Advanced Remote Management

VMware Workspace ONE UEM 1902

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

Introduction to Advanced Remote Management

1

Advanced Remote Management (ARM) allows you to connect to end-user devices remotely to aid in troubleshooting and maintenance. ARM is a premium upgrade that uses a new remote management client with enhanced functionality.

The Remote Management 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.

Advanced Remote Management is already configured for SaaS customers who have purchased the upgrade.

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

This chapter includes the following topics:

- Typical Deployment

- Advanced Remote Management Supported Platforms

- Advanced Remote Management Requirements

Typical Deployment

Most users typically deploy the Advanced Remote Management (ARM) server in an enterprise network to facilitate the communication between the various components.

Without Load Balancer

This sample diagram is a typical deployment without the use of a load balancer.
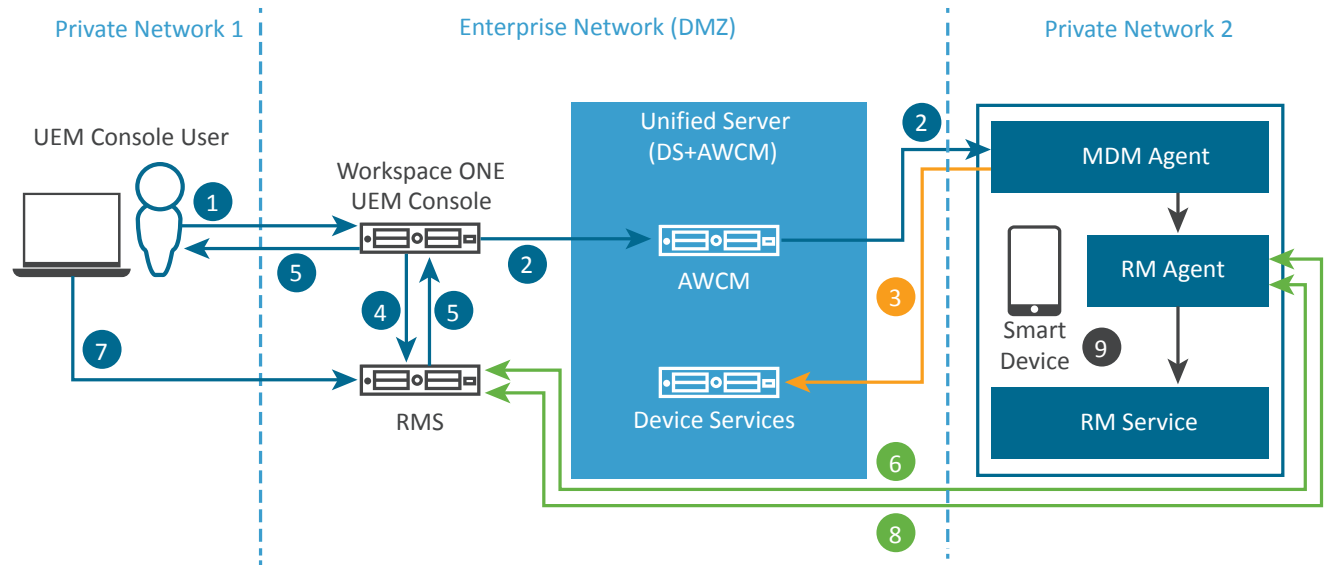
1. Queue RM Command	6. Request Remote Management Session URL.
2. Queuing Command to Connect to RMS	7. Admin Joins Remote Management Session
3. Confirm Command.	8. Device Joins Remote Management Session
4. Create Remote Management Session.	9. Send Commands/Get Frames.
5. Send Session URL.	

With Load Balancer

This sample diagram is a typical deployment that includes a load balancer. For more information, see
Integrate a Load Balancer to Your Deployment.
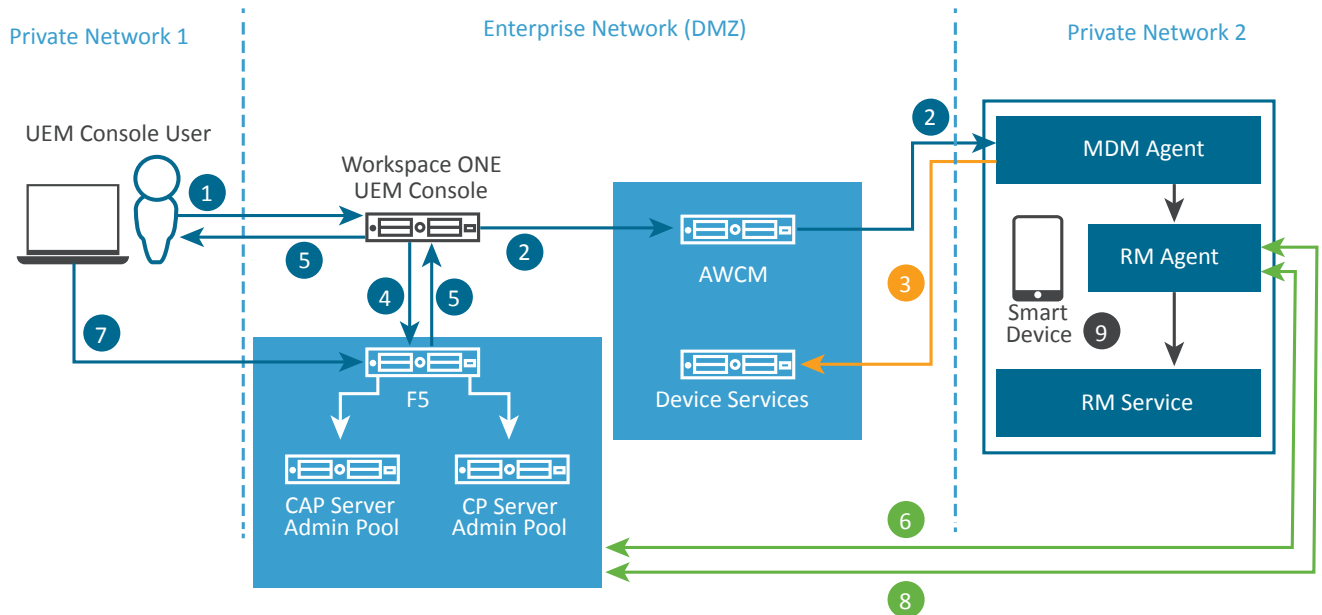
CAP Servers contain Core Services, Application Services, and Portal Services and can be load balanced.

CP Servers cannot be load balanced with the F5 since they use built-in software load balancing.

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

Advanced Remote Management Supported Platforms

Advanced Remote Management (ARM) supports Windows Rugged and Android devices running the proper Workspace ONE Intelligent Hub and Advanced Remote Management service.

iOS devices can be viewed using Remote View, a feature in VMware Workspace ONE UEM console, and requires an Advanced Remote Management server.

ARM supports the following platforms.

- iOS devices running v7.0.0 or later with the Workspace ONE Intelligent Hub v4.9.3 or later (for Remote View only).

- Windows Mobile/CE running .NET 2.0+ with the Workspace ONE Intelligent Hub v6.0.4 or later installed.

  - Advanced Remote Management for Windows Mobile devices is only intended to be used with Windows Mobile devices that are not being actively used by end users (for example, devices that are cradled or docked). When using advanced Remote Management with Windows Mobile devices, no device notification is provided when the remote management functionality is in use. You are solely responsible for notifying any device end users of your use of this remote management functionality.

- Android devices with the Workspace ONE Intelligent Hub v7.0 or later installed.

  - Samsung Knox Devices – ARM can access only the personal side of Knox Dual Persona Mode.

  - Android (previously known as Android Enterprise and Android for Work) – ARM can access only the Work Managed mode running on Android v6.0 (Marshmallow) or later.

You must also download the required Advanced Remote Management CAB (for Windows Rugged) or APK (for Android) from the My Workspace ONE ™ documentation repository (https://my.workspaceone.com/).

Advanced Remote Management Requirements

You must meet the listed requirements before using Advanced Remote Management (ARM).

General Requirements

For SaaS customers, the general requirements are the only requirements that the admin must meet.

Requirements	Minimum
Supported Browsers	Latest version of Google Chrome, Safari, Internet Explorer, or Edge. File Manager feature is supported by Chrome only.
Workspace ONE ™ UEM version	Workspace ONE UEM 9.2 or later with the ARM add-on.

Hardware Requirements

Hardware	Minimum
Advanced Remote Management Server	
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
Advanced Remote Management Database Server	
CPUs	2.4 GHz Processors, 4 Logical Processors,2 CPUs, 2 Core 2x2 or 4 physical depending on machine type, virtual machine or physical.

Hardware	Minimum
Memory	16 GB
Hard Drive IOPS	200
Hard Drive Space	200 GB for databases
Bandwidth	
Average Remote Session Requirement	1 MB/per minute (17 kbps)

Hardware Scaling Requirements

Use the following requirements as a basis for creating an effective advanced remote management system that scales to your on-premises environment.

These requirements do not include network equipment such as load balancers or monitoring servers.

# Devices / # of Concurrent Remote Sessions	Core Server (all in one)	DB Server	CP Server	CAP Server
Less than 1000 / Less than 100.	1 server.(2 CPUs, 10 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012-2016 Express (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 Express.	n/a	n/a
1000 - 10,000 / Less than 100.	1 server.(2 CPUs, 10 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 - 50,000 / Less than 100.	1 server.(2 CPUs, 12 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, 16 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012-2016 Standard.	n/a	n/a
50,000 - 100,000 / Less than 100.	1 server.(2 CPUs, 16 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, 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	Core Server (all in one)	DB Server	CP Server	CAP Server
100,000 - 500,000 / Less than 100.	n/a	SQL cluster.(2 CPUs, 32 GB RAM, 250 GB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012-2016 Standard.	1+ server.(2 CPUs, 16 GB RAM, 250 GB HDD: * Windows 2012 or 2016 w/GUI.	1 server.(2 CPUs, 16 GB RAM, 250 GB HDD: * Windows 2012 or 2016 w/GUI.
500,000 - 1 million / Less than 100.	n/a	SQL cluster.(4 CPUs,32-64 GB RAM, 1 TB HDD): * Windows 2012 or 2016 w/GUI. * MS SQL 2012-2016 Standard.	1+ server.(2 CPUs, 16 GB RAM, 250 GB HDD: * Windows 2012 or 2016 w/GUI.	1 server.(2 CPUs, 16 GB RAM, 250 GB HDD: * Windows 2012 or 2016 w/GUI.

Software Requirements

Ensure that you meet the following on-premises installation requirements.

Requirement	Description
Advanced Remote Management Server	
Operating System	Microsoft Windows Server 2016 or 2012 R2.
Software	Microsoft .NET Framework 4.6.2
Server Roles	■ Application Server. ■ Web Server IIS.

Features	■ .NET Framework 4.6 Features.
	    ■ .NET Framework 4.6.
	    ■ ASP .NET 4.6.
	    ■ WCF Services.
	       ■ HTTP Activation.
	       ■ Message Queuing (MSMQ) Activation.
	       ■ Named Pipe Activation.
	       ■ TCP Activation and TCP Port Sharing.
	 ■ Message Queuing Services.
	 ■ Windows Process Activation Service.
	    ■ Process Model.
	    ■ .NET Environment 3.5.
	    ■ Configuration APIs.

Advanced Remote Management Database	

Requirement	Description
Operating System	■ Microsoft Windows Server 2016 or 2012 R2.
Software	■ MS SQL Server 2012 Standard, orMS SQL Server 2014 Standard and Enterprise, or MS SQL Server 2016 Standard and Enterprise, orMS SQL Server 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 4.6.2. ■ Microsoft SQL Server Management Objects (SMO) DLL.

Database Settings Automatically Created During Installation

You must have a server admin account (or equivalent) for these elements to auto-create at install time.

Server Roles	■ Sysadmin. ■ Bulkadmin. ■ Dbcreator.
User Mapping	■ Dbowner. ■ Dbbackupoperator. ■ SQLAgent dependent. ■ serverGroup dependent.
Users	**Apdbuser** Server role: Db_creator. Database role: Db_owner for all aetherpal user databases. On MSDB, database role to create SQL jobs. [SQLAgentOperatorRole] [SQLAgentReaderRole] {SQLAgentUserRole] **Apadminuser** Server role: Db_creator, to create multitenant databases. Database role: Db_owner for all aetherpal user databases. On MSDB, database role to create SQL jobs. [SQLAgentOperatorRole] [SQLAgentReaderRole] {SQLAgentUserRole]

Network and Security Requirements

The network and security configurations designed for single (all-in-one) server deployments differ from multiple-server deployments. IPv4 is the required protocol for the Advanced Remote Management server. You must disable IPv6.

IP Address and Port Translation, Single-Server Deployment

The ARM server is required to have one static IPv4 address. This address must be accessible from the mobile device network and the user network from which users access the RM 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 ARM server.

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

* Indicates customizable port address.

IP Address and Port Translation, Multiple-Server 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 Portal Services must also have its own static IP address that is accessible from the device network and 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
8443	Connection Proctor Service on CP Server.
8865	Data Tier Proxy (DTP)
8866	Messaging Entity (ME)
8867	Data Access Proxy (DAP)
8870	Service Coordinator (SVC)
12780	Connection Proctor (CP) from Messaging Entity (ME)

* Indicates customizable port address.

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

Persistence for Multiple Server Deployment

Advanced Remote Management 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.

Firewall Rules, Single-Server Deployment

Firewall rules can be summarized based on the number of allocated IP addresses to the ARM 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
Advanced Remote Management server	MS SQL Database Server	TCP	1433	Inbound	Accept

Firewall Rules, Multiple Server Deployment

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
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

Fully Qualified Domain Name and Site SSL/TLS Certificate, Single-Server Deployment

The ARM 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 ARM server's personal certificate store before the ARM 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 the root and intermediate certificates/public key pair must be installed on mobile devices you intend to remote into.

Fully Qualified Domain Name and Site SSL/TLS Certificate, Multiple Server Deployment

One FQDN is assigned to the Portal server and one FQDN is assigned to each CP server deployed in the ARM 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 the root and intermediate certificates/public key pair must be installed on mobile devices you intend to remote into.

Deployments Across Public and Private Security Zones

Single-Server Deployment

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 ARM system.

Multiple Server Deployment

You can deploy ARM servers across multiple security zones, such as DMZ/public and private. You can deploy all servers in public zone or 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.

Domain Name Service

Domain Name Service is required only for multiple server deployments. Domain Name Service is not required on single-server deployments (App+Core+Portal+CP).

In multiple server deployments, the ARM 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 ARM server. The forward lookup zone, the host record, and service records all must point to the ARM server.

Requirement	Description
Forward Lookup Zone	Create a forward lookup zone that points to your ARM server. The forward lookup zone must be named. `controlplane.aetherpal.internal`
Host (A) Record	The Host (A) Record must be named the following. `admin` ■ If the ARM 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 ARM server is not behind a load balancer, then the Host (A) Record must point to the ARM Server IP address.
Service Coordinator Service Records	■ 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 ARM.

Load Balancer 2

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

Integrate a Load Balancer to Your Deployment

You can integrate a load balancer into a new Advanced Remote Management (ARM) configuration, provided you have implemented all the multi-node options during server and database installation.

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

Prerequisites

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.

Procedure

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

2   You must run the database installation by itself even if you are installing other services on the same server.

3   The ARM 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.

What to do next

Ensure that you delete the Default Website from IIS once the server is running. See Domain Name Service. See also Troubleshooting, Modify Database Record for Multi-Node Configuration.

Install Advanced Remote Management

3

Before you can benefit from remotely accessing devices in your fleet, you must install and configure the Advanced Remote Management server.

There are two methods to installing ARM.

- **Standard (Basic)**, for installations that require only the default settings.
- **Advanced (Custom)**, for installations with advanced options such as multiple servers to accommodate high availability and horizontal scaling.

Before deciding which method is right for your needs, you must Generate the Advanced Remote Management Certificates.

This chapter includes the following topics:

- Upgrade to a New Version
- Generate the Advanced Remote Management Certificates
- Install an SSL Certificate
- Standard (Basic) Installation of ARM
- Advanced (Custom) Installation of ARM
- Import Device Profiles with Resource Pack Utility
- Configure the Workspace ONE UEM console
- Configure End-User Devices
- Start an Advanced Remote Management Connection

Upgrade to a New Version

Upgrading to a new version of Advanced Remote Management (ARM) is simple. Take the following steps to install a new version of ARM on top of an existing, older version.

Procedure

1   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.

2   Right-click the installer file and select **Run as administrator**. The installer prompts you to remove the currently installed components, excluding the database.

3   Select **OK** to allow the installer to remove the installed components.

The Uninstall Components screen appears, displaying 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 appears nowhere on this Uninstall Components screen. That is because the database from the old version is going to be used during the upgrade process. This means all your users, administrators, devices, and everything else on the database will be kept intact in the new version of ARM.

4   Select **Uninstall** to commence uninstalling the old components.

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

5   Once all the old components are uninstalled, setup prompts you to install new versions of the same components. Select **Next** to begin.

6   The **Choose Install Location** prompt appears. Accept the default installation location, which appears prepopulated in the text box, by selecting **Install**.

7   The **Installer** screen displays, prompting you to select between **Standard (Basic)** and **Advanced (Custom)**.

For details about each installation method, including all steps, screens, fields, and options, see Standard (Basic) Installation of ARM or Advanced (Custom) Installation of ARM.

8   The installer reads from the install.config file (mentioned in Step 1), applying all the original configurations it finds to the options screens, including SQL server details, usernames, Tenant FQDN, certificates, database configurations, and many other configs. You shouldn't need to modify any of the settings it pulls from this install.config file with the possible exceptions below.

SSL Certificate - If you have installed a new SSL certificate before running this upgrade, ensure you integrate it with the upgrade. Do this by selecting the **SSL Certificate** drop-down menu and choosing the name of the new SSL Certificate.

T10 Certificate - When upgrading from an older version of ARM to a newer version, check the T10 certificate to make sure it is the correct one. If in doubt, 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.

9   The summary page confirms all the installer settings it plans to use for the upgrade. You can use the **< Prev** button to revisit config pages if you want to make changes. Otherwise, select **Install** to begin the upgrade.

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.

10 When the installation completes, select **Next**.

11 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 Advanced Remote Management server has been upgraded.

Generate the Advanced Remote Management Certificates

You must generate the root and intermediate certificates used during installation whether you are performing a **Standard (Basic)** or **Advanced (Custom)** installation.

The installer is called RemoteManagementCertificateGenerator_9_2. This tool 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.

Prerequisites

Download the installer package, titled VMware Workspace ONE ™ UEM Remote Management Installer, from the my Workspace ONE portal (https://myworkspaceone.com).

Procedure

1   Extract all contents from the installer package ZIP file into c:\temp of the ARM 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).

4   The OG you select must be of a 'customer' type.

5   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.

6   If the **Remote Management CN** text box is blank, then you must manually Create the Remote Management CN from the Workspace ONE UEM Database.

7   Set the following values.

Setting	Value
Certificate Type	Remote Management
Deployment	On-Prem
Certificate Common Name	Paste the Remote Management CN copied from the preceding step (Step 6).

8   Select **Generate Certificates**.

9   Set **Password** for the certificates when prompted. Store this password for future use.

10   Navigate to the folder holding the Remote Management Certificate Generator.

11   Find the generated certificates file in the Artifacts\private folder called root_intermediate_chain.p7b.

12 Copy this file to the c:\temp\certs folder on the Advanced Remote Management Server. This file is the T10 Certificate. The T10 interface certificate contains two major certificates that enable Workspace ONE UEM to communicate with the T10 portal. These certs are the Workspace ONE UEM portal Root and Intermediate certificates in a p7b file.

13 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 Troubleshooting, Generate Certificates. Support for multiple Workspace ONE UEM environments is available. For details, see Configure Multi-Workspace ONE UEM Environment Support.

What to do next

Proceed next to Install an SSL Certificate.

Install an SSL Certificate

You must incorporate a secure sockets layer (SSL) certificate into the Advanced Remote Management (ARM) 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. You must provide the SSL certificate as a wildcard or SAN certificate.

This process applies only to the SSL certificate. This process does not apply to the root and intermediate chain, the details of which can be viewed in Generate the Advanced Remote Management Certificates.

Procedure

1 Run the Microsoft Management Console (MMC).

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

2 In the **File** menu of the MMC app, 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** dialog 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 app, 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 marks to the two boxes labeled **Mark this key as exportable** and **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**.

What to do next

If you are installing ARM, then you must decide whether you are executing a Standard (Basic) Installation of ARM or an Advanced (Custom) Installation of ARM.

▪   **Standard (Basic)**, for installations that require only the default settings.

▪   **Advanced (Custom)**, for installations with advanced options such as multiple servers to accommodate high availability and horizontal scaling.

Standard (Basic) Installation of ARM

The Standard (Basic) method of installing the Advanced Remote Management (ARM) server, for environments that require only the default settings, is a process that is comprised of a single phase.

Procedure

1   Download, extract, and save the Advanced Remote Management installer into a temporary directory on the ARM server, right-click the installer file, and select **Run as administrator**.

2   At the Welcome screen, select **Next**.

3   Enter the directory where you want to install the Advanced Remote Management application and select **Install**.

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

4   Select Standard Installation (Basic) and then select **Next**.

5   If SQL Server is already installed on the server or on another server where RM databases will be 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.
Username	If SQL Server Authentication was used, type in the username that is used to authenticate against the SQL server.
Password	Type in the password for the username selected.

a   Select the **…More** button to enter additional details.

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

b   Specify passwords for these accounts.

c   Enter in the path for database MDF, LDF, and NDF files.

d   Select **Save** to proceed.

You are taken back to previous screen.

e   Select **Next** to proceed.

6   In the **Tenant FQDN** field, 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.

7   In the **SSL Certificate** field, select the folder button or the pull-down arrow to select the SSL certificate for the ARM system that should correspond to the FQDN.

The certificate should have been installed in the local system personal certificate store.

8   Select the certificate and then select **OK**.

9   Deselect the **Apply Default Settings** check box and select the folder icon to attach the T10 certificate.

10 Browse for the T10 certificate, select the certificate, and then select **Open**.

11 Select the **…More** button to select additional settings for the ARM system. Verify the parameters.

Setting	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 may be reached. By default, the setting is 'All Unassigned' to enable all interfaces/IPs.

Setting	Description
HTTPS port	Defines the HTTPS port used by portal services for outside access. By default, port 443 is selected. You may use a different port, such as 7443 if 443 is already used.
SSL Enable	Enables SSL/TLS protocol for portal services. By default, this checkbox is enabled so that the portal services utilize SSL/TLS. Leave this checkbox enabled.
T10 Username and Auto Generated	Defines T10 API user for connectivity between AirWatch portal and RM system. By default, if 'Auto Generated' checkbox is enabled, the installer assigns a random username to be created locally on the server. Leave this field defaulted and the checkbox enabled for the Installer to create the T10 API user. If you would like to define the user, disable the check box and type in the T10 username you would like to use.
CP FQDN/Port	Defines the FQDN and port on which CP services may be reached. Enter in the FQDN, which should be the same as the FQDN assigned for portal services. Enter port 8443, which is the default port for CP services. If port 8443 may not be used, you may enter any other port. Be sure that network/security teams will use this assigned port when assigning translation rules from the firewall/router to the RM Server for CP services.

12 Select **Save** to continue.

You are taken to previous screen.

13 Select **Next** to continue.

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

14 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 may need to reboot the server after the prerequisites are installed.

c After the reboot, relaunch the installer.

The installer will be pre-populated with your previous selections.

15 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 of time.

16 When the installation completes, select **Next** to continue.

17 When prompted to run the Resource Pack that loads all available device profiles onto the ARM system, leave the **Execute Resource pack** check box checked and 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.

What to do next

Next, proceed to .

Advanced (Custom) Installation of ARM

The Advanced (Custom) method of installing the Advanced Remote Management (ARM) server, featuring advanced options such as multiple servers to accommodate high availability and horizontal scaling, is a process that is comprised of a single phase.

Take the following steps to install ARM with its advanced (custom) configuration.

Procedure

1   Download, extract, and save the Advanced Remote Management installer into a temporary directory on the ARM server, right-click the installer file, and select **Run as administrator**.

2   At the Welcome screen, select **Next**.

3   Enter the directory where you want to install the Advanced Remote Management application and select **Install**.

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

4   Select Advanced Installation (Custom) and then select **Next**.

5   Select all components to install on the server.

   ■   Database

   ■   Core Services

   ■   Portal Services

   ■   Application Services

   ■   Connection Proctor

6   Select **Next**.

7   Configure the Database settings. Select **Connect to existing SQL Server** and complete the following settings.

Setting	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**.
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 ARM.
Password	Enter the password of the database account.

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

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

Setting	Description
DB Owner User name/ Password	Set the user name and password for the ARM database owner SQL account. This account does not have system-wide permissions. The account only has permissions within the ARM databases. This user name is **apadminuser**.
DB Application User name/ Password	Set the user name and password for the ARM 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).

9   Select **Save** followed by **Next**.

10 Configure the Portal settings.

Setting	Description
Tenant FQDN	Enter the server fully qualified domain name. For example, "rmstage01.awmdm.com"
SSL Certificate	Select the folder icon to browse for the SSL Certificate already installed. For details, see Install an SSL Certificate.
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**.

11 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.

Setting	Description
DB Application User name/ Password	Enter the user name and password for the ARM 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 may enter an alternate port number, such as 8080.
IIS Site Binding IP Address	Defines from which interfaces/IP addresses portal services may 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 may 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.

Setting	Description
T10 User name and **Auto Generated**	Defines T10 API user for connectivity between AirWatch portal and RM 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 field defaulted and the check box enabled for the Installer to create the T10 API user. If you would like to define the user, disable the check box and type in the T10 user name you would like to use.
Forward Lookup Zone	To the right of the **Auto Generated** label, enable this check box and enter your forward lookup zone here. You can also enter a custom lookup zone.

12 Select **Save** followed by **Next**.

13 Configure the Connection Proctor 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.

Setting	Description
Connection Proctor FQDN	Defines the Fully Qualified Domain Name (FQDN) on which CP services may be reached. Enter in the FQDN, which should be the same as the FQDN assigned for portal services.
Port	Enter the port number for CP services. The default is 8443 but you may enter your preferred port number. Whatever port you choose, ensure that network/security teams use this port when assigning translation rules from the firewall/router to the ARM Server for CP services.
SSL Certificate	Select the folder icon to browse for the SSL Certificate already installed. For details, see Install an SSL Certificate. SAN (subject alternative name) certificates are supported. The implementation of SAN certificates depends upon your server arrangement. ▪ Single Node – The SAN certificate must define the FQDN for each public facing server/SSL termination point that hosts the solution. ▪ Multi-Node – The SAN certificate must have an FQDN defined for each connection proctor server and advanced remote management server. ▪ For example, presume you have 2 connection proctor servers and 2 advanced remote management servers. The 2 ARM servers host portal services, which need 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.
Apply Default Settings	Enable this check box to pre-populate the additional setting **Enrollment Certificate**.

14 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 these non default port numbers here.

Setting	Description
DB Application User name/ Password	Enter the user name and password for the ARM database application account. This user name is **apdbuser**.
CP Internal IP Address/Port	Defines from which internal IP addresses the connection proctor may 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 may 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.

15 Select **Save** followed by **Next**.

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

What to do next

Proceed to Configure the Workspace ONE UEM console.

Import Device Profiles with Resource Pack Utility

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

Procedure

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 ARM server.

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

Configure the Workspace ONE UEM console

After installing the Advanced Remote Management (ARM) server and all its components, configure the UEM console to communicate with the ARM server.

Procedure

1   In the UEM console, ensure that you are in the Global OG.

2   Navigate to **Settings > System > Advanced > Site URLs > External Remote Management**.

3   Complete the ARM settings.

Settings	Description
Console Connection Hostname	Enter the ARM server fully qualified domain name (FQDN) plus "/t10". For example: `https://rmstage01.awmdm.com/t10`
Device Connection Name	Enter the ARM server fully qualified domain name (FQDN). For example: `https://rmstage01.awmdm.com`

4   Select **Save**.

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

What to do next

Proceed to Configure End-User Devices.

Configure End-User Devices

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.

Procedure

1   Visit the my Workspace ONE ™ page that lists all the device agents.

    https://my.workspaceone.com/products/AirWatch-Agent

2   Identify and download platform-specific Remote Management agents that are applicable to your deployment.

3   You can push these apps to devices as an internal app through the App Management function in Workspace ONE UEM or you can utilize Product Provisioning.

    For more information about App Management, see the **VMware AirWatch Mobile Application Management Guide**.

    For more information about Product Provisioning, see the **VMware AirWatch Product Provisioning for Android Guide** and **VMware AirWatch Product Provisioning for Windows Rugged Guide**.

    All of these guides and more can be found on docs.vmware.com.

You are now ready to manage devices remotely.

What to do next

Proceed to Start an Advanced Remote Management Connection.

Start an Advanced Remote Management Connection

Connect to devices for troubleshooting and maintenance using the Advanced Remote Management (ARM) connection tool. This tool starts a remote management session and controls the connection to the remote device.

There are three supported remote client tools at your disposal.

▪   **Display Capture** – View a remote device's screens, create shortcuts, and diagnose device issues.

▪   **Manage Files** – Access the file system of the remote device.

▪   **Command Line (Android Only)** – Send commands to the remote device using the Command Line Interface (CLI).

Procedure

1   Navigate to **Devices > List View** and select the friendly name of the device you want to create a remote connection with.

    This page displays the **Details View** for the selected device.

2   Select the **More Actions** drop-down menu and select **Remote Management**.

3   In the Remote Support window, select **Launch Session** after the connection process completes.

(Applicable to devices in Attended Mode only) The console displays a four-digit PIN which you must direct the device user to enter into their device. This action provides authorization to manage the end user's device remotely.

Once the connection is made, the remote management client opens and the device is ready for use.

Advanced Remote Management Client Tools

4

The Advanced Remote Management (ARM) client provides support tools to facilitate troubleshooting and remotely controlling end-user devices. The tools are located around the device view.

Advanced Remote Management does not have the same functionality as Remote Management v3.0. The following features are not currently available in ARM.
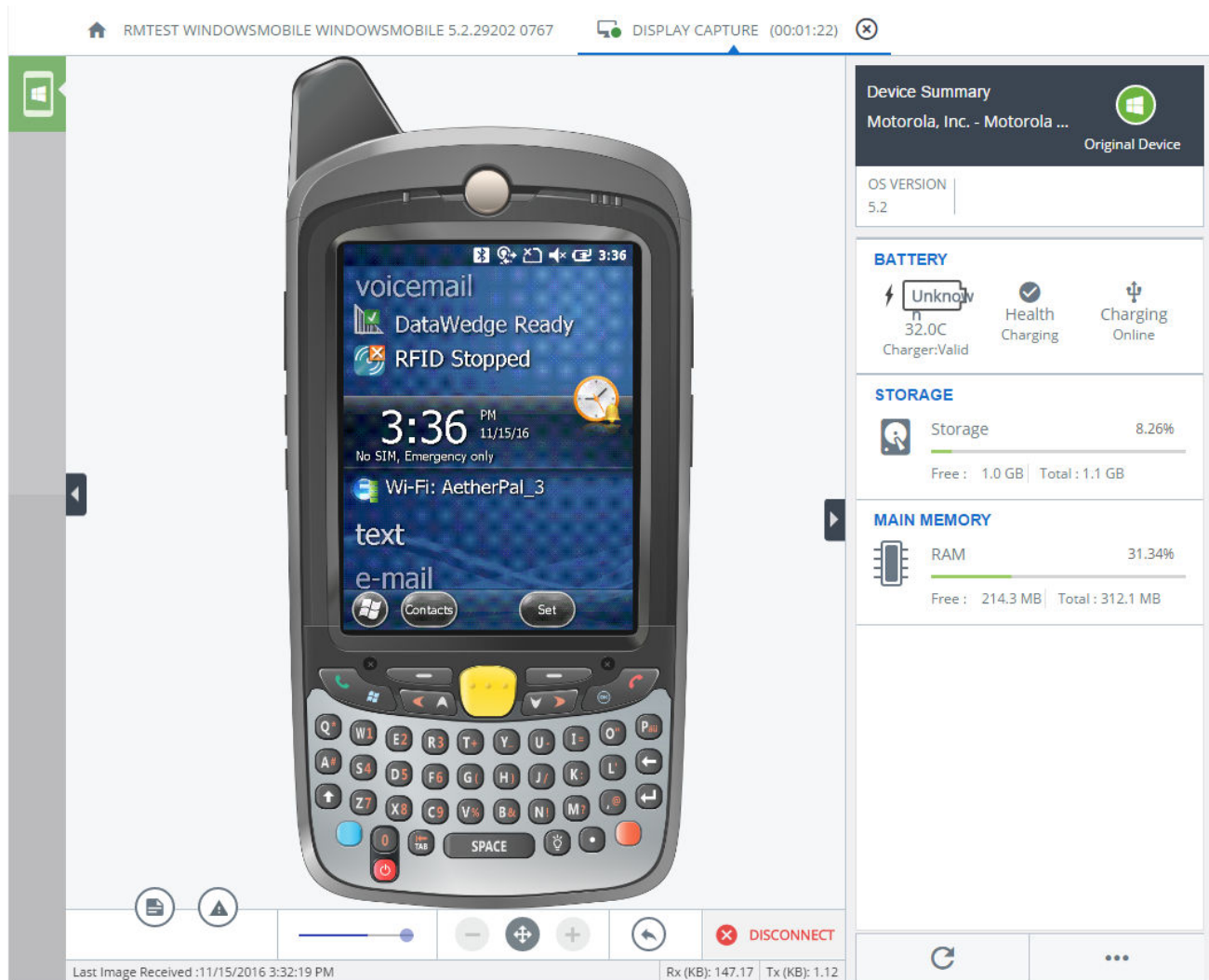
- Registry Manager

- Macros during the session.

This chapter includes the following topics:

- Main Display for Remote Control

- Capture Video and Images

- Manage Files

- Command-Line Interface

Main Display for Remote Control

The main section of the Advanced Remote Management (ARM) client is a device screen view that allows you to control the end-user device remotely.

Control the device by clicking or dragging on the displayed screen and buttons. You can send keystrokes to the device and copy and paste information onto the device during a session.

If a user needs privacy, they can pause a remote control session.

Device Whiteboard, Android Only

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.
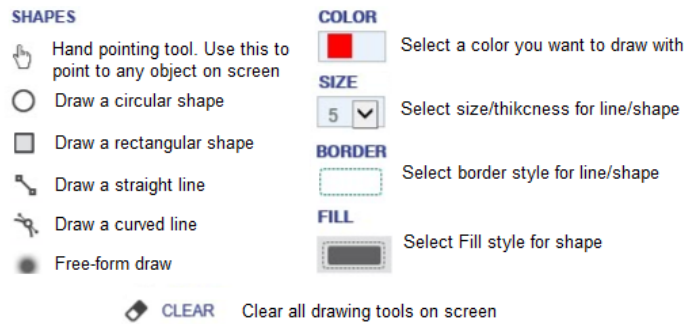
Shortcuts

The ARM client provides a shortcuts menu to navigate quickly to a screen or menu item on the device. The shortcuts icon is on the bottom right, near the whiteboard icon.

Device Summary

The ARM client provides a device summary of information similar to Device Details. Use this information to diagnose issues on a device while connected without navigating away from the ARM client.

The Device Summary pane provides at-a-glance information to use during troubleshooting. The pane displays signal strength, battery, network status, storage, and main memory information. Display additional information not displayed in the information by selecting the Additional Information (•••) icon.

Detailed Device Information

The Additional Information screen provides detailed information on the device, applications, processes, and remote control history.

Select each information list from the left navigation bar.

The Device information displays Device make and model, battery details, storage, connection, RAM, and more. Minimize the pane and manage which panes are visible by clicking each device details section header. You can also search for specific information with the search bar in the top right corner.

The application list provides a list of applications installed on the device and application details such as the version number and package name. You can stop any running app from this list.

The process list displays the current processes running on the device and detailed information. You can kill any running process from this list.

Capture Video and Images

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

Prerequisites

Make sure you have initiated a remote session and that there are no connectivity issues.

Procedure

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.

Manage Files

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

Upload a File

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

Procedure

1   In the active Advanced Remote Management (ARM) 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.

Procedure

1   In the active ARM 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.

Procedure

1   In the active ARM 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.

Procedure

1   In the active ARM 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.

Procedure

1   In the active ARM 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.

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.

Procedure

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.

Procedure

1   In the active ARM 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.

Procedure

1   In the active Remote Management session, locate the header bar toward the top of the browser.
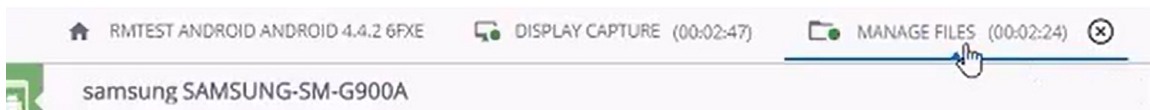
2   Select the circled **X** button to the right of the Manage Files indicator.

3   Select **OK** to confirm closure of the Manage Files session.

Command-Line Interface

The Command-Line Interface (CLI) is the counterpoint to the Graphical User Interface (GUI). While
graphical user interfaces make common tasks easy, command-line interfaces make difficult tasks
possible.

This list applies to Android only.

CLI Commands	Support Level	Function
am get-config	Full	Gather configuration data from a device.
cd	Full	Change directory.
getprop	Full	Get properties via the android property service.
getprop ro.build.version.sdk	Full	Get API level device properties.
ip -f inet addr show wlan0	Full	Show WiFi IP address.
logcat	Full	Prints log data to the screen.
logcat *:D	Partial	Prints log data to the screen, filter to show only the debug level. In a few devices, this command cannot be canceled.
logcat *:E	Partial	Prints log data to the screen, filter to show only the error level. In a few devices, this command cannot be canceled.
logcat *:I	Partial	Prints log data to the screen, filter to show only the info level. In a few devices, this command cannot be canceled.
logcat *:V	Partial	Prints log data to the screen, filter to show only the verbose level. In a few devices, this command cannot be canceled.
logcat *:W	Partial	Prints log data to the screen, filter to show only the warning level. In a few devices, this command cannot be canceled.
ls	Full	List the directory contents.
ls -a	Full	List the directory contents, do not hide entries starting with a dot.
ls -n	Full	List the directory contents, list numeric UIDs, and GIDs.
ls -R	Full	List the directory contents, list subdirectories recursively.
ls -s	Full	List the directory contents, print size of each file, in blocks.
mkdir	Full	Make directory.
netcfg / ifconfig	Full	Configure and manage network connections via profiles.
netstat	Full	Network statistics.
ping	Partial	Test the connection and latency between two network connection. In few devices, this command cannot be canceled.
pm list packages	Full	Prints all packages, optionally only those whose package name contains the text in <FILTER>.
pm list packages -3	Full	Prints all packages filtered to show only the third-party packages.
pm list packages -d	Full	Prints all packages filtered to show only the disabled packages.
pm list packages -e	Full	Prints all packages filtered to show only the enabled packages.
pm list packages -f	Full	Prints all packages including their associated file.
pm list packages -i	Full	See the installer for the packages.
pm list packages -s	Full	Prints all packages filtered to show only the system packages.
pm list packages -u	Full	Prints all packages including uninstalled packages.
pm list permission-groups	Full	Lists all permissions groups.
pm list permissions	Full	Lists all permissions on the device.

CLI Commands	Support Level	Function
pm path <package >	Full	Print the path to the APK of the given <package>.
ps	Full	Print process status.
ps -p	Full	Print process status and show scheduling policy.
pwd	Full	Print the current working directory location.
rm -d	Full	Remove a directory, even if it is not empty.
rm -f	Full	Remove a directory, force remove without prompt.
rm -r	Full	Remove the contents of the directory recursively.
top	Partial	Display top CPU processes. In a few devices, this command cannot be canceled.
touch	Full	Create an empty file or change file timestamps.

Advanced Remote Management Components

<div style="text-align: right">

5

</div>

Advanced Remote Management (ARM) 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 ARM system is comprised 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 ARM 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 ARM 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 ARM. 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 ARM server.

    - The T10 interface uses Representational State Transfer (REST) communication with a JavaScript Object Notation (JSON) payload. The T10 interface allows Workspace ONE UEM to make a mobile device eligibility call.

    - The T10 interface can also start a remote support session using the ARM tool and delete the device from the ARM system.

Application Services

Messaging Entity (MSG) – a core Windows service that provides the means for the ARM tool to send out SMS messages to the device via 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 Advanced Remote Management 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. This is an auxiliary service that is not required by the Advanced Remote Management application for most Workspace ONE use cases. Once installed, 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 Advanced Remote Management application for the majority of Workspace ONE use cases. Once installed, these services may be disabled in Windows services.

Connection Proctor

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

Troubleshooting Advanced Remote Management

6

If you are having issues with your Advanced Remote Management performance or service, consider troubleshooting your issue before calling support.

These troubleshooting steps address the most common issues with the ARM service.

This chapter includes the following topics:

- Troubleshooting, Generate Certificates
- Troubleshooting, Remote Management Not Available - Device Registration Issues
- Troubleshooting, Issues Connecting to Devices
- Troubleshooting, Modify Database Record for Multi-Node Configuration
- Create the Remote Management CN from the Workspace ONE UEM Database
- Configure Multi-Workspace ONE UEM Environment Support

Troubleshooting, Generate Certificates

While running the "Certificate Seed Script.sql" file in Step 10 of the Generate Advanced Remote Management 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.

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.

There are two possible solutions.

- Run the cert provisioning tool 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.

OR (if the first solution is not possible)

- Manually edit the date format in the SQL script to avoid errors while deploying the script during installation.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.

Troubleshooting, Remote Management Not Available - Device Registration Issues

Many remote management sessions that are "not available" are a result of device registration issues. Review these detailed troubleshooting issues to find a solution.

Advanced Remote Management Link Does Not Display in Workspace ONE UEM

Problem

ARM 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 ARM Hub might not have been deployed properly. ARM Hub might have not been installed on the device properly or registration to ARM Server has failed.

Solution

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

Registration Check Returns Failed

Problem

Device does not register with Workspace ONE UEM or the ARM 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 could 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 MMC certificate console.

Error Message, 'Registration Failed: Server Not Found'

Problem

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

Possible cause 1

ARM Site URL capital and lower-case letters. In Advanced Remote Management 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 Advanced Remote Management site URL. Check the ARM site configuration. You need to ensure that the URL has all lower-case letters. In the example above, the URL should be 'https://rmstage01.awmdm.com'.

Possible cause 2

Firewall is ON but misconfigured. If the firewall is incorrectly configured on the Advanced Remote Management 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, usually hosted on port 443 on the ARM server. If this port is blocked on the firewall, registrations are jeopardized. Turn off the firewall and see if registrations succeed. If they do, check 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.

Troubleshooting, Issues Connecting to Devices

If you are having connectivity issues with your Advanced Remote Management performance or service, consider troubleshooting your issue before calling support. These troubleshooting steps address the most common connectivity issues with the ARM service.

Browser Window Does Not Open Remote Management Portal

Problem

The Advanced Remote Management (ARM) 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 ARM.

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 Remote Management Tool.

- Internet Explorer 11 or later.

- Google Chrome.

- Safari.

Possible Cause 2

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

Solution 2

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

Remote Support Validation Fails

Problem

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

Possible Cause(s): Certificate mismatch, ARM server issues. Client/Server certificates might be incorrectly deployed or there might be issues with availability of ARM server and console.

Solution: Check certificates and ensure ARM servers are operational. Ensure that T10 interface certificate has been properly deployed on the ARM servers, ensure that ARM servers are online and operational.

Troubleshooting, Modify Database Record for Multi-Node Configuration

In order for the Advanced Remote Management 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 may 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 complete the record modification, restart all ARM Servers.

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 Advanced Remote Management Certificates, you can run an SQL script against the Workspace ONE UEM Database to create the Remote Management CN. Use the generated CN to create the root and intermediate certificates for Advanced Remote Management (ARM).

Procedure

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.

What to do next

The Remote Management CN is used to generate the root and intermediate certificates for Remote Management. Proceed to **Step 6** of Generate the Advanced Remote Management Certificates or **Step 3** of Configure Multi-Workspace ONE UEM Environment Support.

Configure Multi- Workspace ONE UEM Environment Support

If you want to operate the Advanced Remote Management server across multiple Workspace ONE UEM environments (not multiple organization groups), then take the following steps. This procedure assumes that you have already completed all the steps in Generate the Advanced Remote Management Certificates.

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

Procedure

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 Advanced Remote Management Certificates.

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 Organization Group Type Functions from the **VMware Workspace ONE UEM Mobile Device Management 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.

    a   If this text box is blank, then you must manually Create the Remote Management CN from the Workspace ONE UEM Database.

4   Switch back to the ARM 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

5   Select **Generate Certificates** button.

6   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 Advanced Remote Management Certificates. This certificate is located in `c:\temp\certs` of the ARM server.

7   In the ARM 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.

8   Repeat this entire step for each additional Workspace ONE UEM environment you want ARM to work with.

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

What to do next

After you have completed installing the client certificate for each Workspace ONE UEM environment, proceed to Configure the Workspace ONE UEM console.