VMware AirWatch Advanced Remote Management Guide

Installing, configuring, and using the Remote Management Service v4.3

Workspace ONE UEM v9.4

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to Advanced Remote Management

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 AirWatch Agent and the Remote Management client installed.

Advanced Remote Management Components

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.

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.
- **AetherPal Tool Controller Service (ACS)** – Acts as a gateway service that maintains a consistent socket connection between the Admin Web Portal and the Connection Proctor. It is instrumental in supporting HTML5 Web portal.
- **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.

- **Anchor Web Service** – provides a single point of entry for all devices for enrollment and authentication services during a session. The Anchor service comprises of the following components.
  - **Device Registration:** Before enrollment, devices are required to register themselves with this service.
  - **Device Enrollment:** Enrolls registered devices with the system.
  - **Software Update:** Devices connect to this service to request client updates. If an update is available, the service provides the appropriate client download link. This component also manages various client packages in the system.
  - **Device Management:** When the enrolled device detects a change, this service provides an interface with which to update its parameters in the ARM Tool such as MDN.
  - **Admin Anchor:** Provides the administration component for the Anchor service.
- **T10 Interface** – 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) is 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 with a messaging gateway, such as Google Cloud Messaging (GCM), or any proprietary SMSC aggregator.

Connection Proctor

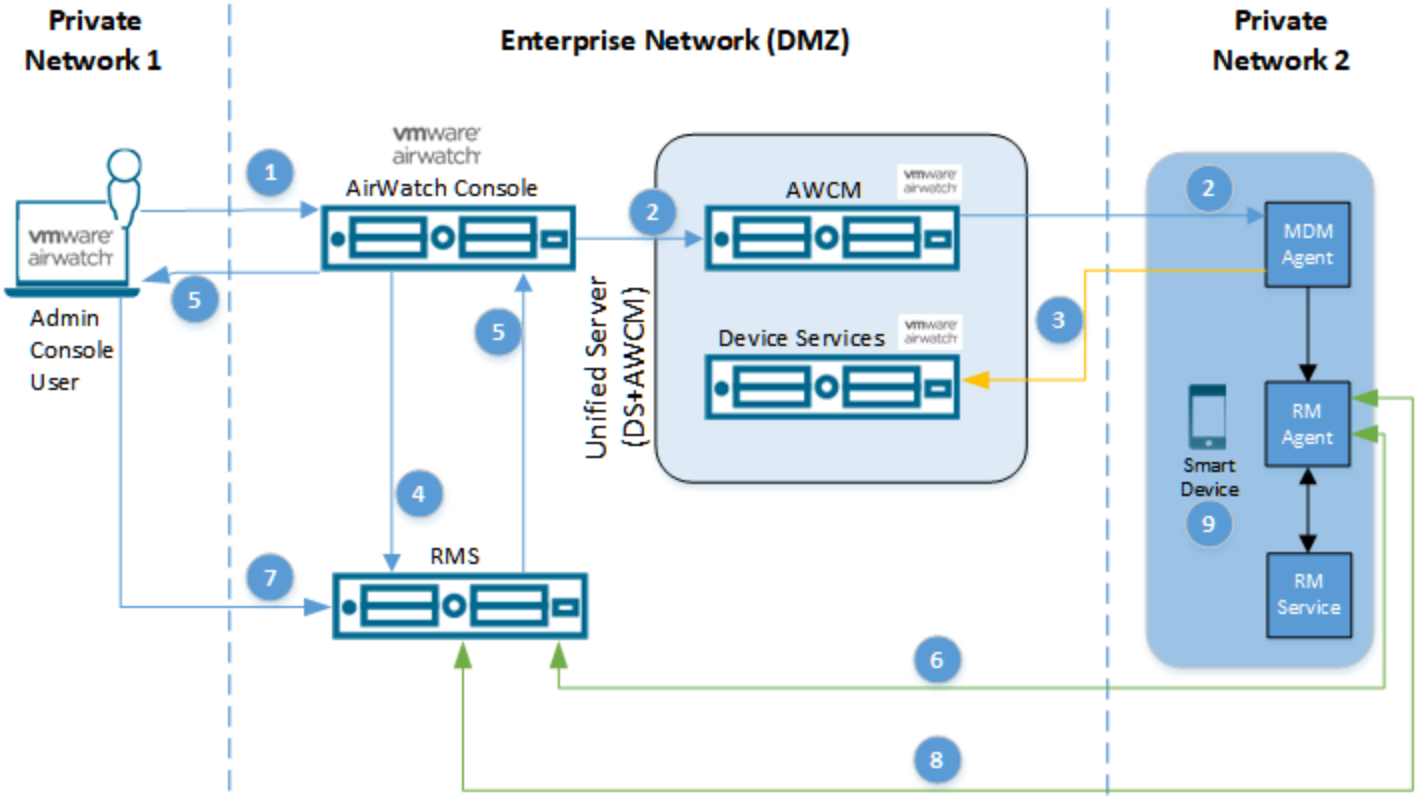
The Connection Proctor component uses the Windows Connection Proctor service to manage device connections to the ARM server. The component also simultaneously handles multiple requests for sessions.

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

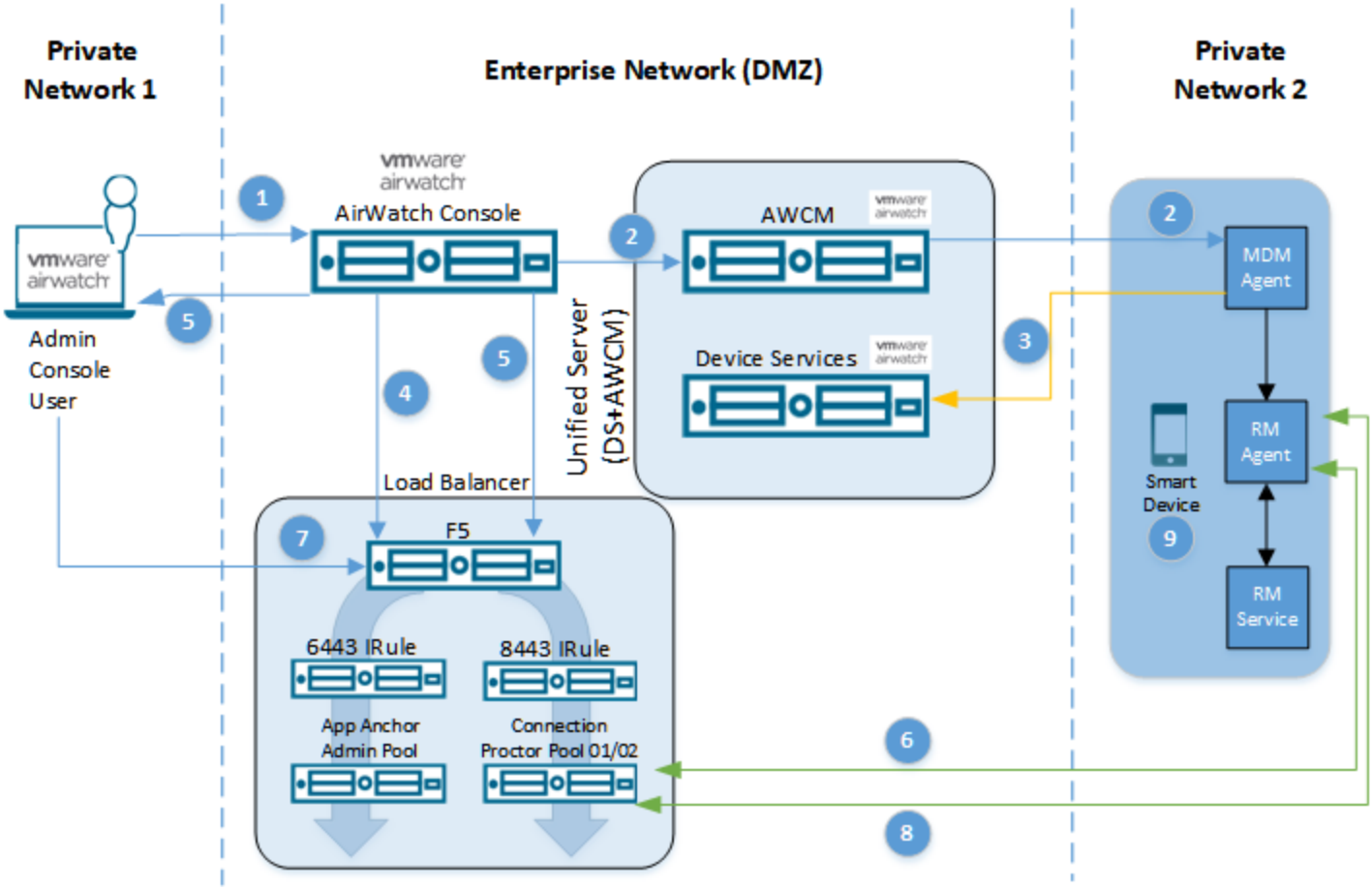
This sample diagram is a typical deployment without the use of a load balancer.



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

With Load Balancer

This sample diagram is a typical deployment that includes a load balancer. For more information, see Load Balancer Overview on page 17.



CAP Servers contain Core Services, Application Services, and Portal Services and can be load balanced.

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

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

Advanced Remote Management Supported Platforms

Advanced Remote Management (ARM) supports Windows Rugged and Android devices running the proper AirWatch Agent and Remote Management service.

ARM supports the following platforms.

- Windows Mobile/CE running .NET 2.0+ with the AirWatch Agent v6.0.40 installed.
- Android devices with the AirWatch Agent v7.0 and greater installed.
  - Samsung Knox Devices – only the personal side of Knox Dual Persona Mode can be accessed by ARM.
  - Android Enterprise (previously known as Android for Work) – only the Work Managed mode running on Android 6.0 or higher can be accessed by ARM.

You must also download the required Advanced Remote Management CAB or APK from the myAirWatch documentation repository.

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 must be met.

Requirements	Minimum
Supported Browsers	Latest version of Google Chrome, Safari, Internet Explorer, or Edge.
Workspace ONE UEM version	Workspace ONE UEM v9.0.2+ with the Workspace ONE UEM Rugged EMM Bundle. Ensure that your version of Workspace ONE UEM includes these features by contacting your account representative.

Active Directory Requirements

If you do not already have Active Directory and a Domain Name Service installed, you can use the included Powershell script file **Install AD_DNS.ps1** which is included in the installer package. For more information, see Install PowerShell Scripts on page 39.

- If you opt to install AD and DNS, then use the included script to do so but make sure you manually **promote this server to a domain controller**. Google the bolded phrase for instructions on performing this task.

ARM requires specific Active Directory users and groups.

Requirement	Description
AD Group	Create an Active Directory group.

Requirement	Description
Portal Admin User	Create a user with the following settings. • First name: **Portal**. • Last name: **Admin**. • Full name: **PortalAdmin**. • User login name: **PortalAdmin**. • Create a password that the user cannot change and which does not expire. • Add this user to the previously created AD Group.

You can automate the configuration of the above settings by running the Powershell script file **Setup AD.ps1**, which is included with the installer. For more information, see Install PowerShell Scripts on page 3 9.

Hardware Requirements

Hardware	Minimum
Remote Management Server	
CPUs	2.4 GHz Processors, 4 Logical Processors, 2 CPU 2 Core 2x2 or 4 Physical depending on machine type VM vs Physical.
Memory	16 GB
Hard Drive IOPS	15,000 SAS minimum
Hard Drive Space	100 GB for OS drive
Remote Management Database Server	
CPUs	2.4 GHz Processors, 4 Logical Processors, 2 CPU 2 Core 2x2 or 4 Physical depending on machine type VM vs Physical.
Memory	16 GB
Hard Drive IOPS	15,000 SAS minimum
Hard Drive Space	200 GB for databases 200 GB for backups and logs
Remote Device Maximum	
Given a single server deployment with the above minimum specifications, the maximum number of concurrent remote device sessions is 250.	

Software Requirements

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

You can automate the configuration of these settings by running the Powershell script file **Install Features.ps1**, which is included with the installer. For more information, see Install PowerShell Scripts on page 3 9.

Requirements	
Remote Management Server	
Operating System	Microsoft Windows Server 2012 R2. Windows Server 2016 is not supported.
Software	Microsoft .NET Framework 4.6.2 Microsoft Report Viewer 2010 Redistributable Package. **Multi-Node Configuration:** the Microsoft Report Viewer 2010 Redistributable Package must be installed where Portal Services are installed.
Server Roles	• Application Server. • Web Server IIS.
Features	• .NET Framework 3.5 Features. ◦ .NET Framework 3.5 (includes .NET 2.0 and 3.0). ◦ HTTP Activation. ◦ Non-HTTP Activation. ◦ IIS Management Console. • .NET Framework 4.5 Features. ◦ .NET Framework 4.5. ◦ ASP .NET 4.5. ◦ WCF Services. ■ HTTP Activation. ■ Message Queuing (MSMQ) Activation. ■ Named Pipe Activation. ■ TCP Activation. ■ TCP Port Sharing. • Message Queuing Services. • Windows Process Activation Service. ◦ Process Model. ◦ .NET Environment 3.5. ◦ Configuration APIs.

Requirements	
Remote Management Database	
Operating System	• Microsoft Windows Server 2012 R2. Windows Server 2016 is not supported. • MS SQL Server 2012 Standard, or MS SQL Server 2014 Standard and Enterprise, or MS SQL Server 2016 Standard and Enterprise. • MS SQL Management Studio 2012. • Microsoft .Net Framework 4.6.2. • Microsoft SQL Server Management Objects (SMO) DLL.
Server Roles	• Sysadmin • Bulkadmin. • Dbcreator.
User Mapping	• Dbowner. • Dbbackupoperator. • SQLAgent dependent. • serverGroup dependent.

Network Requirements

Source Component	Destination Component	Protocol	Port
Workspace ONE UEM console	ARM Server	TCP	443
End-User Devices	ARM Server	TCP	443, 8446
Console User	ARM Server	TCP	443
Remote Management Server	ARM Database	TCP	1433
Remote Management Server	Active Directory	TCP	53, 389, 636
Remote Management Server	ARM Server Note: these ports are internal and within the RMS for service-to-service communication.	TCP	80, 636, 8865, 8866, 8867, 8870, 12780

Security Zones: Private vs. Public

The ARM system is deployed over a single server with two zones, Public/DMZ and Private/Admin. Public zone components include Admin and Anchor Services and Connection Proctor while Private zone components include Database and Data Services. Security zones are separated by hardware and/or software firewalls only allowing specific traffic on specific ports in the prescribed direction.

Internal Ports

The chart below summarizes what ports are utilized by which services.

Port #	Incoming Components/Services	Outgoing Components/Services
53/389/636	Active Directory (AD) Directory Services (DS) Domain Name Service (DNS)	Data Tier Proxy (DTP) Service Coordinator (SVC) Aetherpal Tool Controller (ACS)
80 or 8080 (depending upon your configuration)	Management Services (configurable)	Data Access Proxy (DAP) Management Entity (ME)
1433	Database Server (DB)	Admin/Anchor (ADM/ANC)
8865	Data Tier Proxy (DTP)	Admin/Anchor (ADM/ANC) Management Entity (ME) Connection proctor (CP) Service Coordinator (SVC) AetherPal Tool Controller (ACS)
8866	Messaging Entity (MSG)	Admin/Anchor (ADM/ANC)
8867	Data Access Proxy (DAP)	Data Tier Proxy (DTP)
8870	Service Coordinator (SVC)	Admin/Anchor (ADM/ANC) Management Entity (ME) Connection Proctor (CP)
12780	Connection Procter (CP)	Management Entity (ME)

In a multiple server environment, the servers hosting the components within the private zone occupy their own LAN segment or VLAN without access to the outside world. Ports between servers within the private zone are opened per firewall rules.

Multi-Node Configuration: Install the Connection Proctor component on a sever separate from the server hosting the other components.

Public Ports

Incoming web traffic for Admin/Anchor and the Connection Proctor require that the following ports be open.

443 – Admin/Anchor (ADM/ANC)

8446 – Connection Proctor (CP)

Note: If devices and the CP server are located internally and can access these services, then these ports do not need to be publicly available.

Domain Name Service

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.

You can automate the configuration of these settings by running the Powershell script file **Setup DNS.ps1**, which is included with the installer. For more information, see Install PowerShell Scripts on page 3 9.

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.

Requirement	Description
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
Data Tier Proxy Service Record	• Record type: SRV. • Domain: controlplane.aetherpal.internal • Service: _dtp. • Protocol: _tcp. • Priority: 0. • Weight: 0. • Port number: 8865. • Host Offering this service: admin.controlplane.aetherpal.internal

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.

1. To ensure 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. Run the new installer. The installer prompts you to remove the currently-installed components, excluding the database.
3. Agree to allow the installer to remove the installed components. Once complete, the installer prompts you to install new versions of the same components.
4. Agree to this and let the installer run its course.

Chapter 2 :
Load Balancer Integration

Load Balancer Overview

A load balancer improves the workload distribution across multiple server resources and is valuable in high capacity, high availability environments.

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.

1. When you initially launch the installer which creates the config.installer file, you are presented with the **Database Credentials** screen. For multi-node solutions, you must enter the database server instance *name* or the database server instance *IP address*.

   See **Step 5** in Configure the Advanced Remote Management Installer on page 20.

2. Ensure you delete the Default Website from IIS once the server is running.

   See **Step 8** in Configure the Advanced Remote Management Installer on page 20.

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

4. 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.

   See the **Domain Name Service** section of the Advanced Remote Management Requirements on page 9.

5. 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.

   See Troubleshooting, Modify Database Record for Multi-Node Configuration on page 37.

Chapter 3 :
Install and Configure Advanced Remote Management

Advanced Remote Management Installation Overview

On-premises customers must run the Advanced Remote Management (ARM) installer on a server. SaaS customers do not need to install an ARM server. There are three major steps to installing Advanced Remote Management.

1. The **Generate Certificates** step creates the root and intermediate certificate chain needed by the installer.
2. The **Configure** step creates an install.config file which contains the configuration settings for the different components of the Advanced Remote Management server.
3. The **Install** step uses that install.config file to install the components onto the server.

Generate the Advanced Remote Management Certificates

As part of deploying the Advanced Remote Management (ARM) server, generate the root and intermediate certificates used during installation.

1. Download the installer package, titled **VMware Workspace ONE UEM Remote Management Installer**, from MyAirWatch.
2. 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.
3. Run the Remote Management Certificate Generator which is included in the installer package.
   - Be certain to use the correct version of the tool according to the version of Workspace ONE UEM you are using.

Workspace ONE UEM Version	Certificate Generator Tool Version
Pre 9.2	RemoteManagementCertificateGenerator_Before_9_2
9.2 and after	RemoteManagementCertificateGenerator_9_2

   - This tool must be run on a machine with the same locale settings as the database server to ensure the same date format is set in the SQL script.
   - You must run this certificate generator as an Administrator.
4. In the UEM console, switch to your primary organization group (OG).
   - The OG you choose 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 Guide**.
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** field.
   - If the **Remote Management CN** field is blank, then you must manually Create the Remote Management CN from the Workspace ONE UEM Database on page 37.
6. Set the following values.

Setting	Value
Certificate Type	Remote Management
Deployment	On-Prem
Certificate Common Name	Paste the Remote Management CN copied from step 5 above.

7. Select **Generate Certificates**.
8. Set **Password** for the certificates when prompted. Store this password for future use.
9. Navigate to the folder holding the Remote Management Certificate Generator.
   a. Find the generated certificates file in the Artifacts\ private folder called root_intermediate_chain.p7b.
   b. Copy this file to the c:\ temp\ certs folder on the Remote Management Server. This is the T10 Certificate which is needed later.
      - The T10 interface certificate contains two major certificates that enable Workspace ONE UEM to communicate with the T10 portal. These are the Workspace ONE UEM portal Root and Intermediate certificates in a p7b file.
10. 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 on page 35.

Next, proceed to Configure the Advanced Remote Management Installer.

Support for multiple Workspace ONE UEM environments is available. For details, see Multi-Workspace ONE UEM Environment Support on page 38.

Configure the Advanced Remote Management Installer

The Advanced Remote Management (ARM) installer requires configuring the settings before starting installation. This entails the creation of a config file that the installer requires. You can use this config file to install multiple servers.

1. Install the SSL certificate onto the Personal Certificate Store on the RM server.

   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 8446. You must provide the SSL certificate as a wildcard or SAN certificate.
2. Start the Remote Management installer from the c:\ temp folder on the RM server.
3. Select **Next**.
4. Select **Configure** to configure the server settings before installation.
5. Enter the **Database Credentials**.

Setting	Description
Database Server Name	• For a single server solution, enter the server hostname, IP address, or loopback address. • For a multi-node solution, enter the database server instance name or the database server instance IP address.
DB Owner user name	Enter the user name of the internal ARM Database user that the installation automatically creates in the database.
DB Application user name	Enter the user name of the internal ARM Database user that the installation automatically creates in the database.

6. (Optional) Select the **Advanced** button to configure the Port, LDF, MDF, and NDF paths for the database. Ensure that your Windows account has full access to these folders.

7. Select **Next**.

8. Configure the **Portal Information** settings.

Setting	Description
	Webserver
IP Address	Enter the IP address for the webserver.
Port	Enter the port. The default is 80. Select **check** to validate the port. • If the port is used by a web service, the installer displays Port in use in red. • If the port is not use by any web service, the installer displays Valid! in green. If your IIS Default Website is bound to port 80, then you must either delete the Default Website or use a different port. The suggested replacement is port 8080.
Enable HTTPS Binding	This setting is required. The port defaults to 443.
	Active Directory
Domain Name	Enter your Active Directory domain name.
Group	Enter the Active Directory group created for remote management.
User name	Enter the Active Directory user name created for remote management.

Setting	Description
Enrollment Certificate	
Enrollment Certificate	Select the **...** Button to browse for the EnrollmentCertificate.pfx file, which can be found in the installer package in the c:\temp folder. When you select the certificate, the installer asks for the certificate password which is also included in the installer package in the Password.txt file. **Note:** The enrollment certificate is an SSL certificate that enables remote management devices to enroll or register with the ARM server. The enrollment certificate also secures the connection to the server.

Select **Next**.

9. Configure the **Application Service Information** settings.

Setting	Description
Enable T10 Service	Select to enable the T10 service.
T10 Certificate	Select the **...** button, navigate to the c:\temp\certs folder, and select root_intermediate_chain.p7b.
Auto generate a user in Local Users and Groups	Enable this option to automatically generate a T10 user. If you manually generate a T10 user, you must enter the user name in the provided field.

10. Select **Finish** .

After selecting Finish, the installer creates the install.config file. This file contains all the configuration settings for the ARM installer. When installing on multiple ARM servers, you need to follow this task only once, then export the resulting config file to the other servers.

Next, proceed to Install the Advanced Remote Management Server Components.

Install the Advanced Remote Management Server Components

After running the Configure portion of the Advanced Remote Management (ARM) installer, run the Install portion to install the components.

1. Select **Install** to install the server components after the configuration has completed.
2. Select all components to install on the server.
   - Database
     - The database component is installed remotely based upon the hostname and credentials previously configured in **Step 5** of the Configure the ARM Installer task.
   - Core Services

- Portal Services
- Application Services
- Connection Proctor

3. Select **Next**.
4. Configure the **Datab ase Credentials** settings.

Setting	Description
SQ L Database	
Server N ame	Enter the Database server hostname.
A uth entication	Select the database account authentication. The authentication can be either **Windows Auth entication** or **SQ L Auth entication**.
U ser name	Enter the user name of the database account. This user name is used by the installer to automatically create all the databases required to install Remote Management.
Password	Enter the password of the database account.
A pplication A ccess	
Database Owner Password	Set the 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.
Database U ser Password	Set the password for the ARM database user SQL account. This account does not have system-wide permissions. The account only has permissions within the ARM databases.

5. Select **Next**.
6. Configure the **Auth entication Credentials** settings.

Setting	Description
E nrollment Certif icate Details	
E nrollment Certif icate Password	Enter the password for the enrollment certificate added during the Configuration portion.
A ctive Directory A uth entication	
U ser name	Enter the Active Directory user name.
Password	Enter the Active Directory password.

7. Select **Next**.
8. Configure the **Portal Credentials** settings.

Setting	Description
SSL Certificate	Select the **...** button to browse for the SSL Certificate installed before starting the Configuration portion. 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' .

9. Select **Next**.
10. Configure the **Connection Proctor Credentials** settings.

Setting	Description
CP Binding (Local)	This setting is auto-populated.
Port	This setting is a verification which you can use to check for port 8446.
CP FQDN	Enter the server fully qualified domain name. For example, " rmstage01.awmdm.com"
Port	Enter the actual port number used for the Connection Proctor component. Consider using 8446.
CP certificate	Select the **...** button to browse for the SSL Certificate installed before starting the Configuration portion. This certificate is the same one used on the Authentication Credentials screen in the previous step.

11. Select **Next**.
12. Select **OK** to confirm that you have opened the firewall ports.
13. Select **Next**. The **Execute Resource pack** checkbox option appears. Make sure this checkbox has been enabled.
14. Select **Finish** . The resource pack is then imported automatically.

Next, proceed to Configure the Workspace ONE UEM console.

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.

To configure the UEM console.

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. 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 may be remotely managed.

1. Visit the MyAirWatch page that lists all the device agents (https://resources.air-watch.com/software/device-agents?sort=newest).
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. Next, proceed to Start an Advanced Remote Management Connection.

Chapter 4 : Using Advanced Remote Management

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.

To start an ARM connection.

1. Navigate to **Devices > List View** and select the friendly name of the device you want to create a remote connection with. This 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.
4. The console displays a 4-digit PIN which you must direct the customer to enter into their device. This action provides customer authorization to remotely manage their device.

   Once the connection is made, the remote management client opens and the device is ready for use.
5. There are three supported remote client tools at your disposal.
   a. **Display Capture** – View a remote device's screens, create shortcuts, and diagnose device issues.
   b. **Manage Files** – Access the file system of the remote device.
   c. **Command Line (Android Only)** – Send commands to the remote device using the Command Line Interface (CLI).

Advanced Remote Management Client Tools

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.

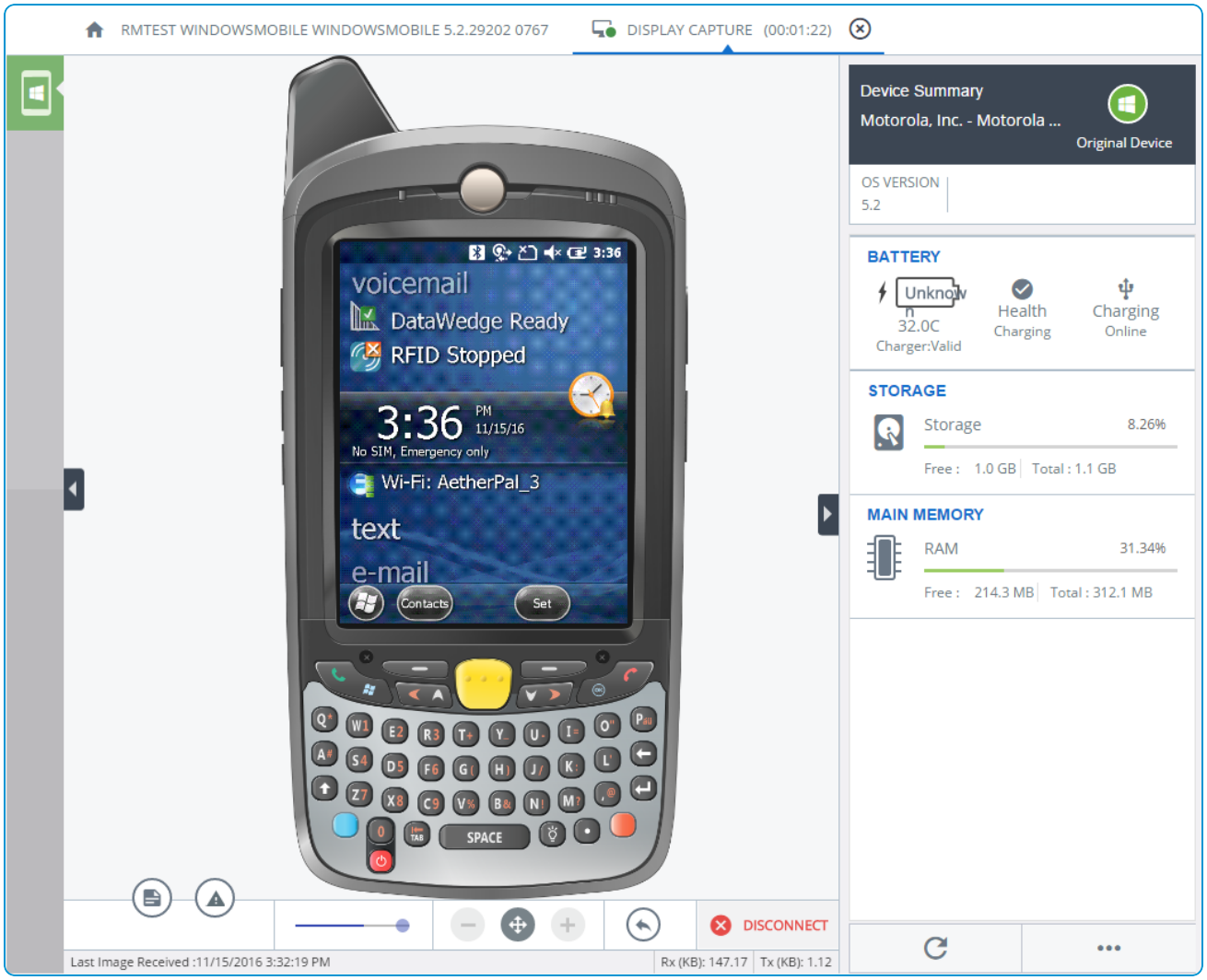
Watch a tutorial video on the ARM client tools: https://support.air-watch.com/articles/115003018507.

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.

Display Capture (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.

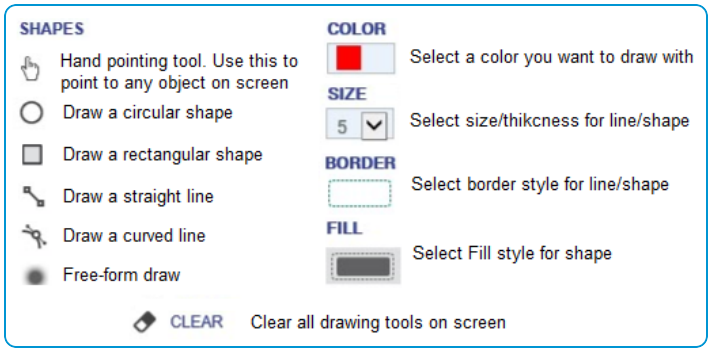
If a user needs privacy, they can pause a remote control session.

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 may 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 kill 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.

Manage Files

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

Upload a File

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

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.

1. In the active ARM session and the Manage Files client tool activated, locate the file on the device you want to download. You may find the " breadcrumbs" style folder path at the top of the file listing a useful navigation aid.
2. Select the **Download** button ( ).
3. 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 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.

1. In the active ARM session and the Manage Files Client tool activated, locate the files you would like to select.
2. Click the checkbox to the left of each file you would like to select.

Cut, Copy, and Paste a File

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

1. Once you have selected the file(s) 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 ARM session and the Manage Files client tool activated, locate the file on the device you want to delete.

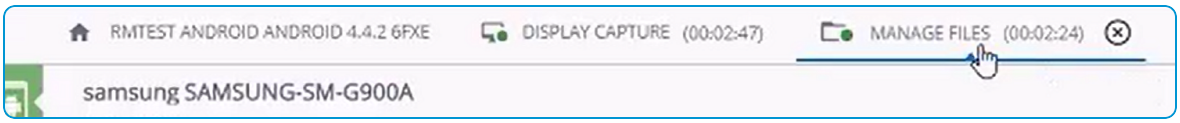
2. Select the **Delete** button ( ).

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.

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 property 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 only show debug level. In a few devices, this command cannot be aborted
logcat * :E	Partial	Prints log data to the screen, filter to only show error level. In a few devices, this command cannot be aborted
logcat * :I	Partial	Prints log data to the screen, filter to only show info level. In a few devices, this command cannot be aborted
logcat * :V	Partial	Prints log data to the screen, filter to only show verbose level. In a few devices, this command cannot be aborted
logcat * :W	Partial	Prints log data to the screen, filter to only show warning level. In a few devices, this command cannot be aborted
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 aborted

CLI Commands	Support Level	Function
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 only show third party packages.
pm list packages -d	Full	Prints all packages filtered to only show disabled packages.
pm list packages -e	Full	Prints all packages filtered to only show 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 only show 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.
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 aborted
touch	Full	Create an empty file or change file timestamps

Chapter 5 :
Troubleshoot Advanced Remote Management

Troubleshooting, Generate Certificates

While running the " Certificate Seed Script.sql" file in **Step 10** of the Generate Advanced Remote Management Certificates task, you may see an error that 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 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 document 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 document.

Troubleshooting, Remote Management Not Available - Device Registration Issues

Advanced Remote Management link does not display in Workspace ONE UEM

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 agent may not have been deployed properly. ARM Agent may 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 ARM agent may be properly downloaded and installed on device. An Workspace ONE UEM Administrator must re-register the device.

Registration check returns failed

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'

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

Possible cause: ARM Site URL capital and lower-case letters. In 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 utilizes upper-case and lower-case letters 'https://rmSTAGE01.awmdm.com'

Solution: Remove upper case characters from Remote Management site URL. Check the Remote Management 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: Firewall is ON but misconfigured. If the firewall is incorrectly configured on the Remote Management Server it may be preventing device registrations from being received.

Solution: Turn off firewall or set up exceptions. When the firewall is on and it is not correctly configured, it may be preventing device registrations. Devices register with the Anchor web service, usually hosted on port 443 on the remote management 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

Browser Window does not open Remote Management portal

The Advanced Remote Management (ARM) portal is not opening on Airwatch users' browser window.

Possible Cause: Incompatible web browser. The browser being used by Airwatch support staff is not compatible with ARM.

Solution: 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 higher
- Google Chrome
- Safari

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

Solution: Enable pop-ups in browser settings. Airwatch users need to update their browser settings to allow pop-ups from the ARM portal.

Remote Support validation fails

During ARM validation steps, one or all of the 3 validation steps and 'Launch Session' button does not appear.

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

Solution: Check certificates and ensure ARM server(s) are operational. Ensure that T10 interface certificate has been properly deployed on the ARM server(s), ensure that ARM server(s) 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 may 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 must be changed.

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 4 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 Remote Management Servers.

Create the Remote Management CN from the Workspace ONE UEM Database

You must 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).

1. Open the Remote Management Certificate Generator. You must run this 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 choose must be a **customer** type, it cannot be of any other type including global, partner, container, and so on.

   For example,

   ```
   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. Proceed to **Step 6** of Generate the Advanced Remote Management Certificates on page 19.

Multi-Workspace ONE UEM Environment Support

If you want to operate the Advanced Remote Management server across multiple Workspace ONE UEM environments, then take the following steps. This procedure assumes you have already completed all of the steps in Generate the Advanced Remote Management Certificates on page 19.

You should not follow this step if you want ARM to work with a single Workspace ONE UEM environment.

1. Log in to the **secondary or other** Workspace ONE UEM environment. Do not log in to the same Workspace ONE UEM environment from **Step 4** in the task linked above.
2. In the UEM console, switch to your primary OG.
   - The OG you choose 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 Guide**.
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** field. If this field is blank, then you must manually Create the Remote Management CN from the Workspace ONE UEM Database on page 37.
4. Switch back to the ARM server. Run the Remote Management Certificate Generator, which comes with 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 above.

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 on page 19. 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.

   For example, if you want to add two additional Workspace ONE UEM environments to the first environment you configured originally, then you would need to follow the steps of this task twice.

9. Once you have completed installing the client certificate for each Workspace ONE UEM environment, proceed to Configure the Workspace ONE UEM console on page 25.

Install PowerShell Scripts

The PowerShell scripts are designed to streamline the Advanced Remote Management server installation. These scripts gather information and create settings on the server.

Take the following steps before running the PowerShell scripts.

1. Log in to the Advanced Remote Management Server as an Administrator.
2. Disable User Access Control (UAC).
3. Install Microsoft .NET Framework 4.6.2.
4. PowerShell commands must be run within an Administrator PowerShell window.

The following PowerShell script files are included in the installer package. They are listed here together but their execution has been prescribed in the Advanced Remote Management Requirements on page 9 section earlier in the guide.

- **Install Features.ps1** – Installs Windows features on the ARM server.
- **Install AD_DNS.ps1** – Installs active directory and domain name service features when both are running on the same server only. This script is only needed if external AD/DNS is not available.
- **Setup AD.ps1** – Configures active directory to work with ARM.
- **Setup DNS.ps1** – Configures domain name service to work with ARM.