macOS devices, be aware of the following.
 - macOS devices running version 10.13 (High Sierra) and 10.14 (Mojave) allow the **Share Screen** feature by default. No additional permissions are required to share the screen, therefore, no prompt is displayed at the beginning of a **Share Screen** session.
 - For macOS devices running version 10.15 (Catalina), the **Share Screen** and **Remote View** features both require that you enable the **Screen Recording** permission to Workspace ONE Assist in the **Privacy** tab of **Security & Privacy** preferences, located in System Preferences. Only during the first time you initiate a **Share Screen** session with a qualifying macOS device, an access request popup displays including a convenience link to this privacy setting in System Preferences.
 - Similarly, macOS devices running version 11 (Big Sur) or later must enable **Screen Recording** permission to Workspace ONE Assist for both **Remote View** and **Share Screen** features. This permission is configured in a slightly different way for version 11:
 Enable Screen Recording by navigating to **System Preferences > Security & Privacy > Privacy tab > Screen Recording** then select the **Lock** icon to unlock the Privacy settings and enter the **Administrator password**. This is a one-time activation by the end user.
- Download and install the latest version of the Workspace ONE Assist agent from the My Workspace ONE™ documentation repository (<https://my.workspaceone.com/>).

Windows Mobile

- Windows Mobile/CE running .NET 2.0 or later.
- Managed by Workspace ONE Intelligent Hub 6.0.4 or later.
- Download and install the latest version of the Workspace ONE Assist agent (MSI file) from the My Workspace ONE™ documentation repository (<https://my.workspaceone.com/>).

Supported Features by Enrollment Type and Ownership, Android

Feature support for Android devices can be categorized by enrollment type (legacy, COPE, BYOD, Fully-Managed), ownership (Personal, Work Profile), and whether the device is made by Samsung or not.

Samsung Devices					
Enrollment Type	Ownership	Remote Management	OS Version	Assist Presence	Knox Plugin

Legacy	Device Administrator	Supported	Android 4.4 – 10.x	Provisioned as an internal application.	Not Required, but a Knox permission prompt is displayed one time.
Fully Managed	Device Owner	Supported	Android 4.4 and later	Provisioned as an internal application.	Not Required, but a Knox permission prompt is displayed one time.
BYOD	Personal Profile	Not Supported	n/a	n/a	n/a
	Work Profile	Supported (view and control Work profile apps only)	Android 9.x	Provisioned as a public application from the play store.	Required, including a Premium Knox License Key to activate remote control APIs.
COPE	Personal Profile	Supported	Android 9.x ONLY	Provisioned as an internal application.	Required, including a Premium Knox License Key to activate remote control APIs.
			Android 10.x	Provisioned as an internal application.	Not Required for non-premium work profiles.
	Work Profile	Supported (view and control Work profile apps only)	Android 9.x and 10.x	Provisioned as an internal application.	Not Required for non-premium work profiles.
			Android 11 and later	Provisioned as a public application from the play store.	Not Required for non-premium work profiles.
Non Samsung Devices (with OEM-signed Assist Service)					
Enrollment Type	Ownership	Remote Management	OS Version	Assist Presence	Knox Plugin
Legacy	Device Administrator	Supported	Android 4.4 – 10.x	Provisioned as an internal application.	n/a
Fully Managed	Device Owner	Supported	Android 4.4 and later.	Provisioned as an internal application.	n/a
BYOD	Personal Profile	Not Supported	n/a	n/a	n/a
	Work Profile	Supported	Android 4.4 and later.	Provisioned as a public application from the play store.	n/a
COPE	Personal Profile	Supported	Android 9.x and 10.x ONLY.	Provisioned as an internal application.	n/a

Work Profile	Supported	Android 9.x and 10.x.	Provisioned as an internal application.	n/a
		Android 11.x and later.	Provisioned as a public application from the play store.	n/a

Which Profile/Ownerships Work with Samsung Knox

Only certain combinations of Android and Knox plugin versions with device ownership and profile types are compatible to make devices work with Workspace ONE Assist.

	Android 8.0 with Knox versions earlier than 3.4.1	Android 9.0 with Knox versions earlier than 3.4.1	Android 10.0 with Knox 3.4.1 or later	Android 11.0 with Knox 3.4.1 or later
Work Profile	Not supported - Knox Service Plugin is not available.	Supported by enabling remote control within Profile Owner using the Knox Service Plugin and Premium Knox License. See How Do You Enable Remote Control with Samsung Knox Service Plugin .	Supported - remote control is enabled on the work profile by default.	Supported - remote control is enabled on the work profile by default.
Premium Work Profile	Not supported - Knox Service Plugin is not available.	Supported by enabling remote control within Profile Owner using the Knox Service Plugin and Premium Knox License. See How Do You Enable Remote Control with Samsung Knox Service Plugin .	Supported by enabling remote control within Profile Owner using the Knox Service Plugin and Premium Knox License. See How Do You Enable Remote Control with Samsung Knox Service Plugin .	Supported by enabling remote control within Profile Owner using the Knox Service Plugin and Premium Knox License. See How Do You Enable Remote Control with Samsung Knox Service Plugin .
COPE (personal side)	Supported - Assist pushed as an Internal app to the personal side can view and control the screen within the personal space ONLY.	Supported - Assist pushed as an Internal app to the personal side can view and control the screen.	Supported - Assist pushed as an Internal app to the personal side can view and control the screen.	Not supported - Assist app can ONLY be installed within the Work Profile through the Managed Play Store and cannot view or control the personal side.
BYOD (personal side)	Not supported - Assist app can ONLY be installed within the Work Profile through the Managed Play Store and cannot view or control the personal side.	Not supported - Assist app can ONLY be installed within the Work Profile through the Managed Play Store and cannot view or control the personal side.	Not supported - Assist app can ONLY be installed within the Work Profile through the Managed Play Store and cannot view or control the personal side.	Not supported - Assist app can ONLY be installed within the Work Profile through the Managed Play Store and cannot view or control the personal side.

Full Remote Control Support by Original Equipment Manufacturer (OEM) and Model, Android

Your Android device can enjoy full remote control support for Workspace ONE Assist if its model is listed here and you have installed its OEM-specific service application, available at the My Workspace ONE™ documentation repository.

Workspace ONE Assist supports the following versions of the Assist service application:

- Version 2.3
 - Compatible with Assist agent version 5.2 and above.
 - Enables Remote view and control capabilities on Android devices.
 - Enables Key injection on Android devices (ability to pass in values from a remote keyboard)
 - Enables File manager capabilities on the android devices
- Version 2.5
 - Compatible with Assist agent version 5.2 and above.
 - Enables remote view and control capabilities on android devices.
 - Enables key injection on android devices (ability to pass in values from a remote keyboard).
 - Enables File manager capabilities on the android devices.
 - Enables remote reboot with auto-reconnect on android devices.
 - Supports scoped storage on android 11 devices without end user input.

Visit <https://my.workspaceone.com/products/Workspace-ONE-Assist> to download the OEM-specific service application for your Android device of the following OEM/models.

OEM Models

- Airbus
- Archos Sense 50X
- Ascom Myco3
- Bitatek
- Bixelon H3
- Blackberry KeyOne
- Bluebird
- Bluebird (Android 9+)
- Cipherlab
- Curbell
- Datalogic
- Edovo Rockchip
- Elotouch
- Elotouch M50C
- Ecom Ex02
- Fortuneship-Alps i-ONiCA 801EX
- Getac ZX70
- Getac ZX70G2
- Handheld Algiz RT7
- Handheld Nautiz 6
- Honeywell
- Honeywell NEXTGEN
- Honeywell CT60
- HP
- Huawei
- Innovi
- Innovi-ChecOut-E1
- Intermec
- iSafe - IS5201
- iSafe - IS910.1
- ITOS
- INCO L608
- I-Ruggy D41A
- Janam
- JREN
- KAICOM-H702
- Kyocera DuraForce Bell
- Kyocera-DuraForce-Pro
- Kyocera E7110
- Lenovo TBX705L
- Lenovo Tab4
- LG
- M3 Mobile SM10
- M3 Mobile SM15
- M3-SL10
- MobileDemand A1180
- MobileDemand Flex 10A
- Motorola LEX L11e
- Nokia 5.3
- Nokia 6.1
- Nokia 6.2
- Nokia 7.1
- Nokia 7.2
- Nokia 9
- Newland MT65
- Newland MT90
- Newland NQ1000
- Outform Rockchip
- Panasonic
- Point Mobile
- Protech-MH-5108
- Paytel
- Panasonic
- RealWear
- Rhino-Mobility-
- Rhino-T5se
- RugGear RG725
- Samsung
- SEUIC
- Sonim
- Sonim XP3800
- Sonim XP5s
- Sonim XP8
- Sony
- Spectralink Versity
- Staples - IBASE
- Staples - HP
- Sandata T5
- Touch Dynamic
- Trimble Nomad 5
- Thumbzup T67
- Unitech
- Unitech EA500
- Unitech TB85
- Unowhy SQOOL 4.0
- Unowhy SQOOL 4.1
- Urovo DT50
- XploreTech
- XploreTech M60

OEM Models	
<ul style="list-style-type: none"> ■ MediaWave ■ Mimo Monitors ■ Malata (M100, M120, IMS-M70 tablet) ■ Mobilebase DS6 ■ Mobile Demand ■ Mobile Demand A680 	<ul style="list-style-type: none"> ■ Zebra (This service application is only necessary for Zebra devices with Android 10.x or earlier. Zebra devices with Android 11.0 or later support Workspace ONE Assist out of the box). ■ Zone24x7

Capabilities by Platform

You can review all the major supported features of Workspace ONE Assist separated by platform.

Table 4-1.

	Android	iOS	macOS	Windows CE	Windows 10
Activity Log (accessed from the app)	✓ *		✓		✓
Attended Mode (BYOD/COPE)	✓	✓	✓		✓
Capture images or video	✓	✓	✓	✓	✓
Chat Messaging	✓		✓		✓
Control device buttons and keypad	✓			✓	
Manage files and folders	✓		✓	✓	✓
Muti Monitor Support			✓		✓
On Screen Notifications and Controls (Halo)	✓ *		✓		✓
Registry editor				✓	
Remote control	✓		✓	✓	✓
Remote view	✓	✓	✓		✓
Remote reboot with auto reconnect	✓			✓	✓
Role-based access to client tools	✓		✓	✓	✓
Run commands	✓		✓		✓
Screen draw	✓		✓		✓
Screenshot Capability	✓	✓	✓	✓	✓
Screen Recording	✓	✓	✓	✓	✓
Shortcuts to commonly used apps and settings	✓		✓	✓	✓
Session Collaboration	✓		✓		✓
Unattended mode (Rugged/Kiosk)	✓			✓	✓

Table 4-1. (continued)

View and export device info	✓	✓	✓	✓	✓
View list active processes and apps	✓ **		✓	✓	✓
Virtual on-screen keyboard	✓		✓	✓	✓
* Attended Mode only					
** Android 6 and earlier only					

Install Workspace ONE Assist to an On-Premises Environment

5

On-premises customers must install and configure the Workspace ONE Assist server(s).

There are two types of installations of Workspace ONE Assist.

- **Standard (Basic)**, for all-in-one single server installations.
- **Advanced (Custom)**, for medium installations where there is a separate CP server and a separate CAP server, or multiple server installations where the CP, Core, Application, and Portal services reside on separate servers. See [On-Premises Hardware Scaling Requirements](#).

Prior to running the installer on the server(s), you must first *Generate the Workspace ONE Assist T10 API Certificate*.

Generate the Workspace ONE Assist T10 API Certificate

You must generate the T10 API root and intermediate certificates used during an on-premises installation whether you are performing a **Standard (Basic)** or **Advanced (Custom)** installation. These certificates are also required for an on-premises build of Workspace ONE UEM while using Workspace ONE Assist in a **SaaS environment**.

Download the installer package, titled [VMware Workspace ONE™ UEM Remote Management Installer](#), from the myWorkspaceONE portal (<https://myworkspaceone.com>).

The certificate generator is called RemoteManagementCertificateGenerator_9_2. This installer must be run on a machine with the same locale settings as the database server to ensure that the same date format is set in the SQL script. You must run this certificate generator as an administrator.

- 1 Extract all contents from the installer package ZIP file into c:\temp of the Workspace ONE Assist server. Do not move the files around inside the temp folder as the installer needs all the files in their extracted locations. Do not rename or move the temp folder.
- 2 Run the Remote Management Certificate Generator which is included in the installer package.
- 3 In the UEM console, switch to your primary organization group (OG). The OG you select must be of a 'customer' type.

- 4 Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs**, scroll down to the Workspace ONE Assist section, and copy the string in the **Remote Management CN** text box. You are not able to see a **Remote Management CN** option unless you are in a 'customer' type OG.

Note If the Remote Management CN text box is blank, then you must manually [Create the Remote Management CN from the Workspace ONE UEM Database](#).

- 5 Set the following values.

Table 5-1.

Setting	Value
Certificate Type	Remote Management
Deployment	On-premises
Certificate Common Name	Paste the Remote Management CN copied from the preceding step (Step 4). Ensure the string you paste has 'CN'.

- 6 Select **Generate Certificates**.
- 7 Set Password for the certificates when prompted. Store this password for future use.
- 8 Navigate to the folder holding the Remote Management Certificate Generator.
- 9 Find the generated certificates file in the Artifacts\private folder called root_intermediate_chain.p7b. This is the T10 Certificate pair file that contains two major certificates that enable Workspace ONE UEM to communicate with the T10 portal. These certificates are the Workspace ONE UEM portal Root and Intermediate certificates.
- 10 Perform the action based on your environment.
 - **For On-Premises Environments** – Copy the p7b file generated in step 9 to the c:\temp\certs folder on the Workspace ONE Assist Server and proceed to step 11.
 - **For SaaS Environments** – Zip up the p7b file and email it to your account team or professional services team member. They will create a ticket for the Assist team with the certificate you provided. *Internal Account Teams and Professional Services Teams, refer to the following knowledgebase article for further instructions.* <https://ikb.vmware.com/s/article/79459>.
- 11 In the Artifacts folder, find the "Certificate Seed Script.sql". Run this script against the Workspace ONE UEM Database to seed the generated certificates into the Workspace ONE UEM database.

If you receive the error message "The conversion of a varchar data type to a datetime data type resulted in an out-of-range value," then see [Chapter 9 Troubleshooting Workspace ONE Assist](#). Support for multiple Workspace ONE UEM environments is available. For details, see [Configure Multi-Workspace ONE UEM Environment Support](#).

Install Site SSL Certificate, Assist On-Premises Only

You must incorporate a secure sockets layer (SSL) certificate into the Workspace ONE Assist on-premises installation process whether you are performing a **Standard (Basic)** or **Advanced (Custom)** installation.

SSL certificates provide secure, encrypted communications between a website and an Internet browser. The SSL certificate secures HTTPS binding for the management website for port 443 and allows a secure connection. This secure connection is between the admin and Web services. Also, the SSL certificate secures the connection to the Connection Proctor on port 8443 (or port 443 when the Connection Proctor (CP) Service runs on a separate server). You must provide the SSL certificate as a wildcard or SAN certificate.

If you are installing Workspace ONE Assist for the first time or upgrading to a newer version, you do not need to bind the SSL certificate to a website or renew the site thumbprint. However, if you are renewing an expired SSL certificate in between Workspace ONE Assist releases, you must bind the SSL certificate to a website and update the renewed site Thumbprint using AdminWebPortal. A link to each of those tasks appears directly after the following steps.

This process applies only to the SSL certificate. This process does not apply to the T10 API root and intermediate certificates.

- 1 Run the Microsoft Management Console (MMC).

Locate this application by typing 'mmc' into the search box found in the Start button.

- 2 In the File menu of the MMC application, select **Add/Remove Snap-in....** The Add or Remove Snap-ins dialog box displays.
- 3 Under **Available snap-ins** on the left panel, select **Certificates** and then select the **Add** button in the middle. The Certificates snap-in dialog box displays.
- 4 Select **Computer Account** and then select the **Next** button.
- 5 Select **Local Computer** and then select the **Finish** button.

Now the **Add or Remove Snap-ins** screen displays **Certificates (Local Computer)** under the Console Root on the right panel.

- 6 Select **OK** to finish. The main MMC window displays.
- 7 Expand the **Certificates (Local Computer)** on the left panel by selecting the **Greater Than** symbol. Select **Personal > Certificates**.
 - a If you do not have a Certificates folder to select, select the Personal folder and a Certificates folder will be created automatically.
- 8 In the **Action** menu of the MMC application, select **All Tasks** followed by **Import....** The Certificate Import Wizard displays.
- 9 Select **Next** to begin the Wizard.

- 10 Select **Browse...** to locate the SSL certificate in the PFX file format. You should familiarize yourself with the name of this file, since you must identify it by name in the future. Once located, select **Open** to import it.
- 11 Enter the certificate's **Password** when prompted. Add check mark only to the box labeled **Include all extended properties**.
- 12 Select **Next**.
- 13 Select **Place all certificates in the following store** and set the Certificate store to 'Personal'.
- 14 Select **Next**.
- 15 Confirm all the presented information is correct and then select **Finish**.

A new SSL certificate has been installed.

If you are installing Workspace ONE Assist, then you must decide whether you are running a [Standard \(Basic\) Installation of Workspace ONE Assist](#) or an [Advanced \(Custom\) Installation of Workspace ONE Assist](#).

- **Standard (Basic)**, for all-in-one single server installations.
- **Advanced (Custom)**, for installations with advanced options such as multiple servers to accommodate high availability and horizontal scaling.

If you are not installing Workspace ONE Assist but rather just updating an expired SSL certificate, then you must *Bind the SSL Certificate to a Management Site* followed by *Update the Renewed Site Thumbprint Using AdminWebPortal*.

Bind the SSL Certificate to a Management Site

If you are renewing an expired SSL certificate in between Workspace ONE Assist releases, you must bind the renewed SSL certificate to the website and update the renewed site Thumbprint using AdminWebPortal. This task binds the SSL certificate.

You do not need to manually bind the SSL certificate each time you install it. During the normal course of installing or upgrading the Workspace ONE Assist server, you must also install the SSL certificate. But the Workspace ONE Assist installation or upgrade process takes care of binding the SSL certificate to the website for you. You only need to follow these steps to bind the SSL certificate if you are manually renewing an expired SSL certificate in between Workspace ONE Assist installations or upgrades.

If you are installing or upgrading the Workspace ONE Assist server, do not take these steps.

- 1 Open Internet Information Services (IIS) on the Workspace ONE Assist server.
- 2 In the **Connection** pane on the left, expand the node of the server by selecting the triangle in front of the server name.
- 3 Expand the node of the **Sites** folder.
- 4 Right-click **Mgmt Web Site** and select **Edit Bindings...** The **Site Bindings** screen displays.

- 5 Select **https** and then select the **Edit** button. The **Edit Site Binding** screen displays.
- 6 Select the updated SSL certificate in the drop-down menu and then select **OK**.

The new SSL Certificate is now bound to the website.

Update the Renewed Site Thumbprint Using AdminWebPortal

If you are renewing an expired SSL certificate in between Workspace ONE Assist releases, you must update the renewed site Thumbprint. This task updates the Thumbprint with AdminWebPortal.

During the normal course of installing or upgrading the Workspace ONE Assist server, you must also update the site thumbprint. But the Workspace ONE Assist installation or upgrade process takes care of updating the site thumbprint.

You only need to follow these steps to update the site thumbprint with AdminWebPortal if you are manually renewing an expired SSL certificate in between Workspace ONE Assist installations or upgrades and have already bound it to the website.

If you are installing or upgrading the Workspace ONE Assist server, do not take these steps.

- 1 Start the MMC console from the Workspace ONE Assist server.
- 2 In the left-side panel, navigate to **Console Root > Certificates (Local Computer) > Personal > Certificates** and locate, by name, the SSL certificate you installed or updated recently.
- 3 Double-click this SSL certificate. The Certificate screen displays.
- 4 Select **Details** tab at the top.
- 5 In the **Show** drop-down menu, select **Properties Only**.
- 6 Click once on the text box **Thumbprint**. A series of number and letter pairs appears in the panel beneath the **Show** panel.
- 7 Select all these pairs of characters and copy them to the clipboard. Close the MMC console.
- 8 Open Notepad from the server desktop.
- 9 Paste the clipboard contents into the empty notepad screen.

Note The new thumbprint when you copy from the certificate is in lowercase. Ensure you change it to uppercase before pasting it in the AdminWebPortal. If unchanged, it can cause errors.

- 10 In Notepad, enter the keyboard shortcut **Ctrl-H**. The **Replace** screen displays.
- 11 Enter a single space in the **Find what** text box.
- 12 Click the **Replace All** button and then close the **Replace** screen by clicking the X.

All the spaces in between the number/letter pairs have been removed. Using notepad also takes the ANSI text copied from the MMC console and converts it to ASCII text, which is the format we want when we go to paste that thumbprint in the AdminWebPortal.

- In Notepad, select the newly formatted thumbprint and copy it to clipboard with **Ctrl-C**. Close Notepad.

- Open your browser and log into the AdminWebPortal using your credentials.

For example, <https://yourdomain.com/AdminWebPortal/login.aspx>

- Select the **Default Service Configurations**.

- In the **Search** bar, enter `certid`.

To display the search results properly, you might need to scroll down to the page size modifier and maximize the number of pages it can display. Doing this sets a large enough playing field to display any search result.

- Identify the certid in the **Parameter Name** column. `:ctl.svc.cnp.tch/certid`. In the **Options** column of the same line, select the Edit () icon.

Upon clicking the Edit icon, you might need to search for certid once again. Locate the certid **Parameter Name** and notice that the **Parameter Value** is now editable.

- Select the existing string of characters in the **Parameter Value** for `:ctl.svc.cnp.tch/certid` and replace it with the new Thumbprint string you have stored in your clipboard by applying the **Ctrl-V** keyboard shortcut.

Note Before you paste the new thumbprint, ensure you change the thumbprint from lowercase to uppercase; if unchanged, it can cause errors.

- Select the Save () icon.

- Select **Service Configuration**.

- Search for `ConnectionProctorService` and review its **Status** column.

- For both **Active** status and **Inactive** status for `ConnectionProctorService`, select the Edit () icon and update the `:ctl.svc.cnp.tch/certid` **Parameter Value** with the new Thumbprint string (**Ctrl-V**).

- Select the Save () icon for each, as applicable.

- Select the **Update** button at the bottom of the page.

- Restart all services (Core and IIS services). Select the Start menu and enter `run` on your keyboard. In the **Open** text box, enter `services.msc` The **Services** application displays.

- Locate all services that are labeled Aetherpal.

- Stop all these Aetherpal services.

28 Start all Aetherpal services.

The site Thumbprint has been updated.

Standard (Basic) Installation of Workspace ONE Assist

The Standard (Basic) method of installing the Workspace ONE Assist server, for on-premises environments that use all-in-one single servers, is a process that is composed of a single phase.

- 1 Download, extract, and save the Workspace ONE Assist installer into a temporary directory on the Workspace ONE Assist server. You can download the installer from the repository at <https://my.workspaceone.com>.
- 2 Right-click the installer file and select **Run as administrator**.
- 3 At the Welcome screen, select **Next**.
- 4 Enter the directory where you want to install the Workspace ONE Assist application and select **Install**.

Note The default installation directory can be customized to any location on the server.

- 5 Select Standard Installation (Basic) and then select **Next**.
- 6 If SQL Server is already installed on the server or on another server where Assist databases are deployed, select **Connect to existing SQL Server** and enter the required parameters.

Setting	Description
SQL server name	Define the SQL Server instance running on the server (such as \\SQLEXPRESS, (local), and so on).
Authentication	Select either Windows authentication to authenticate to SQL Server as current Windows user OR select SQL Server Authentication to select a SQL server account, such as SA.
User name	If SQL Server Authentication was used, type in the user name that is used to authenticate against the SQL server.
Password	Type in the password for the user name selected.

- a Select the **...More** button and enter additional details.

The installer creates two user accounts to access and maintain SQL databases. They are `apadminuser` and `apdbuser`.

- b Specify passwords for these accounts. When making user names and passwords, do not use the following special characters:
 - Ampersand - &
 - Less Than - <
 - Greater Than - >
 - Single Quote - '

- Double Quotes - "
 - Semicolon - ;
 - c Enter in the path for database MDF, LDF, and NDF files.
 - d Select **Save** to proceed.
You are taken back to the previous screen.
 - e Select **Next** to proceed.
- 7 In the **Tenant FQDN** text box, type in the FQDN for portal (web) services.
A Fully Qualified Domain Name is the complete domain name for a specific computer, or host, on the Internet. It consists of two parts: the host and the domain. For example, myhost.thedomain.edu.
- 8 In the **SSL Certificate** text box, select the folder button or the pull-down arrow to select the SSL certificate for the Workspace ONE Assist system that corresponds to the FQDN.
The certificate is installed in the local system personal certificate store.
- 9 Select the certificate and then select **OK**.
- 10 Deselect the **Apply Default Settings** check box and select the folder icon to attach the T10 certificate.
- 11 Browse for the T10 certificate (created while running the Certificate Generator tool in the artifacts folder), select the P7B certificate file, and then select **Open**.
- 12 Select the **...More** button to select additional settings for the Workspace ONE Assist system. Verify the parameters.

Settings	Description
HTTP Port	Defines the internal HTTP port used by portal services. By default, port 80 is selected. You can use a different port if port 80 is being used, such as 8080.
IIS Site Binding IP address	Defines from which interfaces/IP addresses portal services can be reached. By default, the setting is 'All Unassigned' to enable all interfaces/IPs.
HTTPS port	Defines the HTTPS port used by portal services for access from outside the network. By default, port 443 is selected. If port 443 is already being used in your environment for another purpose, then you can use a different port, such as 7443.
SSL Enable	Enables SSL/TLS protocol for portal services. By default, this check box is enabled so that the portal services use SSL/TLS. Leave this check box enabled.

Settings	Description
T10 user name and Auto Generated	Defines T10 API user for connectivity between AirWatch portal and Workspace ONE Assist system. By default, if 'Auto Generated' check box is enabled, the installer assigns a random user name to be created locally on the server. Leave this text box defaulted and the check box enabled for the Installer to create the T10 API user. If you want to define the user, disable the check box and type in the T10 user name you want to use.
CP FQDN/Port	Defines the FQDN and port on which CP services can be reached. Enter in the FQDN, which must be the same as the FQDN assigned for portal services. Enter port 8443, which is the default port for CP services. If port 8443 cannot be used, you can enter any other port. Be sure that network/security teams use this assigned port when assigning translation rules from the firewall/router to the RM Server for CP services.

13 Select **Save** to continue. You are taken to the previous screen.

14 Select **Next** to continue.

The installer performs multiple pre-requisite checks to ensure that the product can be installed. After the installer performs the prerequisites check, a summary report displays.

15 If any of the prerequisites are missing and the check fails, do NOT select Install.

- a Select **Detailed Report** link to see which prerequisites are missing.
- b To install missing prerequisite components, select the **Install Components** link. The installer installs the missing components.

You might need to reboot the server after the prerequisites are installed.

- c After the reboot, relaunch the installer.

The installer pre-populates with your previous selections.

16 If the initial prerequisite check comes back with all components passing, select **Install**.

Once the Install button is selected, the installation process begins.

Note Database execution might take an extended period.

17 When the installation finishes, select **Next** to continue.

18 When prompted to run the Resource Pack that loads all available device profiles onto the Workspace ONE Assist system, leave the **Execute Resource pack** check box selected (enabled) and then select the **Finish** button.

By default, the Resource Pack utility imports all device profiles by using a command-line window. After Resource Pack utility completes, the command-line window closes. For information about importing device profiles, see [Import Device Profiles with Resource Pack Utility](#)

Next, proceed to [Configure the Workspace ONE UEM console with Assist On-Premises](#).

Advanced (Custom) Installation of Workspace ONE Assist

The Advanced (Custom) method of installing the Workspace ONE Assist server for on-premises environments is a multiple phase process. The Advanced (Custom) installation features advanced options such as multiple servers to accommodate high availability and horizontal scaling. This installation allows for individual Assist components to be installed on separate servers which allow achieving the horizontal scaling.

Take the following steps and install Workspace ONE Assist with its advanced (custom) configuration.

- 1 Download, extract, and save the Workspace ONE Assist installer into a temporary directory on the Core, Application, and Portal (CAP) server. You can download the installer from the repository at <https://my.workspaceone.com>.
- 2 Right-click the installer file, and select **Run as administrator**.
- 3 At the Welcome screen, select **Next**.
- 4 Enter the directory where you want to install the Workspace ONE Assist application and select **Install**.

The default installation directory can be customized to any location on the server.

- 5 Select **Advanced Installation (Custom)** and then select **Next**.
- 6 Select all components for installation on the server.
 - Database
 - Core Services
 - Portal Services
 - Application Services
- 7 Select **Next**.
- 8 Configure the Database settings. Select **Connect to existing SQL Server** and complete the following settings.

Settings	Description
SQL Server Name	Enter the database server hostname.
Authentication	Select the database account authentication. The authentication can be either Windows Authentication or SQL Authentication .

Settings	Description
User name	Enter the user name of the database account. This user name is used by the installer to create all the databases required to install Workspace ONE Assist.
Password	Enter the password of the database account.

Note When making user names and passwords, do not use the following special characters:

- Ampersand - &
- Less Than - <
- Greater Than - >
- Single Quote - '
- Double Quotes - "
- Semicolon - ;

9 Select the **...More** button and complete the **Database Advanced Settings**.

Important If you are upgrading an existing installation, you must reenter your user name passwords. You must also reenter the paths of your MDF, LDF, and NDF file locations.

Note When making user names and passwords, do not use the following special characters:

- Ampersand - &
- Less Than - <
- Greater Than - >
- Single Quote - '
- Double Quotes - "
- Semicolon - ;

Settings	Description
DB Owner User name/ Password	Set the user name and password for the Workspace ONE Assist database owner SQL account. This account does not have system-wide permissions. The account only has permissions within the Workspace ONE Assist databases. This user name is apadminuser .
DB Application User name/ Password	Set the user name and password for the Workspace ONE Assist database application account. This user name is apdbuser .
MDF Path	Enter the path of the primary data file (MDF).
LDF Path	Enter the path of the transaction log file (LDF).
NDF Path	Enter the path of the secondary data file (NDF).

10 Select **Save** followed by **Next**.

11 Configure the Portal settings.

Settings	Description
Tenant FQDN	Enter the server fully qualified domain name. For example, "rmstage01.awmdm.com"
SSL Certificate	Select the folder icon and browse for the SSL Certificate already installed. For details, see Install Site SSL Certificate, Assist On-Premises Only .
SQL Server Name	Enter the database server hostname from the previous step.
Apply Default Settings.	Enable this check box to pre-populate the additional settings Enrollment Certificate, T10 Certificate, and License .
Apply Default Enrollment Certificate	If required, select a different Enrollment Certificate provided by the Assist support team.
Apply Default T10 Certificate	Deselect this check box and select the folder button to browse for and load the T10 certificate.

12 Select the **...More** button and complete the **Custom Portal Advanced Settings**.

Important If you are using port numbers other than the defaults referenced in Network and Security Requirements, you must enter these non-default port numbers here.

Settings	Description
DB Application User name/ Password	Enter the user name and password for the Workspace ONE Assist database application account. This user name is apdbuser .
HTTP Port	Enter the internal HTTP port used by portal services. The default is 80 but you can enter an alternate port number, such as 8080.
IIS Site Binding IP Address	Defines from which interfaces/IP addresses portal services can be reached. By default, the setting is 'All Unassigned' to enable all interfaces/IPs.
HTTPS Port	Enter the HTTPS port number. The default is 443 but you can enter your preferred port number.
SSL Enable	Enables SSL/TLS protocol for portal services. By default, this check box is enabled so that the portal services use SSL/TLS. Leave this check box enabled.
T10 user name And Auto Generated	Defines T10 API user for connectivity between AirWatch portal and Workspace ONE Assist system. By default, if 'Auto Generated' check box is enabled, the installer assigns a random user name to be created locally on the server. Leave this text box defaulted and the check box enabled for the Installer to create the T10 API user. If you want to define the user, disable the check box and type in the T10 user name you want to use.

13 Select **Save** followed by **Next**.14 Review your selections at the **Selected Components** screen, then select **Install** and wait for the installer to complete. Once the installer has finished, select **Next**.

- 15 Ensure that the check box **Execute Resource Pack** is selected and select the **Finish** button.
- 16 Download, extract, and save the Workspace ONE Assist installer into a temporary directory on the Connection Proctor (CP) server, right-click the installer file, and select **Run as administrator**.
- 17 At the Welcome screen, select **Next**.
- 18 Enter the directory where you want to install the Workspace ONE Assist application and select **Install**.
The default installation directory can be customized to any location on the server.
- 19 Select **Advanced Installation (Custom)** and then select **Next**.
- 20 Select the 'Connection Proctor' component for installation on the server.
- 21 Configure the Connection Proctor settings.

Important If you are using port numbers other than the defaults referenced in [Chapter 3 Network and Security Requirements](#), you must enter these non-default port numbers here.

Settings	Description
Connection Proctor FQDN	Defines the Fully Qualified Domain Name (FQDN) on which CP services can be reached. Enter in the FQDN, which must be the same as the FQDN assigned for portal services.
Port	Enter the port number for CP services. The default is 443 in multiple server environments but you can enter your preferred port number. Whatever port you select, ensure that network/security teams use this port when assigning translation rules from the firewall/router to the Workspace ONE Assist Server for CP services.
SSL Certificate	<p>Select the folder icon and browse for the SSL Certificate already installed. For details, see Install Site SSL Certificate, Assist On-Premises Only.</p> <p>SAN (subject alternative name) certificates are supported. The implementation of SAN certificates depends upon your server arrangement.</p> <ul style="list-style-type: none"> ■ The SAN certificate must have an FQDN defined for each connection proctor server and Workspace ONE Assist server. <ul style="list-style-type: none"> ■ For example, presume you have 2 connection proctor servers and 2 Workspace ONE Assist servers. The 2 Workspace ONE Assist servers host portal services, which require TLS/SSL traffic terminated at the load balancer. The FQDN for the SAN certificate must reflect the fully qualified domain name, for instance, "rmstage01.awmdm.com". ■ Meanwhile, for each of the 2 CP servers, TLS/SSL traffic terminates at the connection proctor, and therefore, you must have 2 FQDNs defined in the SAN certificate, for instance, "rmstage01.awmdm.com" and "rmstage02.awmdm.com".
SQL Server Name	Enter the database server hostname from the previous step.

Settings	Description
Apply Default Settings	Enable this check box to pre-populate the additional setting Enrollment Certificate .
Apply Default Enrollment Certificate	If required, select a different Enrollment Certificate provided by the Assist support team.

22 Select the **...More** button and complete the **Custom Connection Proctor Advanced Settings**.

Important If you are using port numbers other than the defaults referenced in Network and Security Requirements, you must enter the non-default port numbers here.

Settings	Description
DB Application User name / Password	Enter the user name and password for the Workspace ONE Assist database application account. This user name is apdbuser .
CP Internal IP Address/Port	Defines from which internal IP addresses the connection proctor can be reached. By default, the setting is 'All Unassigned' to enable all addresses. Enter the port number for the Connection Proctor component. The default is 8443 but you can enter your preferred port number.
Forward Lookup Zone	Under the CP Internal IP Address/Port drop-down menu, enable this check box and enter your forward lookup zone here. You can also enter a custom lookup zone. The Forward Lookup Zone setting is optional in a multi-server environment.

23 Select **Save** followed by **Next**.

24 At the **Selected Components** screen, review your selections. Once you have verified your configuration, select **Install**.

Proceed to Configure the Workspace ONE UEM Console with Assist On-Premises.

Configure the Workspace ONE UEM console with Assist On-Premises

After installing the Workspace ONE Assist server and all its components, configure the UEM console to communicate with the Workspace ONE Assist server.

- 1 In the UEM console, ensure that you are in the Global OG.
- 2 Navigate to **Settings > System > Advanced > Site URLs > Workspace ONE Assist**.

3 Complete the Workspace ONE Assist settings.

Settings	Description
Console Connection Hostname	Enter the Workspace ONE Assist server fully qualified domain name (FQDN) plus "/t10". For example: <pre>https://rmstage01.awmdm.com/t10</pre>
Device Connection Name	Enter the Workspace ONE Assist server fully qualified domain name (FQDN). For example: <pre>https://rmstage01.awmdm.com</pre>

4 Select **Save**.

The Workspace ONE Assist server is now ready to handle remote management sessions with end-user devices.

Integrate Deployment Model, On-Prem UEM With SaaS Assist

You can integrate an on-premises Workspace ONE UEM environment with a SaaS build of Workspace ONE Assist, in either single customer and multi-customer deployments.

You must have a working on-prem Workspace ONE UEM installation in order to integrate it with a Workspace ONE Assist SaaS environment.

The typical use case is that a partner with multiple on-premises Workspace ONE UEM environments (with single customer or multi-customer deployments) wants to add Workspace ONE Assist service. It is simple to integrate a SaaS build of Workspace ONE Assist to your on-prem Workspace ONE UEM build.

1 Update the Site URL of the External Remote Management in Settings.

- a In the UEM console, ensure that you are in the Global OG.
- b Navigate to **Settings > System > Advanced > Site URLs > Workspace ONE Assist**.

c Complete the Workspace ONE Assist settings.

Locale	Console Connection / Device Connection
USA	<p>Console Connection Hostname:</p> <p><code>https://rm01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rm01.awmdm.com/</code></p>
Canada	<p>Console Connection Hostname:</p> <p><code>https://rmca01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmca01.awmdm.com/</code></p>
Germany	<p>Console Connection Hostname:</p> <p><code>https://rmde01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmde01.awmdm.com/</code></p>
United Kingdom	<p>Console Connection Hostname:</p> <p><code>https://rmuk01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmuk01.awmdm.com/</code></p>
Australia	<p>Console Connection Hostname:</p> <p><code>https://rmau01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmau01.awmdm.com/</code></p>
Japan	<p>Console Connection Hostname:</p> <p><code>https://rmjp01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmjp01.awmdm.com/</code></p>
Singapore	<p>Console Connection Hostname:</p> <p><code>https://rmsg01.awmdm.com/t10</code></p> <p>Device Connection Name:</p> <p><code>https://rmsg01.awmdm.com</code></p>

The Workspace ONE Assist server can now communicate with Workspace ONE UEM.

- 2 Generate the Workspace ONE Assist T10 API Certificate. This step must be finished no matter what deployment model you are using, but it is the first set of certificates you generate for multi-Workspace ONE UEM environments. See [Generate the Workspace ONE Assist T10 API Certificate](#) and [Supported Deployment Models](#).

- If you are deploying a single customer Workspace ONE UEM environment, then proceed to step 3.
- If you are deploying a multi-customer Workspace ONE UEM environment, then you must .

- 3 Select **Save**.

The Workspace ONE Assist is now ready to handle remote management sessions with end-user devices.

- 4 [Chapter 7 Configure End-User Devices](#)

- 5 While logged into the Workspace ONE UEM console, navigate to **Devices > List View** and locate a suitable device to remotely manage. See [Chapter 4 Supported Platforms](#).

- 6 Select that device's *Friendly Name* to display **Device Details**.

- 7 Initiate a Workspace ONE Assist session on this device by selecting the **More Actions** button and then selecting **Remote Management**.

The single customer or multi-customer on-premises deployment of Workspace ONE UEM is now connected to the Shared SaaS build of Workspace ONE Assist.

Migrate Workspace ONE Assist from On-Premises to SaaS

When you are faced with migrating your on-prem installation of Workspace ONE Assist to a SaaS environment, you can follow these steps without having to uninstall and reinstall the Assist app on all devices.

Before you can migrate your Workspace ONE Assist to a SaaS environment, Workspace ONE UEM must already be in a dedicated SaaS environment. This Workspace ONE Assist migration cannot be applied to an on-premises build of Workspace ONE UEM.

- 1 Follow the instructions for **Step 1 Only** of [Integrate Deployment Model, On-Prem UEM With SaaS Assist](#) to configure the site URLs. Then return to this task to commence migration.
- 2 You must re-push the Intelligent Hub settings to all enrolled devices per the following substeps.
 - a **Android** – Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Intelligent Hub Settings**. No changes need to be made to this settings page, just select **Save**.

- b **iOS** – Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Intelligent Hub Settings**. No changes need to be made to this settings page, just select **Save**.
- c **macOS** – Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple macOS > Intelligent Hub Settings**. No changes need to be made to this settings page, just select **Save**.
- d **Windows CE & Mobile** – Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Rugged > Agent Settings**. No changes need to be made to this settings page, just select **Save**.
- e **Windows 10** – Navigate to **Groups & Settings > All Settings > Devices & Users > Windows Desktop > Intelligent Hub Settings**. No changes need to be made to this settings page, just select **Save**.

The device is silently re-enrolled into Workspace ONE Assist. The device end user is not prompted.

Configure Multi-Workspace ONE UEM Environment Support

If you want to operate the Workspace ONE Assist server across multiple Workspace ONE UEM environments (not multiple organization groups), then take the following steps.

You must have already completed all the steps in [Generate the Workspace ONE Assist T10 API Certificate](#).

Do not follow this procedure if you want Workspace ONE Assist to work with a single Workspace ONE UEM environment.

- 1 Log in to the **secondary or other** Workspace ONE UEM environment.

Do not log into the same environment you selected in **Step 4** of the topic [Generate the Workspace ONE Assist T10 API Certificate](#).

- 2 In the UEM console of this secondary environment, switch to your primary OG.

The OG you select must be of a 'customer' type. For more information about organization groups, see the topic **Organization Group Type Functions** from the **VMware Workspace ONE UEM Console Basics Documentation**.

- 3 Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs**, scroll down to the **External Remote Management** section, and copy the string in the **Remote Management CN** text box.

Note If this text box is blank, then you must manually [Create the Remote Management CN from the Workspace ONE UEM Database](#).

- Switch back to the Workspace ONE Assist server. Run the Remote Management Certificate Generator, which includes the Remote Management Installer, using the following values.

Setting	Value
Certificate Type	Remote Management
Deployment	Upload Intermediate
Certificate Common Name	Paste the Remote Management CN from Step 3 preceding

- Select the **Generate Certificates** button.
- When prompted, you must select the intermediate private cert.
This certificate and password is the same one you originally generated in **Step 8** of [Generate the Workspace ONE Assist T10 API Certificate](#). This certificate is located in `c:\temp\certs` of the Workspace ONE Assist server.
- On the Workspace ONE Assist server, locate the 'artifacts' folder, and run the SQL script file "Certificate Seed Script.sql" against the Workspace ONE UEM Database to seed the generated certificates into the Workspace ONE UEM database.
- Repeat this entire task for each additional Workspace ONE UEM environment you want Workspace ONE Assist to work with.

Example: If you want to add two additional environments to the environment you configured originally, then you must follow the steps of this task twice.

After you have finished installing the client certificate for each Workspace ONE UEM environment, proceed to [Configure the Workspace ONE UEM console with Assist On-Premises](#).

Upgrade to a New Version

Upgrading to a new version of Workspace ONE Assist is simple. Install a new version of Workspace ONE Assist on top of an existing, older version by taking the following steps.

Read through this entire section BEFORE you begin the installation process.

- To ensure that you do not run the old installer file in error, replace the previous version of the installer with the new version in the same folder. All certificates and the `install.config` file remain the same.
- Right-click the installer file and select **Run as administrator**. The installer prompts you to remove the currently installed components, excluding the database.
- Select **OK** and allow the installer to remove the installed components.
The **AirWatch Remote Management Uninstall Components** screen appears.
- Select **Next** and proceed with the uninstall process.

The **Uninstall Components** dialog box displays, listing each component it finds of the old version. Each of these components is selected with a green check mark. Notice that the Database or DB does not appear on this screen. This absence is because the old database is used during the upgrade process, which means everything on the database is kept intact in the new version of Workspace ONE Assist.

- 5 Select **Uninstall** and commence uninstalling the old components.

The uninstallation begins in earnest, displaying each component as it is removed.

- 6 Once all the old components are uninstalled, the **AirWatch Remote Management Setup** prompts you to install new versions of the same components. Select **Next** to begin.

- 7 The **Choose Install Location** prompt appears. The default installation location appears prepopulated in the text box, which it got from the install.config file. Proceed by selecting **Install**.

- 8 The **Get Started with AirWatch** screen displays, prompting you to select between **Standard Installation (Basic)** and **Advanced Installation (Custom)**.

For details about each installation method, including all steps, screens, text boxes, and options, see [Standard \(Basic\) Installation of Workspace ONE Assistor Advanced \(Custom\) Installation of Workspace ONE Assist](#)

- 9 The installer reads from the install.config file, applying all the original configurations it finds to the options screens, including SQL server details, user names, Tenant FQDN, certificates, database configurations, and many other configurations. You might not need to modify any of the settings it pulls from this install.config file with the possible exceptions below.

- **Check Database Accounts** - Depending upon your configuration and the existing permissions in your environment, the install.config settings might not be populated correctly. For this reason, review the database accounts to ensure that they are correct. Do this review at the first screen, **Installer - Basic - Database (Step 1 / 2)** by clicking the **...More** button which displays the **Database Advanced Settings** dialog box. Review the apadminuser and apdbuser accounts and respective passwords for accuracy and select **Save**. Ensuring these accounts are correct now saves you trouble later.
- **SSL Certificate** - If you installed a new SSL certificate before running this upgrade, ensure that you integrate it with the upgrade. Review the certificate at the second screen, **Installer - Basic - Application (Step 2 / 2)** by selecting the **SSL Certificate** drop-down menu and reviewing the name of the new SSL Certificate. If you have not installed a new SSL certificate before running this upgrade, then just ensure that the existing SSL cert is selected.
- **T10 Certificate** - When upgrading from an older version of ARM to a newer version, review the T10 certificate to make sure it is the correct one. If you are in doubt about this certificate's validity, on the **Installer - Basic - Application (Step 2 / 2)** screen, deselect the check box **Apply Default Settings**, select the folder button that corresponds to the **T10 Certificate**, and select the correct certificate file in P7B format.

- **Check the Ports** - At the **Installer - Basic - Application (Step 2 / 2)** screen, select the **...More** button which displays the **Portal Advanced Settings** screen.
 - Ensure all the ports it pulls from install.config are correct for your environment. You should know whether your environment is using port 8443, which is the default connection proctor port for Workspace ONE Assist.
 - If 8443 is not used by your environment, then ensure the **CP Port** text box is 8443.
 - If 8443 is being used by your environment, then you must select another **CP Port** in order for Workspace ONE Assist to function. Consider using port 8446 in such a case.
 - Select **Save** if you have made changes.
- 10 After you have reviewed all the settings above and made all applicable adjustments, proceed with the remainder of the installation by selecting the **Next** button.
- The **Installer - Selected Components** screen displays.
- 11 The **Installer - Selected Components** page confirms all the installer settings it plans to use for the upgrade. If you want to make changes, you can use the **< Prev** button to revisit config pages. Otherwise, select **Install** to begin the upgrade. The installer prompts you again for the installation location. Select **Install**.
- The database account is validated against the apdbuser and apadminuser accounts. During the upgrade, the Installing Database process displays "Error Message: DBAlreadyExists". This simply means it found the existing database and it has begun to upgrade it.
- 12 When the installation finishes, select **Next**.
- 13 The last step is to run the resource pack which consists of configuration files for hundreds of different devices. Ensure the **Execute Resource pack** check box is selected and click **Finish**.

The Workspace ONE Assist server has been upgraded.

Create the Remote Management CN from the Workspace ONE UEM Database

If the **Remote Management CN** text box is empty from step 5 of Generate Workspace ONE Assist Certificates or step 3 of Configure Multi-Workspace ONE UEM Environment Support, you can run an SQL script against the database to create the Remote Management CN manually.

- 1 Open the Remote Management Certificate Generator.

You must run this generator as an administrator.

- 2 Select the Question Mark button.
- 3 Copy the displayed text.

This text is the SQL script to run against the Workspace ONE UEM Database.

- 4 Switch to the Workspace ONE UEM Database server and open SQL Server Management Studio.
- 5 Create a query with the copied text.
- 6 On the first line of the query, replace the NULL value with the GroupID for the customer type OG that you want to use.

The OG you select must be a customer type, it cannot be of any other type including global, partner, container, and so on.

```
DECLARE @GroupID NVARCHAR(20) = NULL;
```

becomes

```
DECLARE @GroupID NVARCHAR(20) = 'RemoteManagement';
```

- 7 In the Results, copy the created Remote Management CN.

The Remote Management CN is used to generate the root and intermediate certificates for Remote Management. Return to **Step 5** of [Generate the Workspace ONE Assist T10 API Certificate](#) or **Step 3** of [Configure Multi-Workspace ONE UEM Environment Support](#).

Import Device Profiles with Resource Pack Utility

Device profiles contain the key mapping, device skin, and Workspace ONE Assist service signatures for full remote control. You can perform a bulk import of these device profiles onto your Workspace ONE Assist Server.

- 1 Run the Resource Pack Utility file provided. The file is called "AW RM Resource Pack Version - v0xx.exe"
- 2 Complete the **Authentication** step.
 - a Enter the **Target Tenant URL** specific to your environment. For example, https://rmstage01.awmdm.com
 - b Enter the user name and password. If new credentials have not been defined, use the default credentials.
 - User name: admin
 - Password: admin
 - c Enter the **Admin URL** of

```
http://admin.controlplane.aetherpal.internal:80
```

If you have not used the WBC portal yet and have not reset your default password, the Resource Pack Utility prompts you at this point to reset the password. Enter your new password and select the **Update Password** button to continue.

- 3 Complete the **Resource Import** step.

You can select one or more device profiles from the list or you can enable the Select All check box to initiate a full importation of all available device profiles.

- 4 Select the **Import** button to continue. The log panel on the right side fills up with confirmation messages which you can review.

The device profiles you selected are installed onto the Workspace ONE Assist server.

- 5 When finished importing device profiles, select the **Exit** button.

Configure Assist Admin User Access

6

To troubleshoot issues on end user devices or assist the users perform device tasks, the Workspace ONE Assist admins must be assigned custom roles with specific permissions set for the role.

Role-Based Access to Workspace ONE Assist

You can make customized roles based on Assist functionality and assign those roles to your admins, giving them varying level of access to Workspace ONE Assist's main features, including Remote View and Share Screen.

Roles specific to Workspace ONE Assist work the same as roles in Workspace ONE UEM. Roles are made of one or more resources (or permissions). Permissions specific to Workspace ONE Assist are included in the same pool of Workspace ONE UEM permissions.

Remote View Session Elevation

A role with the right combination of permissions can give your admins the ability to elevate the current Assist session, allowing them to go from using one client tool to using another in the middle of a session.

For example, if you make a role with the **Remote View** and **Remote Control** permissions, and assign that role to an admin, then that admin can start a Remote View session, provided the host device supports such functionality, and elevate that session to a remote control session simply by using the [Share Screen](#).

Such elevation reflects the natural progression of many Remote View sessions, where the admin completes an initial troubleshooting phase only to discover they require the full range of abilities afforded to them by the Share Screen client tool.

Assign Role Permissions for Workspace ONE Assist Client Tools

You can add resources, or permissions, to the roles you assign to admins with the Workspace ONE UEM console so they can use Workspace ONE Assist to help users of supported devices.

- 1 In the Workspace ONE UEM console, navigate to **Accounts > Administrators > Roles**. You must select between creating a new role and modifying an existing role.
 - a **Create a New Role** – Select the **Add Role** button. The **Create Role** screen displays. Complete the **Name** and **Description** options and proceed directly to step 2.
 - b **Modify an Existing Role** – From the roles listing, locate the role you want to edit, and select the edit icon () that appears to the left of the listing. The **Edit Role** screen displays.
- 2 Select the **Assist** category, located in the left pane labeled **Categories**. All six Assist-related resources, or permissions, display in the right pane.
- 3 Enable the **Allow** check box for the specific permission you want to apply to the role. There are six Assist-related permissions.
 - **Remote View** – "read only" view of the host device with the [Remote View](#).
 - **Remote Control** – "edit" view or full access to the [Share Screen](#).
 - **File Manager** – full access to the [Manage Files](#).
 - **Registry Editor** – full access to the [Registry Editor](#).
 - **Remote Shell** – functionality includes both the [Remote Shell](#) and the [Command-Line Interface, Android](#).
 - **Unattended Access** – provides access to only Windows 10 devices in [unattended mode](#). Unattended access for Android and Windows Mobile devices is handled using their respective dedicated agents.

Note The Unattended Access permission is enabled by default for the AirWatch Administrator and Console Administrator roles.

- 4 **Save** the role.
- 5 Next, you must assign the role to your administrator. Navigate to **Accounts > Administrators > List View** and locate the Administrator you want to assign the role to.
- 6 Select the **Edit** icon () to the left of the administrator user name. The **Add/Edit Admin** screen displays.
- 7 Select the **Roles** tab.
- 8 Select the **Add Role** button. Two empty text boxes display, labeled **Select Organization Group** and **Select Role**.
- 9 Fill the **Select Organization Group** text box with the organization group (OG) in your org structure you want this role assignment to apply.

If your admin is in this OG or downline of this OG, then they gain the abilities of this role. If your admin moves above this OG, or upline of this OG, then they lose the abilities of this role. The higher the OG you select here, the more OGs your admin can apply the abilities of this role.

10 Fill the **Select Role** text box with the name of the role from step 1.

You can repeat Steps 8 through 10 to assign as many roles to an admin as you want.

11 **Save** the role assignment.

Agent Modes

You can connect to devices remotely using two distinct modes of the Workspace ONE Assist agent: Attended Mode and Unattended Mode. Given the enterprise use cases, ownership models, and privacy requirements, understanding the difference between these modes is the foundation of a best practice.

IT and Help Desk staff can use Workspace ONE Assist to support devices in myriad enterprise use cases. These cases include Knowledge Worker employees (Corporate-Owned Personally Enabled (COPE) or Bring Your Own Device (BYOD)), used for business-critical tasks (for example, inventory scanning, logistics) by shift working employees. Contractors with rugged devices and devices used by customers in kiosks are among other use cases.

It is important that Workspace ONE UEM be configured to deploy the correct Workspace ONE Assist client to each device based on these use cases and the privacy requirements and expectations for each device.

Attended Mode

Attended Mode is intended for devices where the Remote User can contain personal or sensitive information and the Remote User can have an expectation or a legal requirement of privacy. Customers generally deploy Attended Mode for BYOD and COPE devices, providing additional privacy protection. In Attended Mode, the user is more actively prompted to authorize access to the device and its information.

- Attended mode is available on Android, iOS, macOS, and Windows 10 devices.
- Windows 10 BYOD devices always default to attended mode connection.
- Android BYOD devices and Windows 10 devices not connected to the Active Directory only support attended mode connection.
- Attended mode is not available on Windows Mobile/CE devices.

Unattended Mode

Unattended Mode is intended for devices that do not contain personal information and might require maintenance or support by IT when there is no Remote User physically using the device (for example, when charging on a cradle between shifts, when in the depot because it was returned as defective, as a customer-facing kiosk). Customers generally deploy Unattended Mode for corporate owned Rugged/Business Critical and Kiosk devices.

There are no device notifications when using Workspace ONE Assist in unattended mode when a session is active. You are solely responsible for notifying device end users of the active remote management session.

Workspace ONE Assist uses device ownership information received during enrollment to recognize devices as corporate or personally owned. Unattended mode is not available to devices identified as personally owned or devices in a non-supervised configuration.

- Unattended mode is available on Android, Windows 10, and Windows Mobile/CE devices.
- Unattended mode is not currently available on macOS devices.

Note On Samsung devices, a Knox permission must be accepted by the user when the application is first launched, even for devices in unattended mode.

Configure Unattended Access for Windows 10 Devices

Administrators must have the **Unattended Access** permission as part of their assigned role. For more information, see [Assign Role Permissions for Workspace ONE Assist Client Tools](#).

- **Kiosk Mode and Long-Term Servicing Channel (LTSC)** – All Assist sessions default to Unattended mode. Once connected, you have full control and are presented with the Log In screen. When you are logged into the Admin profile, all Assist Client Tools become functional. While in Kiosk Profile, however, the following features are unsupported.
 - Whiteboard
 - Halo (On-Screen notifications and controls)
 - Shortcuts (except Ctrl-Alt-Del)
- **Shared Terminals** – Assist supports unattended access on Windows 10 devices that meet the following criteria:
 - Domain joined
 - Azure AD device joined

When you connect to a Windows 10 device that meets the above listed criteria, you can select the connection mode during an Assist session.

To start a session, search for the Windows 10 device from the Device List View in the Workspace ONE UEM console and pull up the Device Details. Select the **Remote Assist** button and choose the **Screen Share** tool. When the connection initiates, you can select between Attended Mode and Unattended Mode.

- If Attended Mode is selected, the connection proceeds to the PIN screen, and the end user is prompted to enter that PIN per the normal procedure.
- If Unattended Mode is selected, Workspace ONE Assist determines the state of the remote device.
 - If the device is being actively used, then end user is prompted to accept the remote session. The end user can allow or deny the session. If the end user does not respond for more than 30 seconds, Assist locks the end user out, saving any information they may have been working on. You are then presented with the Log In screen.
 - If the device is not in use, a connection is established, and you are presented with the Log In screen.

Note

- On Screen notifications and Screen controls (Halo) are displayed on Windows 10 devices in Unattended Mode.
 - A session that is initiated by choosing the File Manager or the Remote Shell tool, defaults to Attended mode.
-

Configure End-User Devices

7

Now that the servers have been installed and configured you must install the platform-specific agents on the devices so that they can be remotely managed with Workspace ONE Assist. You may also have to enable the device to accept remote control.

Install the Assist App for Windows and macOS

- 1 Visit the <https://my.workspaceone.com/products> page that lists all the available device agents.
- 2 Identify and download platform-specific Workspace ONE Assist agents that are applicable to your deployment.

Note With regard to the permission prompts for the Remote View and Remote Control functions on macOS devices, be aware of the following.

- macOS devices running version 10.13 (High Sierra) and 10.14 (Mojave) allow the **Share Screen** feature by default. No additional permissions are required to share the screen, therefore, no prompt is displayed at the beginning of a **Share Screen** session.
- For macOS devices running version 10.15 (Catalina), the **Share Screen** and **Remote View** features both require that you enable the **Screen Recording** permission to Workspace ONE Assist in the **Privacy** tab of **Security & Privacy** preferences, located in System Preferences. Only during the first time you initiate a **Share Screen** session with a qualifying macOS device, an access request popup displays including a convenience link to this privacy setting in System Preferences.
- Similarly, macOS devices running version 11 (Big Sur) or later must enable **Screen Recording** permission to Workspace ONE Assist for both **Remote View** and **Share Screen** features. This permission is configured in a slightly different way for version 11:

Enable Screen Recording by navigating to **System Preferences > Security & Privacy > Privacy tab > Screen Recording** then select the **Lock** icon to unlock the Privacy settings and enter the **Administrator password**. This is a one-time activation by the end user.

Install the Assist App for iOS

iOS devices do not require a separate Assist application. The Assist libraries are built into the Intelligent Hub. To prepare your iOS devices to use the Remote View feature, see [How Do You Enable Remote View For iOS Devices](#).

On Workspace ONE UEM version 2101 or later, a privacy flag is introduced to enable or disable Remote View on iOS devices at an Organization Group (OG) level.

To configure this flag:

- 1 Navigate to **Groups & Settings > All Settings > Devices & Users > General > Privacy**.
- 2 On the Privacy screen, turn on or off the **Remote Control** flag for each ownership type.

On existing Customer Organization Groups, this flag value remains the same as the previous value set prior to the 2101 upgrade. On new Customer Organization Groups, this flag is disabled by default. To enable Remote view, simply turn the flag on for the necessary ownership types.

Install the Assist App for Android

- 1 Visit the <https://my.workspaceone.com/products> page that lists all the available device agents.
- 2 Download and install the platform-specific Workspace ONE Assist agent.
- 3 To provide full remote control support on Android devices, VMware has partnered with many of the top Android device manufacturers to make OEM-specific service applications. Download and install the OEM specific service application on the device.
- 4 If the launcher mode is enabled on Samsung devices, you must whitelist the following activities in order for you to be able to respond to the prompts during the installation of the Assist agent.

```
com.samsung.klmsagent.activities.ConfirmDialog
```

```
com.android.packageinstaller.permission.ui.GrantPermissionsActivity
```

Note

- Android devices by Samsung and Sony do not require this OEM-specific service application, as they include support for Assist out of the box. Zebra devices with Android 11 or later also support Workspace ONE Assist out of the box. This support means customers do not need to deploy the Zebra-specific service application APK file on their Zebra devices running Android 11 or later.
 - For Android Enterprise Enrolled BYOD Devices, see [How Do You Enable Remote Control for Android Enterprise Enrolled BYOD Devices](#).
 - For Android Enterprise Enrolled COPE Devices, see [How Do You Enable Remote Control for Android Enterprise Enrolled COPE Devices](#).
-

How Do You Enable Remote Control with Samsung Knox Service Plugin

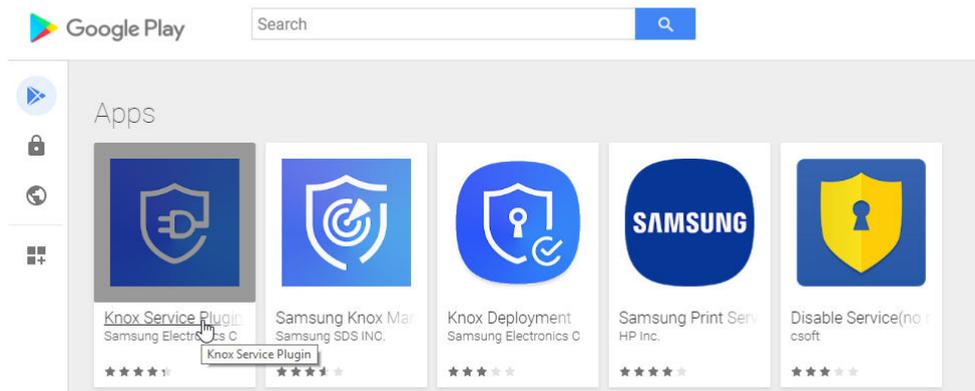
You can enable Samsung Knox devices to be remotely controlled with Workspace ONE Assist by installing the Knox Service Plugin.

The Samsung Knox Service Plugin is only available on Android 9.0 (Pie) and later. The only deployment modes supported are Profile Owner (PO) and Device Owner (DO). For detailed compatibility information, see [Which Profile/Ownerships Work with Samsung Knox](#).

With the introduction of Knox version 3.4.1, Samsung has enabled remote control on non premium Work Profiles by default. This is available on Samsung devices running Android 10.0 and later.

- 1 Log in to the Workspace ONE UEM Console.
- 2 Navigate to **Apps and Books > Applications > Native**, select the **Public** tab, and then select **Add Application**.
- 3 Select **Android** as the platform and enter "Knox Service Plugin" for the **Name** option.
- 4 Select the **Knox Service Plugin** from the list of

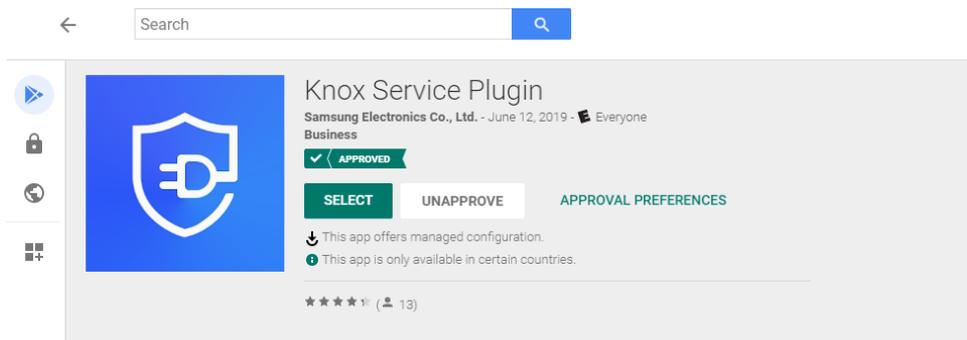
Add Application



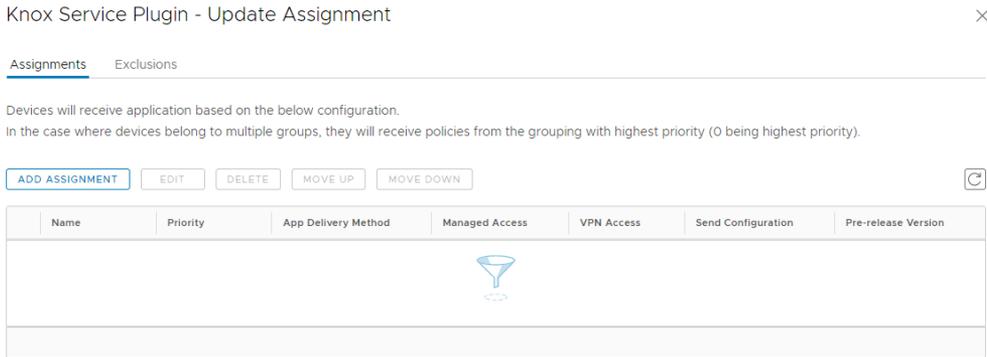
applications.

- 5 Click the **Select** button.

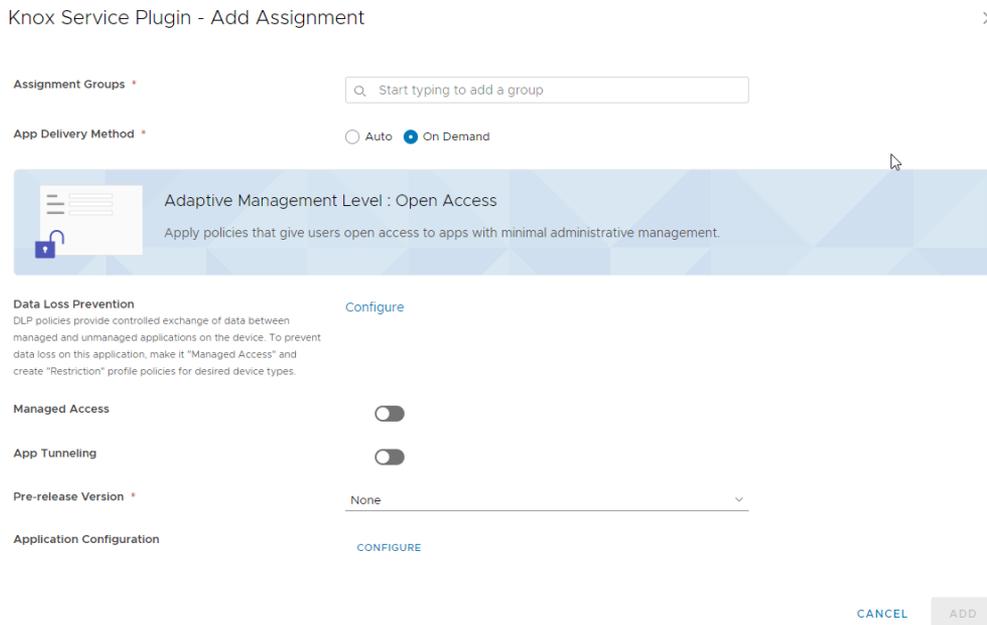
Add Application



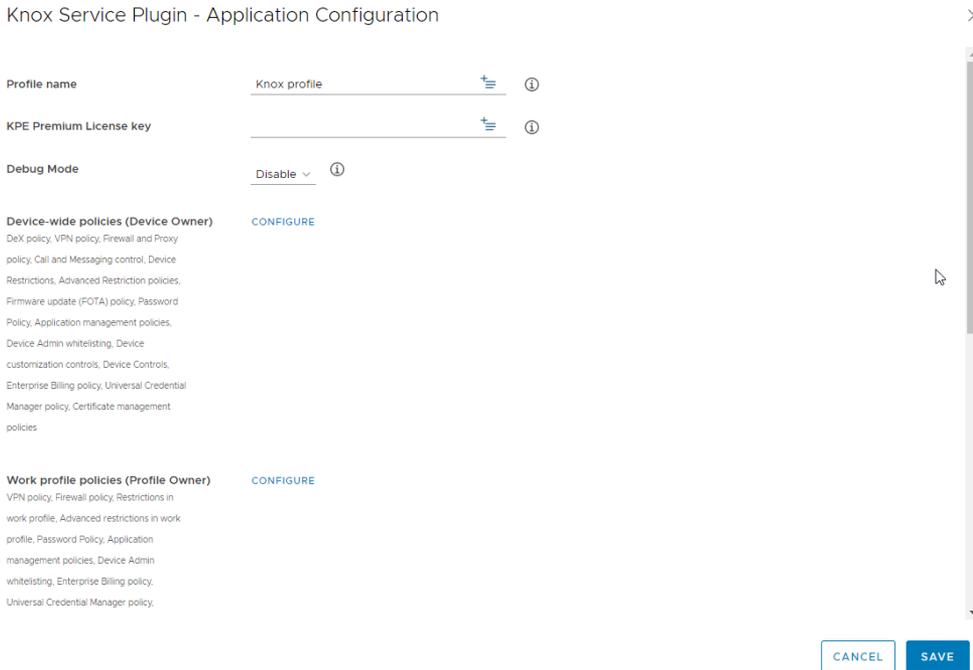
- 6 Add additional details as needed. Select **Save and Assign** to continue.
- 7 Select **Add Assignment**.



- 8 Select your applicable assignment Groups.
- 9 Select the desired application delivery method: **Auto** to automatically apply the application assignment and **On Demand** to allow the device user to opt-out of the app assignment.

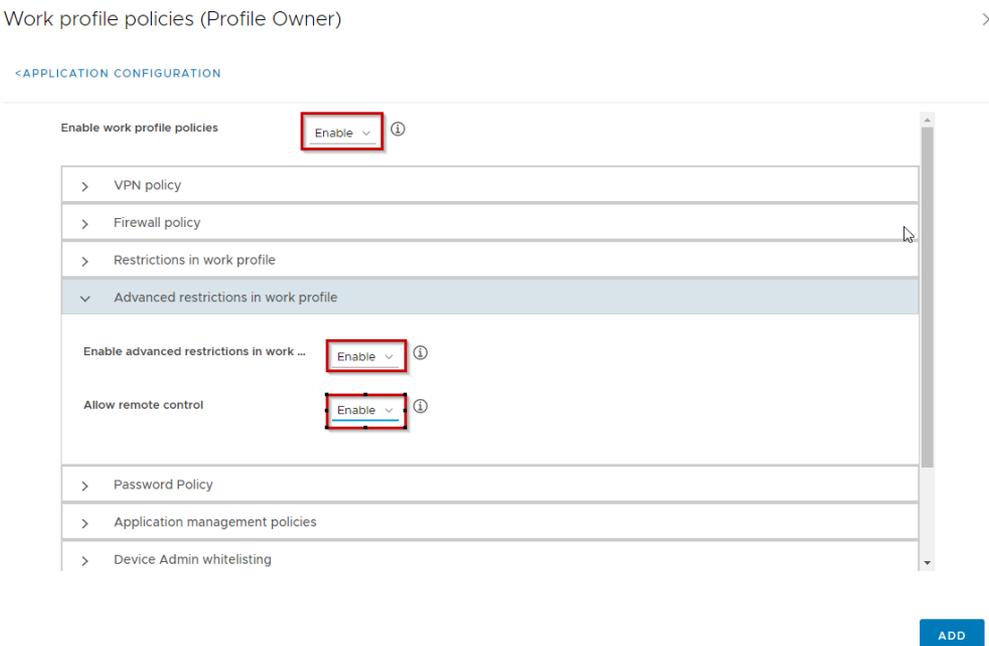


- 10 Select **CONFIGURE** next to **Application Configuration**.
- 11 Enter the KNOX Premium License Key.



The Knox premium license key is mandatory to enable remote control within the work profile on Android 9.x.

- 12 Select **CONFIGURE** next to Work profile policies (Profile Owner).
- 13 Select the **Enable** drop-down next to **Enable Work Profile Policies**. Then enable the two options under Advanced restrictions in work profile and Allow remote control. Then select the **ADD** button.



- 14 Select **Add** again to save the assignment.

- 15 Finally, select **Save and Publish** to publish the Knox Service Plugin with the configured policies.

Once the Knox Service Plugin is installed on the device and the policies are applied successfully, remote control is available within the work profile.

Samsung Knox devices can now be remotely controlled using Workspace ONE Assist.

Note On Samsung BYOD devices, only applications in the Work Profile can be viewed and controlled. If you navigate to the Work profile home screen or personal side of a Samsung BYOD device during a Workspace ONE Assist session, it only displays a blank screen.

How Do You Enable Remote View For iOS Devices

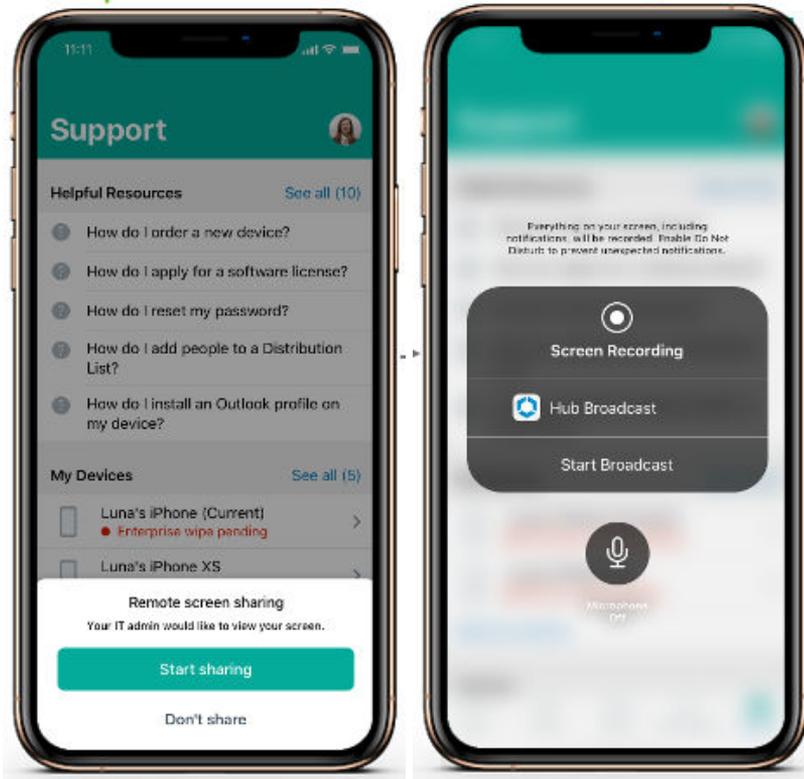
The steps for enabling the Remote View feature for your iOS devices vary based on the Intelligent Hub version installed on the devices. Follow the steps for the appropriate Intelligent Hub version on your device.

For devices with Intelligent Hub 20.11 or later

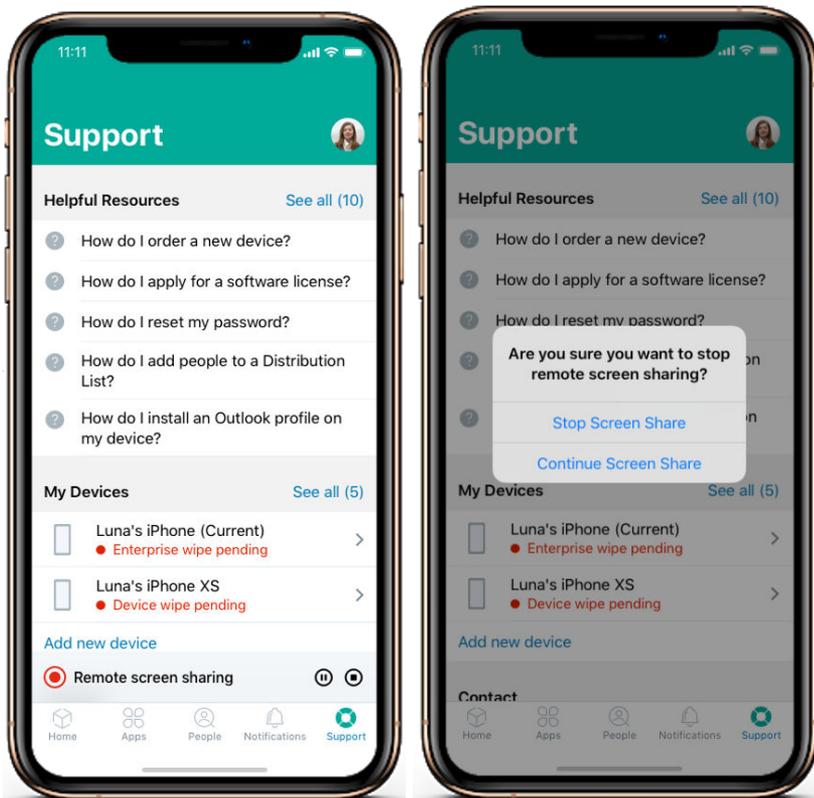
- 1 Ensure Workspace ONE Intelligent Hub 20.11 or later is installed.

Note The iOS version used must be 13 or later.

- 2 Request the iOS device user to open the Hub notification received or launch the Workspace ONE Intelligent Hub.
- 3 Select **Start Sharing** and then select **Start Broadcast**.



The end user can pause or disconnect the connection anytime during the remote view session.

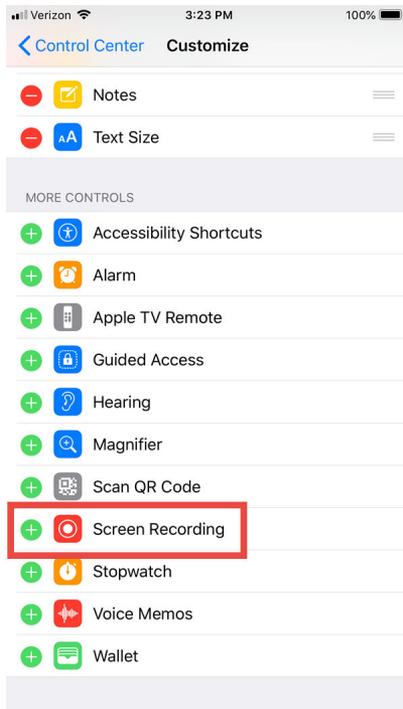


- 4 If the session is interrupted, the end user must start the screen broadcast from the Control Center using the following procedure:
 - a Open **Control Center** using the screen gesture appropriate for your iOS model.
 - b Press and hold down the **Screen Recording** icon ().
 - c Enable **Hub Broadcast**.
 - d Select **Start Broadcast**.



For devices with Intelligent Hub 20.11 or earlier

- 1 Ensure Workspace ONE Intelligent Hub 20.11 or earlier is installed.
- 2 Request the iOS device end user to perform the following one time setup.
 - a Navigate to **Settings > Control Center > Customize Controls** and add **Screen Recording** to the Control Center by selecting its green plus sign.



- 3 Request the iOS device end user to perform the following procedure before each Remote View session.
 - a Open **Control Center** using the screen gesture appropriate for your iOS model.
 - b Press and hold down the **Screen Recording** icon ()
 - c Enable **Hub Broadcast**.
 - d Select **Start Broadcast**.



This iOS device can now be remotely viewed using Workspace ONE Assist.

How Do You Enable Remote Control for Android Enterprise Enrolled BYOD Devices

You must enable your Android Enterprise enrolled BYOD devices to work with Workspace ONE Assist before they can be remotely controlled.

The Assist Agent and OEM-specific Assist Service package can be auto installed from Workspace ONE UEM or made available for the end user to install when needed.

The Workspace ONE Assist Agent is available at <https://my.workspaceone.com/products>.

- On BYOD Enrolled devices, the Assist agent always behaves as an Attended agent. Even if the Unattended agent is pushed to the device, the Assist agent continues to behave as an Attended agent due to the presence of the Work Profile.

CHOOSE ONE PATH ONLY

YOU MUST SELECT BETWEEN TWO CHOICES.

YOU CAN EITHER PUSH CONTENT USING UEM **OR** LEAVE IT TO THE END USER. **Do not perform both.**

PUSH CONTENT USING UEM	LEAVE IT TO THE END USER
<ol style="list-style-type: none"> 1 From the Workspace ONE UEM console, use Apps and Books or Product Provisioning to add the Workspace ONE Assist agent as a managed PlayStore application. For more information, see Mobile Application Management. 2 From the Workspace ONE UEM console, use Apps and Books or Product Provisioning to add the OEM-specific Assist Service as a managed PlayStore application. This step is required to enable remote control on all supported OEMs except Samsung and Sony. For more information, see Product Provisioning. 3 Create a smart group that includes these Android Enterprise enrolled BYOD devices. 4 Assign the agent and OEM-specific Assist Service to the smart group you created and automatically push the application to all managed devices in the smart group. For more information, see Smart Groups. 5 Proceed directly to the What to do next section. 	<ol style="list-style-type: none"> 1 Make the Workspace ONE Assist agent and OEM-specific service application available as Public applications through the Play Store. 2 Direct your Android BYOD end users to navigate to the Work Profile. 3 The end user must open the Play Store from within the Work Profile. 4 End user must download and install the Workspace ONE Assist Agent. 5 If applicable, the end user must download and install the OEM-specific service application. This step is required to enable remote control on all supported OEMs except Samsung and Sony. 6 Proceed directly to the What to do next section.

Note On Samsung BYOD devices, only applications in the Work Profile can be viewed and controlled. If you navigate to the Work profile home screen or personal side of a Samsung BYOD device during a Workspace ONE Assist session, it only displays a blank screen.

Note On Samsung BYOD devices, remote control is disabled by default within All Work Profiles under Android 9.0 (with Knox versions earlier than 3.4.1) and Premium Work Profiles under Android 10.0 or later (with Knox 3.4.1 or later). You can enable remote control on these work profiles by installing the KNOX Service Plug-in together with the appropriate OEM Config policy. For more information, see [How Do You Enable Remote Control with Samsung Knox Service Plugin](#) and [Full Remote Control Support by Original Equipment Manufacturer \(OEM\) and Model, Android](#).

With the introduction of Knox version 3.4.1, Samsung has enabled remote control on non premium Work Profiles by default. This is available on Samsung devices under Android 10.0 and later.

A Knox Premium License is necessary to enable remote control on Work Profiles with Knox versions earlier than 3.4.1.

How Do You Enable Remote Control for Android Enterprise Enrolled COPE Devices

You must enable your Android Enterprise enrolled COPE (Corporate-Owned, Personally-Enabled) devices to work with Workspace ONE Assist before they can be remotely controlled.

- On COPE Enrolled devices, the Assist agent always behaves as an Attended agent. Even if the Unattended agent is pushed to the device, the Assist agent continues to behave as an Attended agent due to the presence of the Work Profile.

- Devices running under Android 8 (Oreo), 9 (Pie), and 10, the Workspace ONE Assist application operates on the personal side of the device to provide remote control functionality to the entire device. As a result, the Workspace ONE Assist app must be installed as an internal application.
- On devices running Android 11, the Workspace ONE Assist app can no longer run on the personal side of a COPE device. The Assist application can operate only within the Work profile on COPE devices. As a result, once a device is upgraded to Android 11, the Assist application must be uninstalled from the personal side and reinstalled on the Work profile as a managed Play Store application.

The Workspace ONE Assist Agent is available at <https://my.workspaceone.com/products>.

- 1 From the Workspace ONE UEM console, use **Apps and Books** or **Product Provisioning** to add the Workspace ONE Assist agent.
 - Android 8, 9, and 10 devices must add the Workspace ONE Assist agent as a managed internal application.
 - Android 11 devices must add the Workspace ONE Assist agent as a managed PlayStore application.

For more information, see *Mobile Application Management* documentation.
- 2 From the Workspace ONE UEM console, use **Apps and Books** or **Product Provisioning** to add the OEM-specific Assist Service. This step is required to enable remote control on all supported OEMs except Samsung and Sony.
 - Android 8, 9, and 10 devices must add the OEM-specific Assist Service as a managed internal application.
 - Android 11 devices must add the OEM-specific Assist Service as a managed PlayStore application.

For more information, see [Product Provisioning](#).
- 3 Create a smart group that includes these Android Enterprise enrolled COPE devices.
- 4 Assign the agent and OEM-specific Assist Service to the smart group you created and push it to managed devices. For more information, see [Smart Groups](#).
- 5 Direct the device End User to uninstall the Workspace ONE Assist application if it was previously installed on the personal side of the device in Android 8, 9, or 10.
 - For Android 8, 9, and 10 devices, the end user must uninstall Workspace ONE Assist from the **personal side** of the device.
 - For Android 11 devices, the end user must uninstall Workspace ONE Assist from the **work profile** on the device.

On Samsung COPE devices, the Personal profile and Work profile can be remote controlled.

Note On Samsung COPE devices, remote control is disabled by default within All Work Profiles under Android 9.0 (with Knox versions earlier than 3.4.1) and Premium Work Profiles under Android 10.0 or later (with Knox 3.4.1 or later). You can enable remote control on these work profiles by installing the KNOX Service Plug-in together with the appropriate OEM Config policy. For more information, see [How Do You Enable Remote Control with Samsung Knox Service Plugin](#) and [Full Remote Control Support by Original Equipment Manufacturer \(OEM\) and Model, Android](#).

With the introduction of Knox version 3.4.1, Samsung has enabled remote control on non premium Work Profiles by default. This is available on Samsung devices under Android 10.0 and later.

A Knox Premium License is necessary to enable remote control on Work Profiles with Knox versions earlier than 3.4.1.

Start an Assist Session



Initiate a Workspace ONE Assist session, and depending on the platform, you can view the host device screen, manage the host's files, make changes to the host's registry, and access the Remote Shell.

- 1 Navigate to **Devices > List View** and select the **Friendly Name** of a device capable of being remotely managed.

The Details View for the selected device displays.

Note Windows 10 devices now support unattended mode access. For more information, see [Agent Modes](#).

- 2 Select the **Remote Assist** button and then select a tool from among the presented options. The options are Screen Share, File Manager, and Remote Shell.

The Remote Support screen displays and it commences with reviewing device registration, queuing remote management command, and creating the remote management session.

A confirmation PIN displays on the screen intended for the end-user of the host device.

- 3 Relay this PIN information to the end-user and ask them to enter the PIN on their device to authorize the session.
 - If they enter the PIN, they consent to the remote session and the session begins.
 - If they refuse to enter the PIN, they do not consent and the session ends.

Note On Samsung BYOD devices, only applications in the Work Profile can be viewed and controlled. If you navigate to the Work profile home screen or personal side of a Samsung BYOD device during a Workspace ONE Assist session, it only displays a blank screen.

Privacy Notices and End-User Prompts

Workspace ONE Assist provides end users visibility and transparency during remote control sessions by displaying privacy notices, on screen prompts, notifications, and an on screen toolbar giving the end user power over the remote session.

Privacy Notices

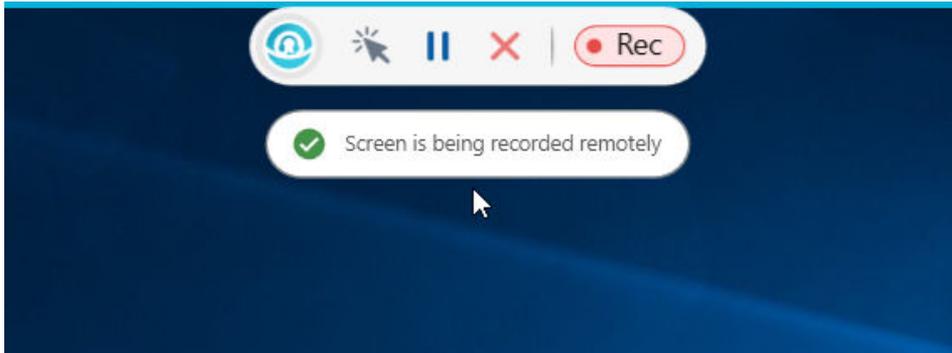
When the end user launches Workspace ONE Assist for the first time, whether in Attended or Unattended mode, they see a Privacy Notice that informs them of the data accessed by the Assist application. Attended sessions always present the end user with a PIN prompt. However, if the application is launched for the first time through a connection process, the privacy notice is displayed only on the Attended mode agent. The Unattended mode agent does not display a privacy notice during the connection process.

PIN Prompt at the Beginning of a Session

When you start a session in Workspace ONE Assist, a four-digit PIN displays as a pop-up message to you, the admin. You must provide this PIN to the host device end user so they can enter it into the PIN prompt on their device. Communicate this PIN by telephone, text message, or email. This exchange represents the host device end user's acknowledgment of the privacy notice. The end-user grants access (by entering the PIN you provide) or denies access (by not entering the PIN you provide).

The Halo

When you use any client tool (Remote View, Remote Control, File Manager, or Remote Shell), a blue outline is drawn around the outer edge of the host device end user's screen called a "halo". This halo serves as a persistent notification that a Workspace ONE Assist session is active.



There is a toolbar that appears with the halo. This toolbar gives the host device end user the power to pause a session, revoke remote control privileges demoting the session back to Remote View only, and the power to disconnect the session entirely. The toolbar also indicates when the screen is being recorded.

Note The halo effect, and other notifications, are disabled on corporate owned, fully managed Android devices using the Unattended Agent ONLY.

Permission Prompts

When you start any other client tool during a Screen Share session, the end user is again asked permission for access.

For example, an end user enters the PIN provided by the Admin resulting from initiating a Screen Share session. This action grants the Admin view only access to the end user's Windows 10 device to troubleshoot a problem. During this Screen Share session, the Admin starts the Manage Files client tool. Before the Admin gets to see and manage the end user's files remotely, the end user of the host device must select **Deny** or **Allow** from the Manage Files prompt that appears. The Screen Share session is not impacted by either choice. However, the Manage Files session cannot proceed until after the end-user grants access.

Android 11 and Manage Files Client Tool

Beginning with Android 11, Google is enforcing scoped storage on all applications targeting API level 30. The enforcement of scoped storage means an app is limited to only accessing its own file sandbox and specific types of media files that the app has created.

To provide access to other file locations on the device, VMware has partnered with many of the top Android device manufacturers to create a newer version of the OEM-specific service application (v2.5). Download and install the latest version of the Assist service application to access all files on the remote device.

On devices where an OEM-specific service application is not available (for example, Samsung and Sony devices) the end user on the remote device must explicitly grant additional permissions to the application when requested. Workspace ONE Assist prompts the Android 11 device end user to 'Allow access to manage all files'. This permission must be granted to the Assist application one-time at the beginning of the first Manage Files session.

- In Attended mode, this permission must be granted or denied by the end user of the device.
- In Unattended mode, you must grant this permission through the Share Screen client tool.

Once permission is granted, all files on the remote device can be accessed during the Manage Files session. In the absence of this permission, you can only access Media and Downloads folder.

Agent Modes

The PIN prompt and User Consent prompts are displayed only during an Attended mode of connection. When using Workspace ONE Assist in Unattended mode, no device notifications are provided when a remote management session is active. You are solely responsible for notifying device end users of Assist sessions in unattended mode.

Note

- On Samsung devices, the end user must accept a Knox permission when the application is first launched, even for devices in Unattended mode.
- An additional prompt requesting the accessibility permission in the Attended mode also displays on the Samsung devices. This permission ensures that the device screen is dimmed, blocking the admin's view when the user enters a password in the foreground.

For more information, see [Agent Modes](#).

Notifications Sent Per Video Recording and Screenshot

For Android, macOS, and Windows 10 devices only, the first time you initiate a video recording or request a screenshot in a session, the host device end user is prompted to grant permission. After the end-user grants permission, each subsequent video recording or screenshot made in the same session results in a "pop-up" on-screen notification instead of a permission request.

These notifications, together with the PIN prompts and the other permissions, are designed to foster transparency during any Workspace ONE Assist session.

For more information about VMware's stance on privacy, see the [VMware Privacy Notice](#).

Session Collaboration Notifications and Prompts

Device end users receive a popup notification for each participant that joins the active session collaboration. The only exception is for Android devices in Unattended mode.

Main Menu Toolbar

The Workspace ONE Assist client provides support tools to facilitate troubleshooting and remotely controlling end-user devices. Not all client tools are available for all platforms. You can also assign tool-specific role permissions to your admins from the Workspace ONE UEM console

The main menu toolbar appears in the top-center of the Workspace ONE Assist client screen, giving you direct access to multiple features and functions.



 – The Home button gives you access to all the client tools including Manage Files, Remote Shell, Registry Editor, and Share Screen.

 – The Info button displays the session logs, the VMware Privacy Policy, and the version number of Workspace ONE Assist.

 – The Screen Share button indicates when an active Screen Share session is running.

 – The Fit to Screen button stretches or shrinks the remote device skin in a way that makes it fully visible given the current size of the Assist window.

 – The Multi-Monitor button appears when your host machine has more than one monitor attached. It allows you to select which monitor you want to view or control. Only one monitor may be viewed or controlled at any given time.

 – The Virtual Keyboard button starts the on-screen keyboard. You can find details about the virtual keyboard in its own section of this topic.

 – The Record button initiates a video recording of the remote session. For more information, see [Capture Video and Images](#).

 – The Screenshot button takes a static screenshot of the remote session. For more information, see [Capture Video and Images](#).

 – The Remote View button indicates that a Remote View is in session and selecting it lets you request a session elevation (to Control Screen) from the host device end-user.

 – The Control Screen button indicates that a Control Screen session is running and you can select it to demote your session to Remote View.

 – The Manage Files button gives you access to storage space on the host device. For more information, see [Manage Files](#).

 – The Add Folder button lets you add a new storage folder on the host device.

 – The Refresh button refreshes folder views and their contents. This can be useful when you work with session collaborators who contribute files to host storage.

 – The Session Collaborate button lets you invite other participants into your active Share Screen and Remote View session. Getting extra help can be useful to troubleshoot advanced issues. Select this button to invite Guests to your active session. For more information, see [Session Collaboration](#).

 – The Chat button lets you exchange text messages, including private messages, between all the participants of an Assist session: the remote user host, the Assist console user who initiated the session, and all session collaborators. See below for details.

 – The Ellipsis button contains access to **Shortcuts** and the **System Summary**. You can find details about each of these screens in their own sections of this topic.

 – The Fullscreen button maximizes the Assist window in such a way that it fills the display at its current maximum resolution.

 – The End Session button stops the currently running session.

Virtual Keyboard

The virtual keyboard is used to send platform-specific key commands, language-specific keys, and other special keystrokes to the remote device.

For example, if your remote management device is an Apple Mac, you must use the virtual keyboard to send a Windows key keystroke to the Windows 10 remote device.

If you remote into a device that is configured in a different language than your remote management device, you must use the virtual keyboard to access those special keys.

Lastly, the virtual keyboard lets you send special keystrokes to the remote device, ensuring they are not confused with keystrokes for your own device, for example Ctrl-Alt-Del.

Copy & Paste with Virtual Keyboard

The virtual keyboard is the method by which you can copy a string of text from your remote management device, and paste it onto the remote device.

Initiate copy & paste during a Share Screen session by taking the following steps.

- 1 On the remote management device, select a text string from your application of choice.
- 2 Copy it to the clipboard by hitting Ctrl-C on your keyboard.
- 3 Switch to the Share Screen session and open the virtual keyboard.
- 4 Click anywhere in the grey colored area that runs across the top of the virtual keyboard, to the right of the Auto Send switch.
- 5 Paste it onto the virtual keyboard by hitting Ctrl-V on your keyboard.
- 6 Ready the application on the host device to receive the text string. Do this by placing the pointer on the spot you want the text string to be pasted.
- 7 Switch back to the virtual keyboard and select the green send button to the far-right of the virtual keyboard to paste it onto the application you made ready above.

Chat

You can exchange text messages to and from the device end user and session collaborators no matter what client tool you use. You can also send private messages to individual session participants. Chat is available during Assist sessions on Android, macOS, and Windows 10 devices.

- Initiate a chat session by selecting the Chat icon  from the main menu toolbar of the Assist Console.
- End users access the Chat tab from the Assist application installed on their devices in both Attended and Unattended modes.
 - Only devices connected by Attended mode receive notifications about chat messages.
- The Chat feature is available while using any Assist Client Tool including Manage Files, Remote Shell, and so on.
- To send a private chat message, select an individual participant from the **To:** drop down menu.
- You can get the device end user's attention of an incoming chat message by selecting the Chat Bullhorn button . This button directs the connected device to emit an audible signal, which can be useful for when the end user is in a noisy environment.

Shortcuts

The shortcuts menu grants access to common administrator tools and useful functions. You can pin the shortcut menu to the screen, giving you immediate access to these functions without having to select the  button from the toolbar.

- Command Prompt

- Control Panel
- Ctrl-Alt-Del
- Event Viewer
- Lock Screen
- Log Out of device (including confirmation prompt for end user)
- Network and Sharing screen
- Registry Editor
- Restart PC
- Services
- Show Desktop
- Task Manager

System Summary

The System Summary contains information similar to Device Details in Workspace ONE UEM. Use this information to diagnose issues on a device while connected. There are five subsections within System Summary.

- The **Device Information** pane provides at-a-glance information about the remote device during troubleshooting. The pane displays signal strength, battery, network status, storage, and main memory information.
- The **Application List** subsection displays all the installed applications on the device.
- The **Process List** subsection displays all processes running on the device and includes the option to kill or stop only those processes that can be killed.
- The **Service Book** subsection displays all services running on the device.
- The **Share Screen** subsection displays a historical log of all prior remote sessions.

All the content in each subsection can be searched using the **Search list below** feature, located in the upper-right corner of the **System Summary** screen.

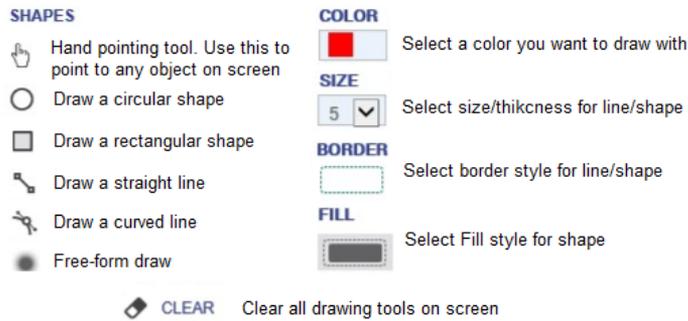
You can also select the **Export** button (to the right of the search function) to export each subsection to an Excel-viewable file saved to your device for detailed analysis.

Device Whiteboard

The device whiteboard functionality allows you to highlight a specific item to the user. The whiteboard allows you to draw, highlight, and point to areas on the screen.

To use the whiteboard, select the whiteboard icon () in the bottom right of the device screen view.

The whiteboard menu consists of the following items.



This feature is supported by Android, macOS, and Windows 10 devices.

Be sure that the Android devices in your fleet are configured to use the Whiteboarding feature. For more information, see [Configure Android Devices for Whiteboarding Feature](#).

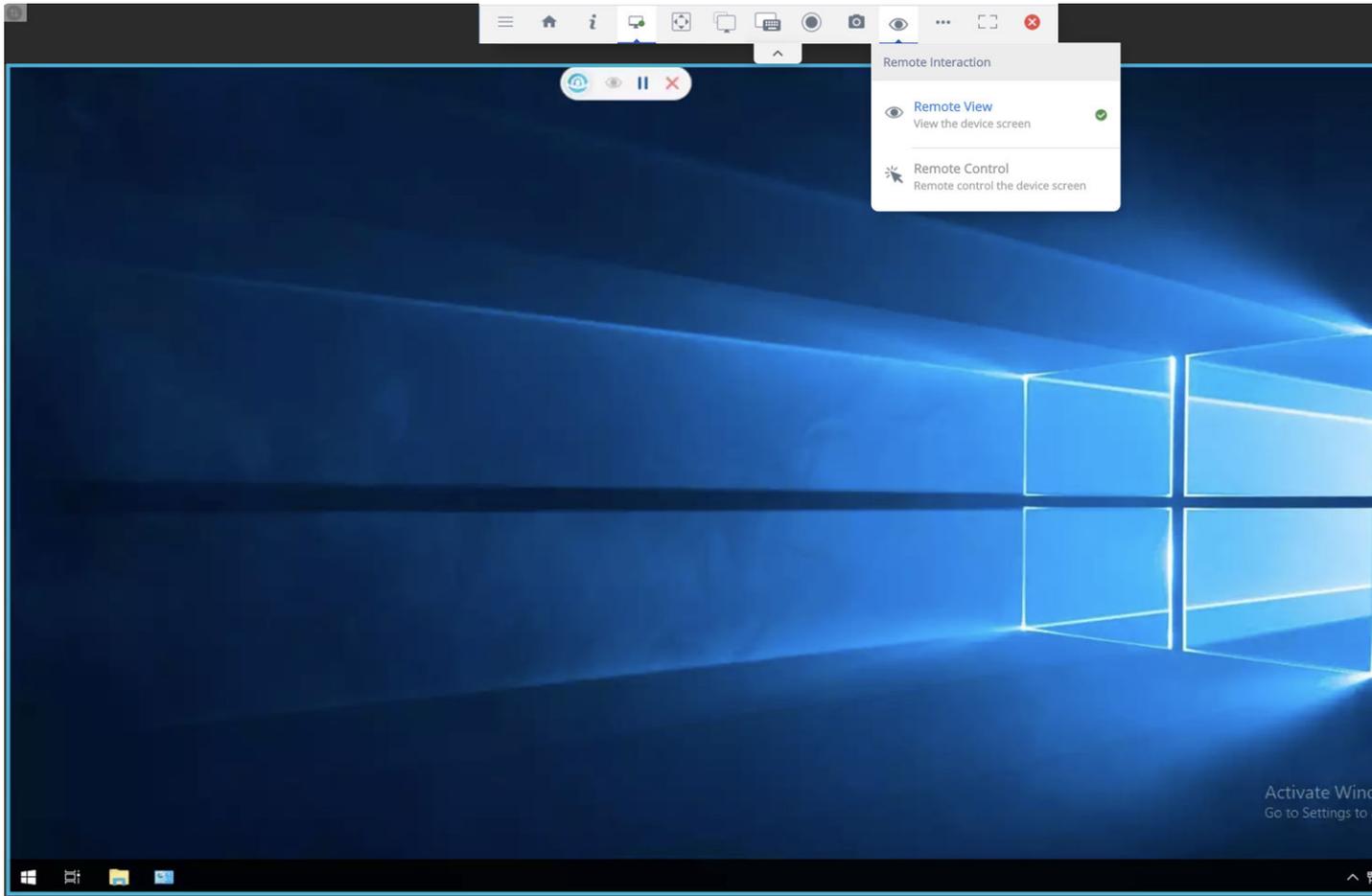
Share Screen

The Share Screen tool is the section of the Workspace ONE Assist which allows you to control the end-user device remotely for troubleshooting and research purposes.

This functionality requires the **Remote Control** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

For more information about the main menu toolbar, see [Main Menu Toolbar](#).

Figure 8-1. Share Screen Session



Note With regard to the permission prompts for the Remote View and Remote Control functions on macOS devices, be aware of the following.

- macOS devices running version 10.13 (High Sierra) and 10.14 (Mojave) allow the **Share Screen** feature by default. No additional permissions are required to share the screen, therefore, no prompt is displayed at the beginning of a **Share Screen** session.
- For macOS devices running version 10.15 (Catalina), the **Share Screen** and **Remote View** features both require that you enable the **Screen Recording** permission to Workspace ONE Assist in the **Privacy** tab of **Security & Privacy** preferences, located in System Preferences. Only during the first time you initiate a **Share Screen** session with a qualifying macOS device, an access request popup displays including a convenience link to this privacy setting in System Preferences.
- Similarly, macOS devices running version 11 (Big Sur) or later must enable **Screen Recording** permission to Workspace ONE Assist for both **Remote View** and **Share Screen** features. This permission is configured in a slightly different way for version 11:

Enable Screen Recording by navigating to **System Preferences > Security & Privacy > Privacy tab > Screen Recording** then select the **Lock** icon to unlock the Privacy settings and enter the **Administrator password**. This is a one-time activation by the end user.

End-User Can Pause Share Screen Session

During a long share screen session, an end user might need to perform some activity that requires privacy, for instance, answering an email.

If an end user needs privacy, they can pause a remote control session by clicking the blue Pause button () located in the **Assist** window, which places the share screen session in a "hold" state. The end user can unpaused the session by clicking the blue button again.

Capture Video and Images

You can capture video of your Workspace ONE Assist remote session and save it as a file to your download folder. You can do the same with still images (screenshots).

For Android, macOS, and Windows 10 devices only, the first time you initiate a video recording or request a screenshot in a session, the host device end user is prompted to grant permission. After the end-user grants permission, each subsequent video recording or screenshot made in the same session results in a "pop-up" on-screen notification instead of a permission request.

Devices in Unattended mode receive no permission requests and no notifications.

- 1 Invoke the drop-down toolbar by selecting the down arrow at the top-center of your remote session window.
- 2 Select the icon of the action you want to perform.
 - For **video capture**, select the round 'Record' icon () . Stop recording the session to video by clicking the same button.

- For an **image capture** (screenshot) of the session, select the 'Camera' icon ()
- 3 Once completed, your captures can be found in the default downloads folder of your browser.
- **Video captures** are saved as .WEBM files.
 - **Image captures** are saved as PNG files.

Configure Android Devices for Whiteboarding Feature

You can configure Android devices to use the Whiteboarding feature in Workspace ONE Assist's Share Screen client tool. The Whiteboarding feature enables you to draw freehand on the host's screen and be viewed by the host user, which you can use to call the host user's attention to certain screen elements.

Before you begin:

- Confirm whether an OEM-specific service APK is available for your Android device and install it.
- Android devices with an OEM-specific service APK installed are preconfigured to use the Whiteboarding feature and require no other setting.
- Android devices made by Samsung, Sony, and any other OEM without a specific service APK installed must take the following steps to use the Whiteboarding feature.

1 Include a customization to the device profile that allows the system UI overlays.

- a In Workspace ONE UEM, navigate to **Devices > Profiles & Resources > Profiles**.

Choose From:

- **Existing Profile** - If you want to include this customization to an existing device profile, then find the profile you want to modify in the listing. Then select the edit icon () next to the profile name in the **Profile Details** column. Before you can make changes to an existing profile, you must select the **Add Version** button.
 - **New Profile** - If you want to include this customization to a new device profile, then select **Add** followed by **Add Profile**, select the **Android** platform, and make all your other device profile specifications. The **Android Legacy** platform does not support enabling system UI overlays. For details, see *Device Profiles* in the *Managing Devices* documentation and *Android Device Management* and *Android (Legacy) Platform* documentation, each available on docs.vmware.com.
- b Select the **Restrictions** payload and if necessary, select the **Configure** button. The **Restrictions** payload screen displays.
- c In the **Device Functionality** section, scroll down to **Allow System UI (Toasts, Activities, Alerts, Errors, Overlays)** and enable this option by adding a check mark to its check box.
- d Select **Save and Publish**. The device profile (including the customization to allow system UI overlays) is saved and pushed to all applicable devices.
- 2 On the Android device, navigate to Settings.

- 3 Navigate to App Settings.
- 4 Open the Assist app settings.
- 5 Locate the Advanced section.
- 6 Enable permission to Draw over other Apps.

The Whiteboarding feature can now be used by this Android device lacking an OEM-specific service APK.

Remote View

The Remote View client tool in Workspace ONE Assist allows you to only view a host device screen remotely. You can elevate to a full remote control session if you have the proper permissions from the assigned role as well as from the device end user.

This functionality requires the **Remote View** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

Think of the **Remote View** client tool as the "read only" component of Workspace ONE Assist. The virtual keyboard feature is unavailable. You can see what the host device end user sees but you cannot intervene unless you elevate the Remote View session to a fully remote controlled Share Screen session.

If you have an admin role with the **Remote Control** permission, you can initiate this elevation by selecting the **Remote View** button from the toolbar () and then selecting the **Control Screen** option (). Doing so notifies the device end user that remote control is being requested. For more information, see [Privacy Notices and End-User Prompts](#).

Manage Files

You can use the Manage Files client tool in Workspace ONE Assist to upload files, download files, download folders, rename files, and delete files on the device.

This functionality requires the **File Manager** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

Beginning with Android 11, Google is enforcing scoped storage on all applications targeting API level 30. The enforcement of scoped storage means an app is limited to only accessing its own file sandbox and specific types of media files that the app has created.

To provide access to other file locations on the device, VMware has partnered with many of the top Android device manufacturers to create a newer version of the OEM-specific service application (v2.5). Download and install the latest version of the Assist service application to access all files on the remote device.

On devices where an OEM-specific service application is not available (for example, Samsung and Sony devices) the end user on the remote device must explicitly grant additional permissions to the application when requested. Workspace ONE Assist prompts the Android 11 device end user to 'Allow access to manage all files'. This permission must be granted to the Assist application one-time at the beginning of the first Manage Files session.

- In Attended mode, this permission must be granted or denied by the end user of the device.
- In Unattended mode, you must grant this permission through the Share Screen client tool.

Once permission is granted, all files on the remote device can be accessed during the Manage Files session. In the absence of this permission, you can only access Media and Downloads folder.

Upload a File

You can upload a file to the device you are managing remotely.

- 1 In the active Workspace ONE Assist session and the Manage Files client tool activated, select the red, circular **Upload** button in the bottom-right corner of the screen.
- 2 Select the **Browse** button and select a file accessible to the Workspace ONE™ UEM console you want to add to the device's file system.
- 3 Select **Close** on the File Upload Completed confirmation.

Download a File

You can download a file from the device with the Manage Files client tool.

- 1 In the active Workspace ONE Assist session and the Manage Files client tool activated, locate the file on the device you want to download.

You can find the "breadcrumbs" style folder path at the top of the file listing a useful navigation aid.

- 2 Select the **Download** button (📄).

Downloaded files are saved according to your default browser's downloaded file action.

Rename a File

You can rename a file on the remote device using the Manage Files client tool.

- 1 In the active Workspace ONE Assist session and the Manage Files client tool activated, locate the file on the device you want to rename.

- 2 Select the **Rename** button.

This button is located in the button cluster to the left of the **Size** column.

The **Rename** screen displays where you can enter the new name for the file.

- 3 Select **OK** to save your changes.

Select Multiple Files

You can select multiple files on the remote device using the Manage Files client tool. Multi-selecting files can be useful if you want to cut, copy (followed by paste), or delete them.

- 1 In the active Workspace ONE Assist session and the Manage Files Client tool activated, locate the files you want to select.
- 2 Click the check box to the left of each file you want to select.

Download a Folder

You can download an entire folder from the remote device including the folder's contents.

- 1 In the active Workspace ONE Assist session and the Manage Files client tool activated, locate the folder on the device you want to download.

You might find the "breadcrumbs" style folder path at the top of the file listing a useful navigation aid.

- 2 Select the **Download** button (📄).

The downloaded folder and all its content is saved according to your default browser's download action.

For example, if you select a folder to download called "remoteDocs" and your default browser's download action is to save all downloads to "C:\Documents\downloads", then once the download successfully completes, you can expect to find the folder's content in C:\Documents\downloads\remoteDocs.

Cut, Copy, and Paste a File

You can cut, copy, and paste files on the remote device using the Manage Files client tool in Workspace ONE Assist.

- 1 Once you have selected the files you want, select the **Cut** button (✂) or **Copy** button (📄).

Cutting files removes the files from the source location while copying files leaves the files in the source location.

- 2 Navigate to the target location on the device.
- 3 Select the **Paste** button, which only becomes visible when either the Cut or Copy buttons have been selected.

Delete a File

You can also delete a file from the remote device.

- 1 In the active Workspace ONE Assist session and the Manage Files client tool activated, locate the file on the device you want to delete.
- 2 Select the **Delete** button (🗑).
- 3 Select **OK** to confirm file deletion.

Close the Manage File Session

When you are finished managing files remotely, you can close the Manage Files session while keeping the Display Capture session running.

- 1 In the active Workspace ONE Assist session, locate the header bar toward the top of the browser.



- 2 Select the circled **X** button to the right of the Manage Files indicator.
- 3 Select **OK** to confirm closure of the Manage Files session.

Remote Shell

Workspace ONE Assist's Remote Shell client tool, you can remote into the PowerShell interface of connected Windows 10 and macOS devices, enabling you to make detailed and precise configurations in a command-line environment.

Microsoft's PowerShell interface combines automation with a sophisticated scripting language with a configuration management framework. For more information about PowerShell, see <https://docs.microsoft.com/en-us/powershell/>.

This functionality requires the **Remote Shell** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

Command-Line Interface, Android

The Command-Line Interface (CLI), available for Android devices and supported in Workspace ONE Assist, is the counterpoint to the Graphical User Interface (GUI). While a graphical user interface makes common tasks easy, a command-line interface makes complicated tasks possible.

This functionality requires the **Remote Shell** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

CLI Commands	Support Level	Function
<code>am get-config</code>	Full	Gather configuration data from a device.
<code>cd</code>	Full	Change directory.
<code>getprop</code>	Full	Get properties by way of the android property service.
<code>getprop ro.build.version.sdk</code>	Full	Get API level device properties.
<code>ip -f inet addr show wlan0</code>	Full	Show the WiFi IP address.
<code>logcat</code>	Full	Prints log data to the screen.
<code>logcat *:D</code>	Partial	Prints log data to the screen, filter to show only the debug level. In a few devices, this command cannot be canceled.

CLI Commands	Support Level	Function
<code>logcat *:E</code>	Partial	Prints log data to the screen, filter to show only the error level. In a few devices, this command cannot be canceled.
<code>logcat *:I</code>	Partial	Prints log data to the screen, filter to show only the info level. In a few devices, this command cannot be canceled.
<code>logcat *:V</code>	Partial	Prints log data to the screen, filter to show only the verbose level. In a few devices, this command cannot be canceled.
<code>logcat *:W</code>	Partial	Prints log data to the screen, filter to show only the warning level. In a few devices, this command cannot be canceled.
<code>ls</code>	Full	List the directory contents.
<code>ls -a</code>	Full	List the directory contents, do not hide entries starting with a dot.
<code>ls -n</code>	Full	List the directory contents, list numeric UIDs, and GIDs.
<code>ls -R</code>	Full	List the directory contents, list subdirectories recursively.
<code>ls -s</code>	Full	List the directory contents, print size of each file, in blocks.
<code>mkdir</code>	Full	Make a directory.
<code>netcfg / ifconfig</code>	Full	Configure and manage network connections by way of profiles.
<code>netstat</code>	Full	Network statistics.
<code>ping</code>	Partial	Test the connection and latency between two network connection. In few devices, this command cannot be canceled.
<code>pm list packages</code>	Full	Prints all packages, optionally only those package names included in <FILTER>.
<code>pm list packages -3</code>	Full	Prints all packages filtered to show only the third-party packages.
<code>pm list packages -d</code>	Full	Prints all packages filtered to show only the disabled packages.
<code>pm list packages -e</code>	Full	Prints all packages filtered to show only the enabled packages.
<code>pm list packages -f</code>	Full	Prints all packages including their associated file.
<code>pm list packages -i</code>	Full	See the installer for the packages.
<code>pm list packages -s</code>	Full	Prints all packages filtered to show only the system packages.
<code>pm list packages -u</code>	Full	Prints all packages including uninstalled packages.
<code>pm list permission-groups</code>	Full	Lists all permissions groups.
<code>pm list permissions</code>	Full	Lists all permissions on the device.
<code>pm path <package ></code>	Full	Print the path to the APK of the given <package>.
<code>ps</code>	Full	Print process status.
<code>ps -p</code>	Full	Print process status and show scheduling policy.

CLI Commands	Support Level	Function
<code>pwd</code>	Full	Print the current working directory location.
<code>rm -d</code>	Full	Remove a directory, even if it is not empty.
<code>rm -f</code>	Full	Remove a directory, force remove without prompt.
<code>rm -r</code>	Full	Remove the contents of the directory recursively.
<code>top</code>	Partial	Display top CPU processes. In a few devices, this command cannot be canceled.
<code>touch</code>	Full	Create an empty file or change file timestamps.

Registry Editor

You can edit the registry of Windows CE devices remotely using the Workspace ONE Assist client tool.

Much like the Registry Editor that includes Windows desktop PCs, the Workspace ONE Assist client tool includes a Registry Editor for Windows CE devices. Using this editor, you can add, rename, and delete registry keys and values on the Windows CE devices in your fleet.

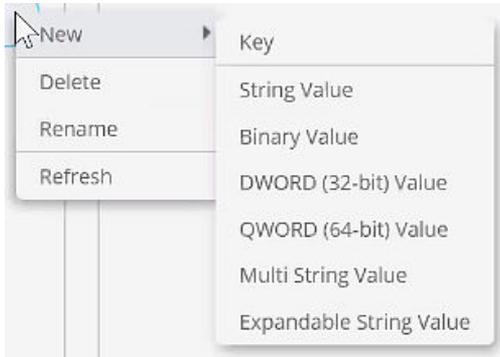
This functionality requires the **Registry Editor** permission to be part of your assigned administrator roles. For more information, see [Role-Based Access to Workspace ONE Assist](#).

Before you begin any of the following registry procedures, you must start a remote management session. For details, see [Chapter 8 Start an Assist Session](#) and select **Registry Editor** when prompted.

The registry editor is arranged with Keys listed on the left side panel and Values listed on the right side panel.

Add a Key

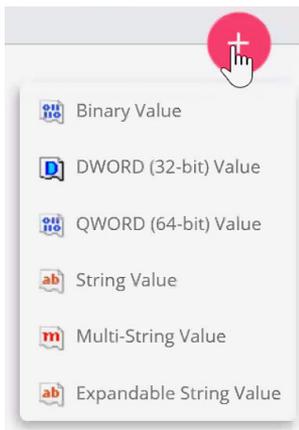
- 1 Once a connection has been established to the remote device, you can add a key by selecting the hive you want to add a key to. Select a hive folder on the left and the entire hive folder opens up, revealing all the existing keys.
- 2 Select the 'Hamburger menu' icon to the right of the hive folder. A menu displays showing options for making new keys and values, renaming keys and values, and deleting keys and values.



- 3 Select **New** followed by **Key**. A new key (or folder) appears in the left side panel, labeled **New Key**, selected, and ready for editing.
- 4 Give the **New Key** a new label and press the Enter key.

Add a Value

- 1 With the correct key selected in the left side panel, select the 'Hamburger menu.' A menu displays showing options for making new keys and values, renaming keys and values, and deleting keys and values.
- 2 Alternately, you can select the Plus Sign circled in red to create a Value.



- 3 Select the type of Value you want to add. The right side panel displays, featuring the options you must complete to create the value you selected.
 - Binary Value
 - DWORD (32-bit) Value
 - QWORD (64-bit) Value
 - String Value
 - Multi String Value
 - Expandable String Value
- 4 Complete the **Value Name** and **Value Data** options then select **Save**.

Rename a Key or Value

- 1 Identify the key or value you want to rename.
- 2 To rename a key or value, select from among the following.
 - **Key** – In the left side panel, select the 'Hamburger menu' icon to the right of the key name and select **Rename**.
 - **Value** – With the key selected in the left side menu, identify the value in the key you want to rename. Select the pencil icon to the far right side of the Value listing.
- 3 Enter the new **Key Name** or **Value Name**.

Delete a Key or Value

- 1 Identify the key or value you want to delete.
- 2 To delete a key or value, select from among the following.
 - **Key** – In the left side panel, select the 'Hamburger menu' icon to the right of the key name and select **Delete**.
 - **Value** – With the key selected in the left side menu, identify the value in the key you want to delete. Select the trash bin icon to the far right side of the Value listing.
- 3 Confirm that you want to delete the **Key Name** or **Value Name** or you can cancel the deletion.

Session Collaboration

You can get additional help during advanced troubleshooting sessions in Workspace ONE Assist by starting a Session Collaboration. Share your active session with 'Tier 2' technical support and allow them to remotely view and control the same end user device.

Session Collaboration is available during Screen Share and Remote View Assist sessions on Android, macOS, and Windows 10 devices.

As the initiator of the Assist session with the end user, you are the **Host** during session collaborations. The Host invites other participants, called **Guests**, to join the active Assist session by chat or email. If you grant your Guest control of the active Assist session, then they become a **Privileged Guest**.

- **Bandwidth Limitations** – In order to ensure a smooth session collaboration, you are limited to a grand total of six (6) participants in any given session. This includes the Host, the device End User, and four (4) Guests, only one of which can be the Privileged Guest at any given time.

The only active sessions **Guests** and **Privileged Guests** are able to see is Screen Share and Remote View sessions. During a Session Collaboration, if the **Host** invokes other client tools such as Manage Files or Registry Editor, **Guests** and **Privileged Guests** see the Screen Share or Remote View screen while the **Host** uses the other client tool. The session becomes visible again to **Guests** and **Privileged Guests** only when the **Host** returns to the Remote View or Screen Share session.

For more information about what the end user experiences during a session collaboration, see [Session Collaboration Notifications and Prompts](#).

Session Collaboration Features by Participant Type

Features	Host	Privileged Guest	Guest
AppList / Device Info / Process List	YES	NO	NO
Connect to a new Tool (File Manager / Remote Shell / Command Line / Registry Editor)	YES	NO	NO
Invite a Guest	YES	NO	NO
Key / Touch / Mouse Events	YES	YES	NO
Multiple Monitors	YES	YES	NO
Remove a Guest from the session	YES	NO	NO
Revoke Session Control	YES	NO	NO
Screen Recording / Capture	YES	NO	NO
Session Elevation from remote view to Share Screen	YES	YES	NO
Shortcuts	YES	YES	NO
Transfer Session Control	YES (to Guest)	YES (to Host Only)	NO
Virtual Keyboard	YES	YES	NO
Whiteboard	YES	YES	YES

Invite Guests to a Session

Only you, the **Host**, can invite guests to a session.

- 1 Initiate an invitation by selecting the Session Collaboration icon  on the main menu toolbar.
 - If you have hosted a session collaboration before, a list of past guests displays, allowing you to select from this list.
- 2 Select the **+Invite Guest** link. The Invite Guest screen displays.
- 3 Select the **Copy invitation** button.
- 4 Open a separate email app or chat app. Paste the copied invitation into a new email or chat and send to the contact of your choice.
 - The link included is a one-time use link and valid only while the Assist session remains active.

Once the invitation is sent, you can cancel the invitation by selecting the Session Collaboration icon  and clicking the cancel button  next to the invitation.

Joining a Session as a Guest

- 1 Select the link provided in the invitation. You are redirected to a Guest Login Page.
- 2 Enter your **Name** and the **password** provided in the invite.
- 3 Once connected, the Host and device End User are notified of your arrival to the session.
- 4 You can view the list of participants by selecting the Session Collaboration icon .

Request to be Elevated to a Privileged Guest

Guests can request to become a Privileged Guest and take control of the session.

- 1 The Guest must select the Session Collaboration icon  and click the **Request Session** link. You receive a notification that a Guest has requested elevation.
- 2 If you grant access, the Guest becomes a Privileged Guest and takes control of the session.

Elevate One of Your Guests to a Privileged Guest

As the Host, you can hand off control to one of the Guests of a session, elevating them to a Privileged Guest.

- 1 Select the Session Collaboration icon  and click the mouse icon  next to the guest you want to elevate to Privileged Guest.
- 2 Your new Privileged Guest now has control over the session.
 - Despite the temporary loss of control over the session, you are still the Host.

Revoke Controls from a Privileged Guest

As the Host, you can Revoke control from the Privileged Guest of a session.

- 1 Select the Session Collaboration icon  and click the solid mouse icon  next to the Privileged Guest you want to demote to Guest.
- 2 You now have control over the session once again.

Remove a Participant from a Session Collaboration

As the Host, you can remove or excuse a Guest or Privileged Guest from a session.

- 1 Select the Session Collaboration icon  and click the cancel icon  next to the participant you want to excuse from the session.
- 2 The participant is excused from the session and disappears from the participant listing.

Leaving a Session Collaboration as a Guest

Guests can select the Disconnect icon  in the main menu toolbar at any time to leave the active session.

Ending a Session Collaboration as Host

To end a session as the Host, select the Disconnect icon  in the main menu toolbar at any time to leave the active session.

Activity Logs (Accessed From App Only)

The device end user can access activity logs from the Workspace ONE Assist App during and after remote support sessions.

Activities Logged

These logs provide the end user full visibility into all activity performed by the Help Desk Admins during a remote session related to the following tools

- File Manager
- Remote Shell (Windows 10 and macOS)
- Command Line (Android)

During a remote session, access the log by selecting the Log tab () located next to the Home tab.

After a remote session, access the log by selecting the Settings icon () in the upper-right corner of the app.

Troubleshooting Workspace ONE Assist

9

If you are having issues with your Workspace ONE Assist performance or service, consider troubleshooting your issue before calling support.

These troubleshooting steps address the most common issues with the Workspace ONE Assist service. The problems below are grouped by category. Some problems may have more than one possible cause and solution.

Generate Certificates

Problem

While running the "Certificate Seed Script.sql" file in Step 10 of the Generate Workspace ONE Assist Certificates task, you might see an error. This error reads "The conversion of a varchar data type to a datetime data type resulted in an out-of-range value."

Possible cause

Such an error is likely the result of a difference in locale between the machine upon which the SQL script was generated and the database server on which it is being run.

Solutions

There are two possible solutions.

- Ensure that the same date format is set in the SQL script by running the cert provisioning tool on a machine with the same locale settings as the database server.

OR (if the first solution is not possible).

- Manually edit the date format in the SQL script. For more information about date formats, see <http://www.sql-server-helper.com/tips/date-formats.aspx>. References in this documentation to any specific service provider, manufacturer, company, product, service, setting, or software do not constitute an endorsement or recommendation by VMware. VMware cannot be held liable for any damages, including without limitation any direct, indirect, incidental, special, or consequential damages, expenses, costs, profits, lost savings or earnings, lost or corrupted data, or other liability arising out of or related in any way to information, guidance, or suggestions provided in this documentation.

Remote Management Not Available - Device Registration Issues

Problem - Workspace ONE Assist Link Does Not Display in Workspace ONE UEM

"Remote Management" link does not display in the More Actions drop-down menu as seen in Device Details View OR device is not shown in the Device List View.

Possible cause

Registration failed or Intelligent Hub might not have been deployed properly. Intelligent Hub might have not been installed on the device properly or registration to Workspace ONE Assist Server has failed.

Solution

Attempt to re-register the device. Update Resource portal to ensure that Intelligent Hub can be properly downloaded and installed on device. A Workspace ONE UEM administrator must re-register the device.

Problem - Registration Check Returns Failed

Device does not register with Workspace ONE UEM or the Workspace ONE Assist portal.

Possible cause

P7b file missing root/intermediate certificates in certificate chain. In MMC (Microsoft Management Console) certificate console when opening the certificate, the certificate path is missing and certificate status displays: the issue of this certificate can not be found.

Solution

Reinstall the certificate including intermediate and root certificate. Reinstall all the certificates for this client and ensure that the root certificate is placed into the root certificate folder and the intermediate certificate is placed in intermediate certificate folders in the MMC certificate console.

For more information about the device registration failed error, see the knowledge base article, ['Device registration check failed' error is displayed in Workspace ONE UEM Console when initiating a remote session on enrolled devices.](#)

Problem - Error Message, 'Registration Failed: Server Not Found'

Device does not register with Workspace ONE UEM or the Workspace ONE Assist portal.

Possible cause 1

Workspace ONE Assist Site URL capital and lower-case letters. In Workspace ONE Assist tool versions 4.4.2.6291 and prior, the URL for remote management server is CAPS sensitive. In the example shown below, the URL uses upper-case and lower-case letters 'https://rmSTAGE01.awmdm.com'.

Solution 1

Remove upper case characters from the Workspace ONE Assist site URL. Review the Workspace ONE Assist site configuration. You must ensure that the URL has all lower-case letters. In the example above, the URL must be 'https://rmstage01.awmdm.com'.

Possible cause 2

Firewall is ON but misconfigured. If the firewall is incorrectly configured on the Workspace ONE Assist Server, it might be preventing device registrations from being received.

Solution 2

Turn off firewall or set up exceptions. When the firewall is on and it is not correctly configured, it might be preventing device registrations. Devices register with the Anchor web service, hosted on port 443 on the Workspace ONE Assist server. If this port is blocked on the firewall, registrations are jeopardized. Turn off the firewall and see if registrations succeed. If they do, review the exceptions to ensure that the Anchor web service on port 443 or other port defined for this service is in the list of exceptions.

Issues Connecting to Devices

If you are having connectivity issues with your Workspace ONE Assist performance or service, consider troubleshooting your issue before calling support. These troubleshooting steps address the most common connectivity issues with the Workspace ONE Assist service.

Problem - Browser Window Does Not Open Remote Management Portal

The Workspace ONE Assist portal is not opening on Workspace ONE UEM users' browser window.

Possible cause 1

Incompatible web browser. The browser being used by VMware Support staff is not compatible with Workspace ONE Assist.

Solution 1

Use a different web browser. Install or switch to a compatible browser. The following is a list of browsers currently supported by the Workspace ONE Assist Tool.

- Google Chrome
- Safari

Possible cause 2

Browser pop ups are blocked. The browser being used is blocking pop-up windows from the Workspace ONE Assist portal.

Solution 2

Enable pop-ups in browser settings. UEM console users must update their browser settings to allow pop-ups from the Workspace ONE Assist portal.

Problem - Remote Support Validation Fails

During Workspace ONE Assist validation steps, one or all the three validation steps and 'Launch Session' button does not appear.

Possible cause(s): Certificate mismatch, Workspace ONE Assist server issues. Client-server certificates might be incorrectly deployed or there might be issues with availability of Workspace ONE Assist server and console.

Solution: Review certificates and ensure that Workspace ONE Assist servers are operational. Ensure that T10 interface certificate has been properly deployed on the Workspace ONE Assist servers, ensure that Workspace ONE Assist servers are online and operational.

Modify Database Record for Multi-Node Configuration

In order for the Workspace ONE Assist server to operate correctly in a multi-node configuration, you might need to modify DB records in [ApAdmin].[dbo].[Server].[FQDN]. Some installations result in these tables pointing to the external Virtual IP (VIP) address by default. This default arrangement must be changed.

Note Active-passive configurations with standard, all-in-one installations do not need this FQDN change inside the database table. Applying this change in such an environment might break the configuration. Consult with support if you are unsure which configuration you have.

Ensure that each [FQDN] record in the [ApAdmin].[dbo].[Server] table in the database points to the internal IP address of the VIP (also known as Virtual IP) for the load balanced pool.

The number of [FQDN] records is equal to the number of application/connection proctor servers in your deployment. Therefore, you must update each one in the table. For example, if your deployment has four connection proctor servers, then you must locate and modify 4 [FQDN] records in the [ApAdmin].[dbo].[Server] table.

After you finish the record modification, restart all Workspace ONE Assist Servers.