VMware AirWatch Remote Management Guide

Installing, configuring, and using the Remote Management Service

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 Remote Management v3.0

The Remote Management Service allows you to connect to end-user devices remotely to aid in troubleshooting and maintenance. The Remote Management Service installs onto a Windows server during the initial AirWatch installation as a go-between for the AirWatch Console and the end-user device.

Remote Management for SaaS customers does not require an on-premises installation. SaaS customers must configure the AirWatch Agent and AirWatch Console settings only for the device platforms they want to use. See AirWatch Agent Configuration for Remote Management v3.0 on page 23 for more information.

On-premises customers must install and configure the Remote Management Service onto a server before using the Remote Management functionality. Hybrid SaaS customers can install their own Remote Management Server.

Remote Management v4.0 is an enhanced version of remote management with more features and functionality. Ensure your version of AirWatch includes these features by contacting your account representative.

Important: VMware AirWatch is preparing Remote Management version 3.0 for its end-of-life event, including last order date, availability, and support. For details about this transition, see https://support.air-watch.com/articles/115016060567. For a viable and advanced replacement, see **VMware AirWatch Advanced Remote Management Guide**, available on Accessing Other Documents.

AirWatch Remote Management Service v3.0 System Requirements

To deploy the AirWatch Remote Management Service, ensure that your system meets the requirements.

Server Requirements

Requirements	Minimum
Hardware	
Physical/Virtual Memory	4-GB RAM
Number of Cores Required	2 Cores
Software	
Server versions supported	Windows 2008/2012
Minimum supported Java version	JRE 1.8 Update 60
General	
Valid SSL certificate and bindings	

Important: Whenever Java Runtime Environment (JRE) updates to the latest version, you must update the environment variables to point to the latest JRE. This environment variable update must occur through a background process or through a manual installation. The TS_JAVA_HOME variable must point to the most recent JRE file path.

For more information on updating Java certificates, see Update the Java Key Store on page 20.

Network Requirements

Your network solution determines the network requirements for remote management. Customize these settings as necessary.

The following table contains the default ports used by the remote management service.

Source Component	Destination Component	Protocol Port
Devices (from Internet and Wi-Fi)	Remote Management	TCP 7779
Console Server	Remote Management	TCP 7779
Remote Management Server	Device Services	HTTPS 443
Remote Management Server	AirWatch Console	HTTPS 443
Remote Management Server	AWCM	HTTP/HTTPS 2001

Admin Computer/Console

The following are the requirements for the computer used to log in to the AirWatch Console.

Requirements	Maximum/Minimum
Admin Desktop/Console	
Supported Browsers	Firefox 32-bit, up to version 51 with admin rights. Internet Explorer 11.
Minimum supported Java version for applet	Java 7+
AirWatch version	• For on-premises customers, AirWatch v8.1.4+. • For SaaS customers, AirWatch v8.2+.

Supported Platforms

The following platforms and OS versions support remote management.

- Android with AirWatch Agent v5.3.1+.
  - Motorola/Zebra MX 1.3+ devices.
  - Samsung with SAFE 4+.
  - Panasonic.
  - Honeywell.
  - Kyocera.
- macOS with AirWatch Agent v2.2+.
- QNX.
- Windows Mobile/CE.
- Windows Desktop.
- Windows 7 with AirWatch Agent v7.2.0+.

Update the Java Key Store

After updating the Java Runtime Environment on your Remote Management server, you must update the Java key store certificates. This process requires admin rights on the server.

1. On the server, navigate to **C:\Program Files\Java\jre1.8.0_65\lib\security** and back up the cacerts file.
2. Copy the cacerts file and paste it into **C:\Program Files\Java\jre1.8.0_65\bin**.
3. Open an administrative command prompt.
4. Enter `SET PATH=%TS_JAVA_HOME%\bin;%PATH`.
5. Change the directory to **%TS_JAVA_HOME%\bin**.
6. Add the root cert to the cacerts file using the following command and substitute the bold values with your values.

```
keytool -import -alias [unique-alias] -file [certfilepath] -keystore cacerts -storepass
changeit
```

Changeit (all lowercase) is the default password for java cert store provided it remains unchanged.

7. Restart the Remote Management Service.

For example, if you want to add a root certificate that was exported to airwatchroot.cer, use the following command.

```
keytool -importcert -file C:/Users/User/Desktop/awrootca.cer -alias CA_ALIAS -keystore cacerts
```

Chapter 2 :
Architecture

Remote Management v3.0 Architecture Overview

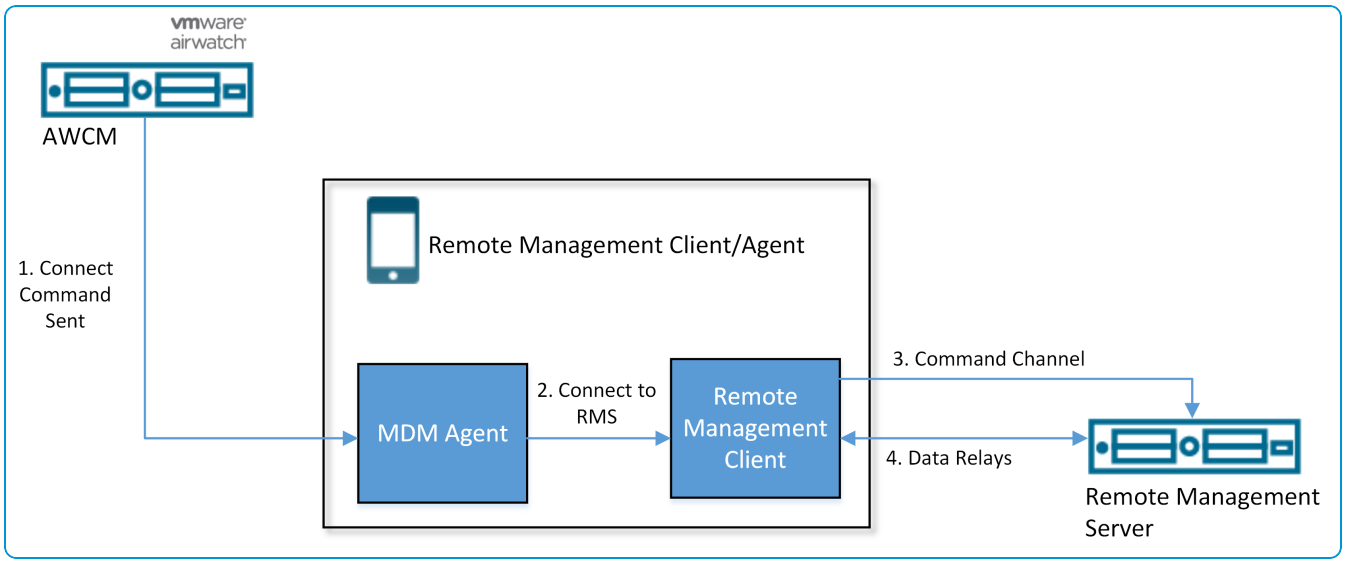
The Remote Management Service brokers connections between the viewers and the Remote Management client on the device that is not directly connected on the same network. This connection requires specific server architecture.

The Remote Management Services meets the needs of IT administrators from a security standpoint by using HTTP(S) protocol and WebSockets. This section illustrates the Remote Management Service architecture focusing on the applet to foster the communication.

Important: Consider using AirWatch Cloud Messaging in your AirWatch deployment, because the AWCM component sends an immediate request to initiate the remote management session. Without the AWCM component, the remote management session does not start until the device checks in with the AirWatch Console using a beacon.

Remote Management Applet Flow in WebSocket Mode

The Remote Management Service uses a browser-based applet to facilitate commands sent from the console user to the end-user device.

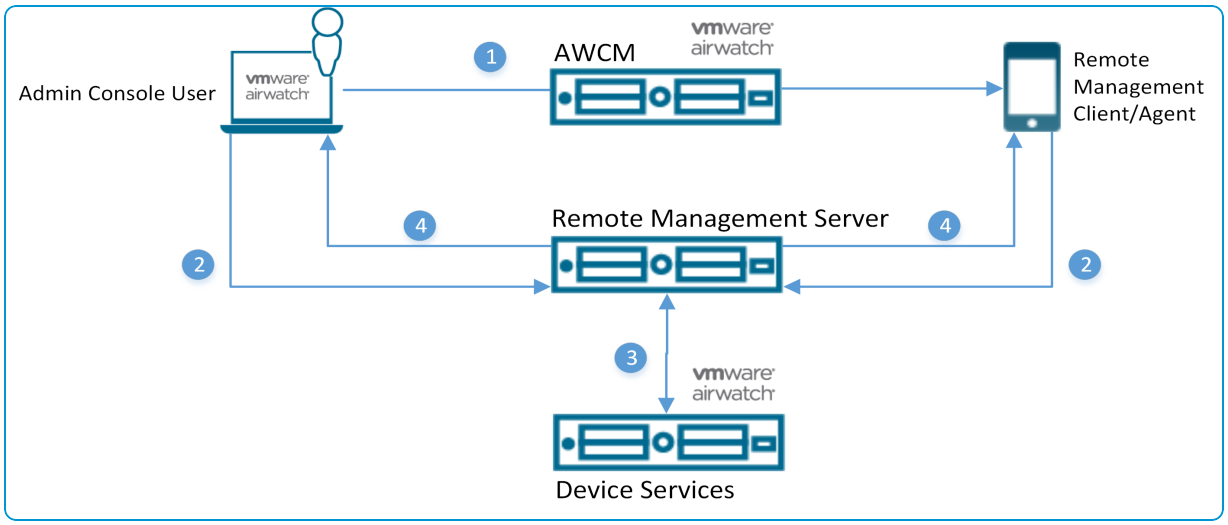


The flow works as follows:

1. The admin starts Remote Management from the AirWatch Console Device Details page. This action sends a Connect Command to AWCM. The Connect Command is sent on to the end-user device.
2. The MDM Agent triggers the Remote Management Client on the end-user device and sends the Connect Command to the Remote Management Server.
3. The RMS server validates the connection with Device Services. Device Services maps the connection to the particular device.
4. The relay between device and applet is completed once the device establishes a data channel connection to the RMS Server.

Remote Management Client Flow

The Remote Management Client does not communicate with the Remote Management Service unless instructed by the MDM agent. The agent states communication in response to an AWCM command sent by the AirWatch Console when Remote Management is launched.



The client flows as follows.

1. The admin starts a Remote Management session. This action starts a connection command through the AWCM to the AirWatch Agent.
2. Both the Web applet on the admin's computer and the tunnel agent on the end-user device send WebSocket connection requests to the Remote Management Server. This connection is called the command channel.
3. The RMS server validates the requests with Device Services.

   Once validated, the command channel remains connected to receive any data connection requests from the AirWatch Console. For every data connection request received through the command channel, the device requests a new WebSocket connection to the RMS server. This connection is called a data session or relay session.
4. RMS validates the relay session and maps the connection to the original applet connection. RMS starts relaying data originating from either endpoints.

If no data channel requests arrive after 5 minutes, the command channel disconnects. This disconnection can result in the server closing all data sessions on the device.

Chapter 3 :
Typical Deployment Scenarios

Typical Remote Management Deployments Overview

This section covers the typical deployment scenarios for WebSocket mode Remote Management. The scenarios included focus on instances where the device and the Web applet are not on the same internal network.

All server URLs used in the sample diagrams are fictitious and are provided for illustration only. From a server perspective, connections are inbound except for cases where the RMS server makes an outbound connection to Device Services. This outbound call validates tokens from the RM client.

Remote Management Deployment Options

You can deploy the Remote Management Server (RMS) in four modes. In most cases the Two Instances (Active – Passive Servers) mode is the preferred method.

The following is a list of the three available modes and a description of each.

1. **Single Instance**

   Single RMS processes all requests. This mode is the simplest configuration.

2. **Two Instances (Active – Passive Servers)**

   Both servers (an active primary server and a passive secondary server) run behind a load balancer. The load balancer periodically checks the health of the primary and secondary servers. If the primary server is deemed to be down, the load balancer switches all the requests to the secondary server until the primary is back online.

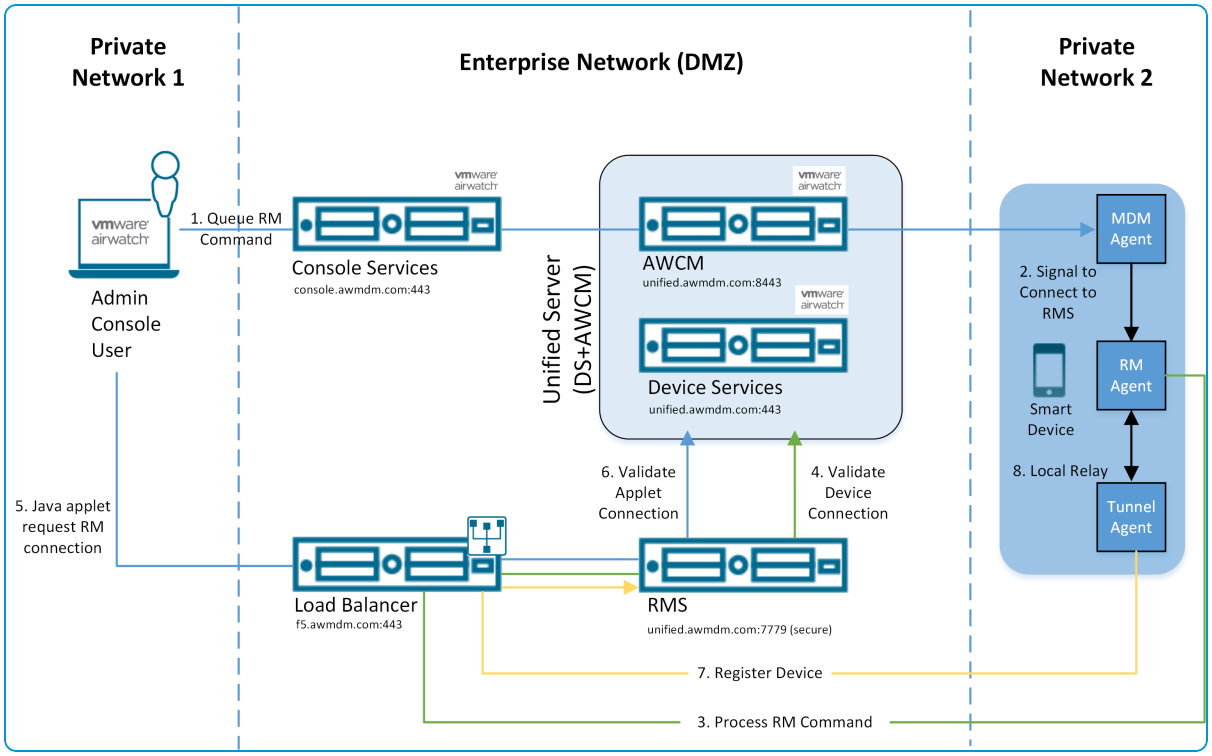
   This method ensures that high availability is maintained. This method is suggested when there is a low number of concurrent RM connections or when the load balancer does not support a persistent session.

3. **Horizontal Scaling with Multiple Instances (Active – Active Servers)**

   RMS instances using session persistence on a load balancer is the optimal solution for maintaining growth and performance. Multiple RM servers run behind a load balancer. Unlike the "active-passive" deployment above, this method is preferred when network traffic from balancing connections between multiple RM sessions is more important than just high availability.

Scenario 1: WebSocket Mode on Disjointed Network using a Load Balancer

There are three typical ways to deploy your remote management server in the AirWatch solution. This scenario describes cases where you want a single point for SSL offloading and horizontal scaling when one RMS server cannot handle the load.



Enterprise Integration Sample Configuration

When configuring the Remote management settings at **Groups & Settings > All Settings > System > Enterprise Integration > Remote Management**, do not configure the RMS server for SSL. The load balancer handles SSL.

The external port in the example is set to the unsecured default 7779 port.

Consider changing the external port to 443 when you install the Remote Management Service on a separate server.

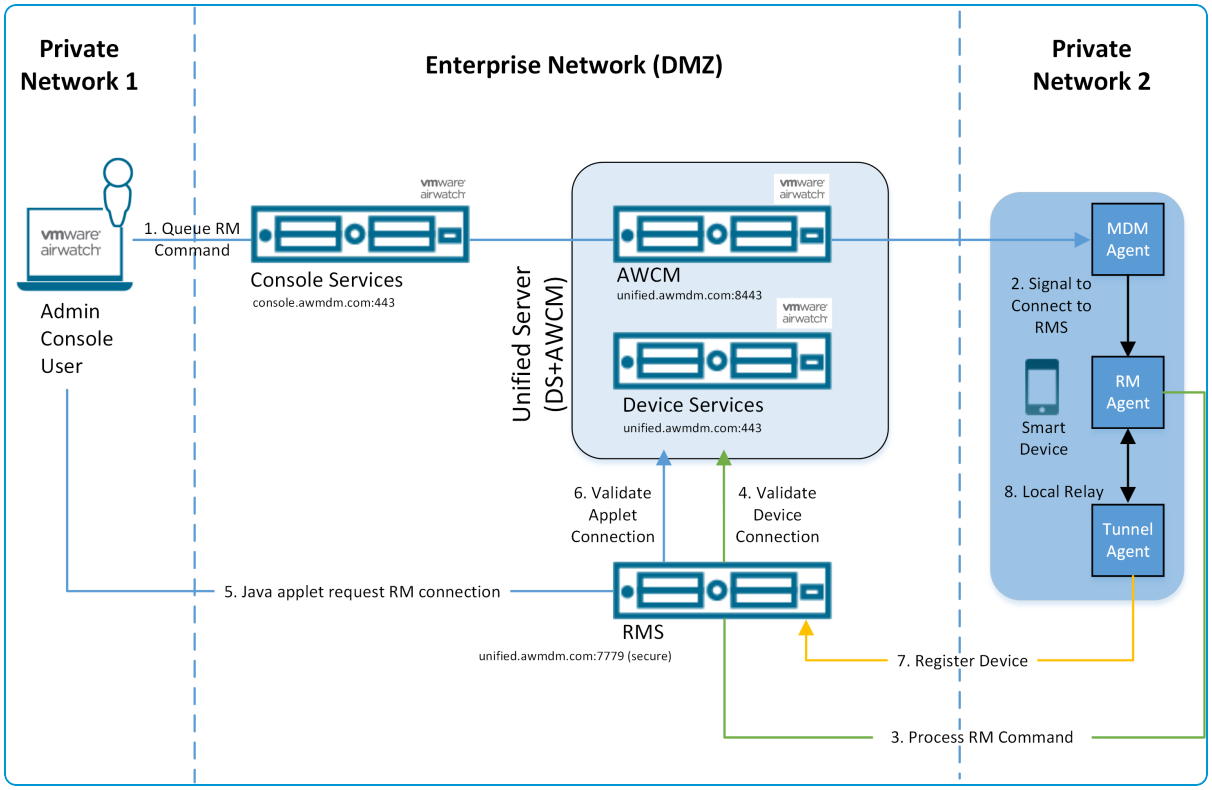
Site URLS

When you configure the Site URLs, you must set the **Remote Management Server URL** to the load balancer URL. In the sample, that is wss://f5.awmdm.com. The **Remote Management Server Port** is set to 443 for the load balancer.

Scenario 2: Web Sock et Mode on Disjointed Network Without a Load Balancer

There are three typical ways to deploy your remote management server in the AirWatch solution. This scenario describes cases where the deployment has a few devices enrolled and no load balancer present to offload the SSL.

In this scenario, horizontal scaling is not required. Usually this scenario is seen in small, on-site deployments.



Enterprise Integration Sample Configuration

When you configure the Remote management settings at **Groups & Settings > All Settings > System > Enterprise Integration > Remote Management**, you must configure SSL for the RMS server.

Consider changing the external port to 443 when you install the Remote Management Service on a separate server.

Site URLS Configuration

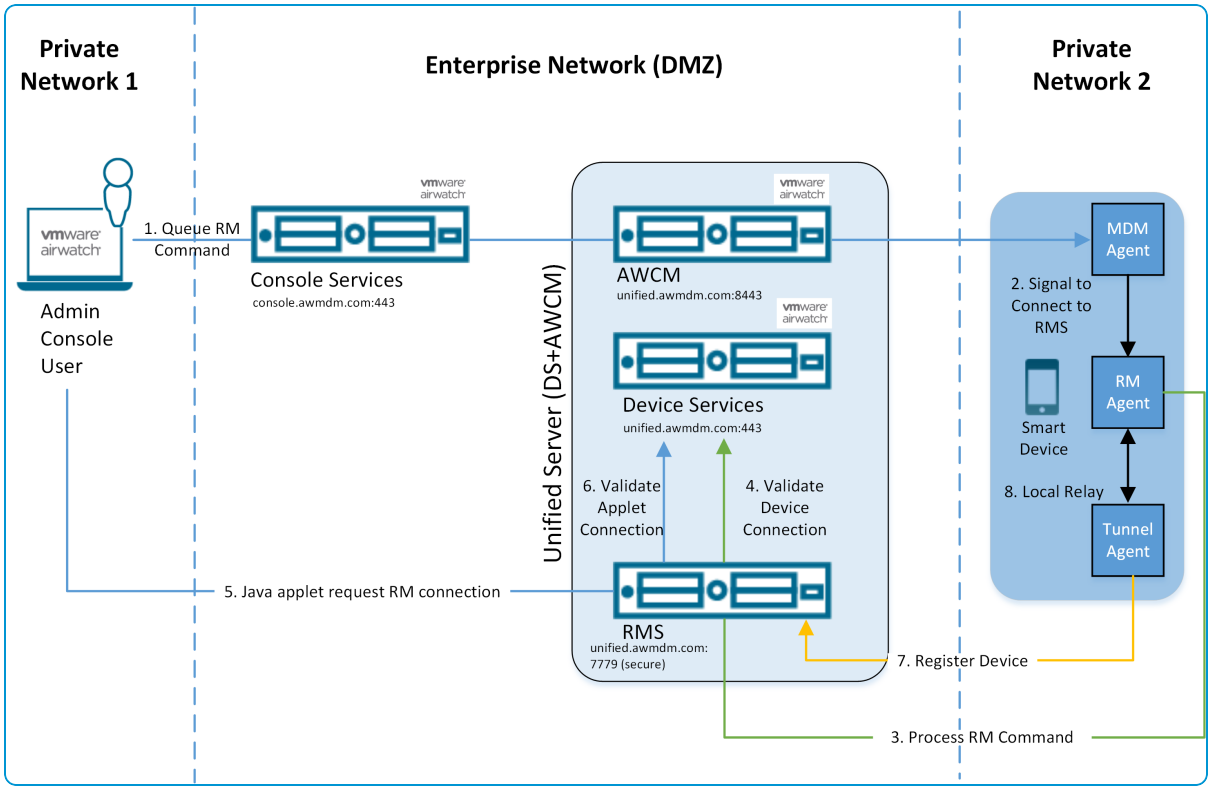
When you configure the Site URLS, the **Remote Management Server URL** must be set to the direct RMS server URL. The **Remote Management Server Port** is set to 7779 because it is the default port.

Scenario 3: Web Sock et Mode on Disjointed Network Without a Load Balancer and Unified Server

There are three typical ways to deploy your remote management server in the AirWatch solution. This scenario describes cases where the deployment uses one server to handle Remote Management, Device Services, and the AirWatch Cloud Messaging.

This model is for deployments that have a few devices enrolled, no load balancer present to offload the SSL, and no requirement for horizontal scaling. Usually this scenario is seen in small, on-site deployments.

Caution: This scenario is not the optimal configuration, as this deployment can lead to performance issues. Consider using separate servers for Remote Management, Device Services, and the AirWatch Cloud Messaging services. Contact AirWatch Support or your Account Representative for more information.



Enterprise Integration Sample Configuration

When you configure the Remote management settings at **Groups & Settings > All Settings > System > Enterprise Integration > Remote Management**, you must configure SSL for the RMS server.

Site URLS Configuration

When you configure the Site URLS, the **Remote Management Server URL** must be set to the direct RMS server URL. The **Remote Management Server Port** is set to 7779 because it is the default port.

Chapter 4 :
Remote Management Service Configuration and Installation

On-premises Deployment of the Remote Management Service

The installation and configuration of the Remote Management Service changes based on your deployment model. On-premises customers must install and configure a Remote Management Server, while SaaS customers need only configure the Agent settings to meet their business needs.

Configuring the Remote Management Service for on-premises deployments requires extra steps to use with your specific deployment. To use the Remote Management Service in an on-premises configuration, you must install the service on a server. Consider installing the Remote Management Service on its own server. Before you install the server, you must configure the installer to communicate with the AirWatch Console.

If you are a SaaS customer who wants to use an on-premises solution for your Remote Management Server, follow the steps detailed in this section.

Consider configuring the installer in the Global organization group (OG). Child OGs inherit settings configured in the Global OG.

Important: A single instance of a Remote Management server can only have one signer certificate per environment. You need one certificate for the Global organization group or any specific child organization group. If you need a separate RMS for the different organization group levels, you must configure separate Remote Management servers for each instance.

Configure the Remote Management Server v3.0 Installer

Before you install the remote management service onto your server, configure the installer in the AirWatch Console. This installer contains all the settings your remote management server requires to communicate with the AirWatch Console.

To create the configuration package, take the following steps.

1. In the AirWatch Console, navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Remote Management**.
2. Select **Configure** to start the remote management setup wizard. If the Configure button is dimmed, select Override to change the Remote Management settings for the Organization Group.
3. On the Configuration Type screen, enter the server **Hostname** and **HTTPS Port**. Select whether the server is **External Facing** or **Behind a Proxy** (load balancer). Select **Next**.
4. On the Details screen, enable SSL Offloading and upload the SSL certificate if applicable.

   Enable this option when the Remote Management Server has its own SSL certificate (and not SSL offloaded from the load balancer). This setting is required in cases where your configuration does not include intermediate entities such as load balancers. If you enable this feature, you must also upload the PFX containing the server certificate and a valid password if the PFX private key is password-protected.

   The Remote Management Server host certificate must be uploaded on the AirWatch Console for whitelisting.
5. If your server is behind a proxy, enter the **Listening Port**. This port is the port where the Remote Management server listens for connections. The default port is 7779.

   If you are using a load balancer, the external port is an approved standard port (typically 443 if no other service is using this port). The external port is then forwarded internally to a different port on the Remote Management Server

(7779 by default but any custom port can be configured). If you are using a non-secured configuration, you can use port 80 (assuming no other service is using this port).

If the RMS server is a node behind a load balancer, you must configure the load balancer to forward all the requests to this external port.

If you use the default port of 7779, you may need to configure an exemption in your firewall.

6. Select **Save**.
7. On the Summary screen, select **Download Remote Management Server Installer**. Depending on your device platform, there may be other steps necessary. These steps are listed on the Summary screen.
8. Enter a **Password** that secures the Signer Certificate and the SSL certificate (if you have enabled Secure Deploy).

Install the Remote Management Service

After completing the configuration wizard, install the Remote Management Service using the installer. Download the installer download from the Remote Management settings page.

IIS is NOT required for the Remote Management Service.

Important: Consider installing the Remote Management Server on its own server. For additional information about the installation process of other AirWatch application servers, refer to the **VMware AirWatch Installation Guide**. For on-premises customers, the Remote Management Service must be installed on a server with which the remote control applet and the device can both communicate.

To install the Remote Management Service, take the following steps.

1. Download the installer from **Groups & Settings > All Settings > System > Enterprise Integration > Remote Management**.
2. Run the AirWatch Installer on the server.
3. Enter the **Certificate Password** you created when exporting the installer from the AirWatch Console.
4. Complete the remaining steps of the AirWatch Installer.

After a successful installation of the Remote Management Service, the Windows Service Applet in the Control Panel will list the AirWatch Remote Management Service. The service does not start automatically after the installation.

Post-Configuration Maintenance for Remote Management

After installing the remote management service, maintain your server using extra tools and settings. These settings are optional depending on your server configuration.

Health Check

After installing the Remote Management Service, you can perform a health check on the Remote Management Service by navigating to <<RMS URL>>/health.

If the RMS is performing as expected, hitting the URL returns a 200 OK.

Log Level

The Remote Management Service is not configured to create debug logs by default. If you require troubleshooting, you can configure the config.xml in the RMS installation folder.

Change the log level to debug by adding the following tag.

< logLevel> 0< /logLevel> .

If you change the config.xml file, you must manually restart the Remote Management Service. The default log level is " info" even if the logLevel tag is not present in the config.xml file.

Load-balanced Remote Management Server

You can deploy the RMS server behind a load balancer. Consider using a load balancer to offload SSL and route traffic to an RMS server configured in non-secured mode.

The load balancer also balances traffic between multiple RMS servers configured for an environment. The address of the Remote Management Service in the Site URLS settings page must be the URL (address and port) of the load balancer. For more information on configuring the Site URLS, see AirWatch Agent Configuration for Remote Management v3.0 on page 23.

If you are using multiple RMS servers behind a load balancer, configure the load balancer for persistence. This setting is required because the applet and the RM client connections must always end at the same RMS node. The applet and the RM client contain a header named **AW-Device-UDID** that includes the UDID of the device. This header is in the applet and RM client initial HTTP request.

For information on setting up an F5 load balancer with Remote Management, see the KB article: https://support.air-watch.com/articles/1150016664 4 8 .

Update the Java Key Store

After updating the Java Runtime Environment on your Remote Management server, you must update the Java key store certificates. This process requires admin rights on the server.

1. On the server, navigate to **C:\Program Files\Java\jre1.8.0_65\lib\security** and back up the cacerts file.
2. Copy the cacerts file and paste it into **C:\Program Files\Java\jre1.8.0_65\bin**.
3. Open an administrative command prompt.
4. Enter `SET PATH=%TS_JAVA_HOME%\bin;%PATH%`.
5. Change the directory to **%TS_JAVA_HOME%\bin**.
6. Add the root cert to the cacerts file using the following command and substitute the bold values with your values.

```
keytool -import -alias [unique-alias] -file [certfilepath] -keystore cacerts -storepass
changeit
```

Changeit (all lowercase) is the default password for java cert store provided it remains unchanged.

7. Restart the Remote Management Service.

For example, if you want to add a root certificate that was exported to airwatchroot.cer, use the following command.

```
keytool -importcert -file C:/Users/User/Desktop/awrootca.cer -alias CA_ALIAS -keystore cacerts
```

Chapter 5 : Remote Management Agent Settings

AirWatch Agent Configuration for Remote Management v3.0

Before you use remote management to connect with end-user devices, configure the AirWatch Agent and AirWatch Console settings for the supported platforms. If your device fleet uses multiple device platforms, you must configure the settings for each related AirWatch Agent in the system settings.

The agent settings control communication between the Remote Management server and the end-user devices.

The remote management viewer has different functionality depending on the device platform. When you start the viewer Java applet to manage a device remotely, the different functions display in the top toolbar.

Configure Remote Management v3.0 for Android

Remote Management allows you to control a device directly to troubleshoot it, or to ensure that a device is properly provisioned. Configure the remote management settings for the Android AirWatch Agent.

Supported Devices

- Motorola/Zebra MX 1.3+ devices
- Samsung with SAFE 4+
- Panasonic
- Honeywell
- Kyocera

Prerequisites

- AirWatch Remote Management Service v2.1 for Android installed on the device.

  Important: You must uninstall the Remote Management Service v1.0 before you install the Remote Management Services v2.1.

- AirWatch Agent v5.3.1 for Android for Remote Management Service v2.1.
- Java 7+ installed on the admin computer to run the remote management applet.

Procedure

Consider configuring these settings in the Global organization group. The child OGs inherit the settings configured at the Global OG.

To configure Remote Management.

1. Navigate to **Devices > Device Settings > Android > Agent Settings**.
2. Under the Remote Management section, complete the following settings related to the use of Remote Management.

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

3. Download the Remote Control .apk from the Resources portal.
4. Deploy the .apk as an internal application sent to devices through AirWatch. For more information on deploying internal applications, see the **VMware AirWatch Mobile Application Management Guide**.

Important: If you use multiple Remote Management Servers in load balance configuration, all HTTPS requests must contain the header " AW-Device-UDID" . Specifying this header ensures the applet and the device reach the same mode. The header must be sent from both the applet and the device.

Use the Android Remote Management v3.0 Viewer

To manage Android devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage Android devices.

To use Remote Management.

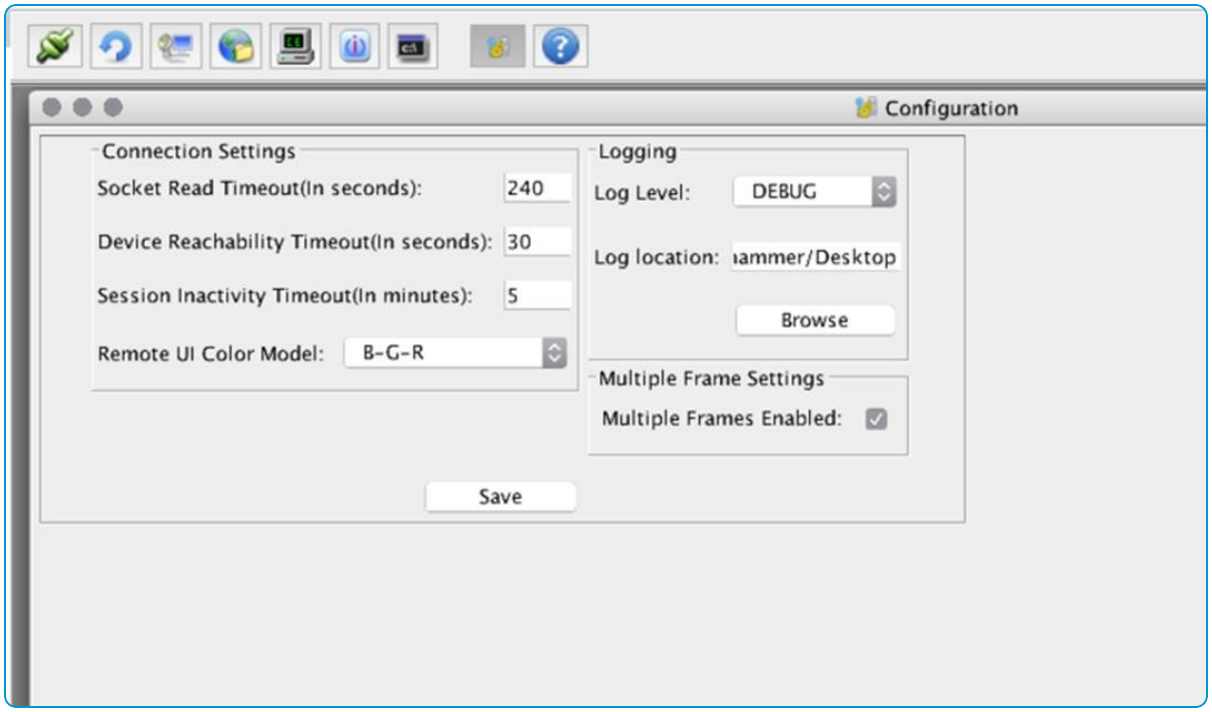
1. Navigate to **Devices > List View** and select the device you want to manage.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish the tasks you want.
   - **Connection** – Shows the connection settings used to communicate with the device.
   - **Retry** – Attempts to connect with the device again.
   - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share**toolbar also allows you to adjust the view depth and size. The toolbar also allows you to capture and save screenshots and videos to your computer. You can also record sequences of actions as macros that can be used again later.

   - **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. Files and directories can also be dragged and dropped between the file system on the device and the remote control admin's machine.
   - **Task Manager** – Displays a list of the processes currently running on the device. Stop or kill a process by selecting the process from the list. You can also start an executable on the device by entering the full path and any parameters to be passed.
   - **Applications** – Displays a list of any applications currently managed by the OS on the device. Uninstall a managed application by right-clicking on the listed application. You may also load a managed application from your local machine and install it to a specified directory on a device.
   - **Command Prompt** – Displays the command prompt. For a full list of supported commands and details, type 'help' into the command prompt and press enter.
   - **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management

applet and the log.

- If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



- **About** – Displays the version information about the remote management applet in use.

5. When you finish your remote management session, select **Cancel** below the applet window to close the connection.

Configure Remote Management v3.0 for macOS

Remote Management allows root control over the file system of a device. Use this access to provide better remote support and troubleshooting assistance on corporate and multi-user devices.

Prerequisites

- AirWatch Agent 2.2+ installed on the client computer.
- The latest version of Java installed on the admin computer to run the remote management applet.

Supported browsers include: Latest stable builds of Safari, Internet Explorer, and Firefox. Consider using a browser other than Chrome due to the limited functionality of Java within its security settings.

Procedure

Consider configuring these settings in the Global organization group (OG). Child OGs inherit the settings configured at the Global OG. To configure Remote Management.

To configure Remote Management.

1. Navigate to **Devices > Device Settings > Apple > Apple macOS > Agent Settings**.
2. Under the Remote Management section, configure the following settings.

Setting	Description
Seek Permission	Accept/decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	Choose extra configuration options.
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for catching the different frames on the device for use with the screen sharing feature. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Choose the number of retries allowed before communication stops.
Retry Frequency (Seconds)	The amount of time between attempts to communicate.
Heart Beat Interval (Seconds)	The amount of time (in seconds) that passes between status updates are sent from the device.
Connection Loss Retry Frequency (Seconds)	The amount of time (in seconds) that passes between attempts to reestablish a connection.

3. Select **Save**.

Use the macOS Remote Management v3.0 Viewer

To manage macOS devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage macOS devices.

To use remote management.

1. Navigate to **Devices > List View** and select the macOS device you want to manage.
2. Display an expanded list of management options on the **Device Details View** by selecting the **More** option ( ).
3. Select **Remote Management**. A Remote Management applet screen appears. If Java is not already installed, a

" missing plug-in" prompt appears in the window.

- **Installing Java with Internet Explorer and Firefox :** Install the latest version of Java by following the prompts. Enable Java helpers to allow Java to run as needed. Before running Java, you may optionally select the check box for " Do not show again" to prevent the application window from appearing again. Last, restart the browser and select**Remote Management** again to continue.
- **Installing Java with Safari:** Install the latest version of Java and " trust" the application by following the prompts. Next, Navigate to the computer's **Apple menu bar > Safari > Preferences**. **Go to Security > Plug-in Settings. Choose Java > Allow**. Option-click the drop-down menu and unselect **Run in Safe Mode**. Return to the AirWatch Console. Consider refreshing the Web page before enabling UI Control.
- Return to the AirWatch Console. Consider refreshing the Web page before enabling UI Control.

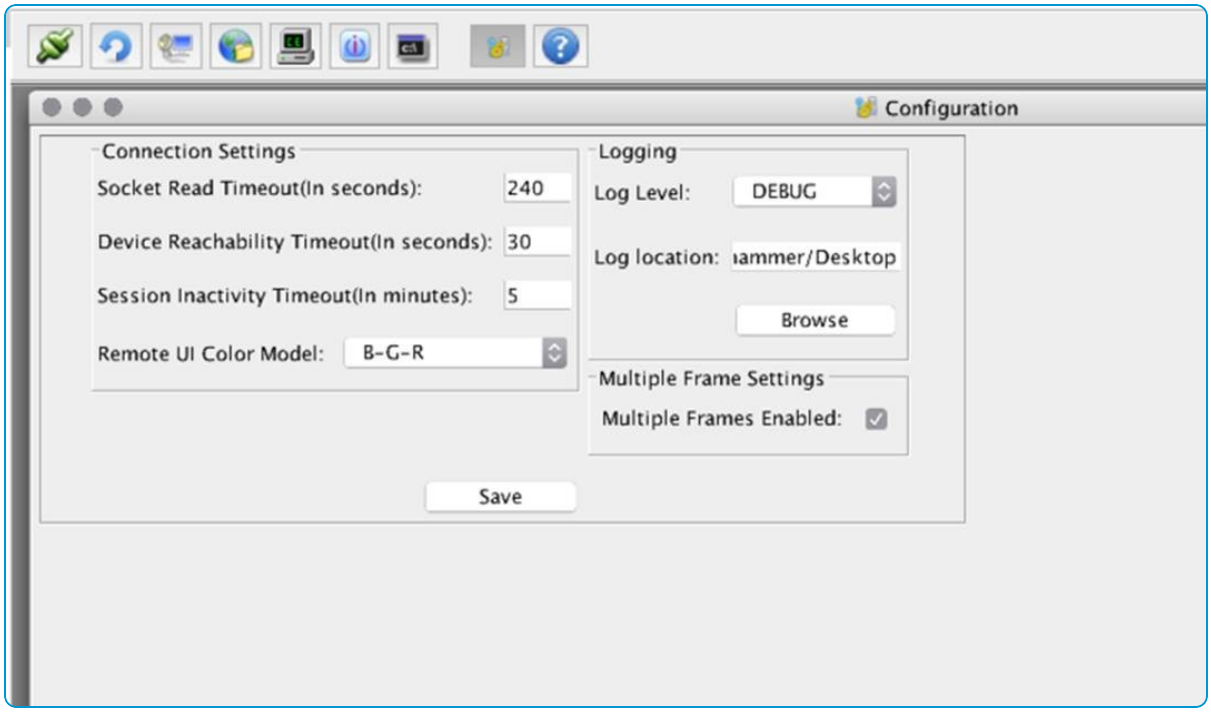
4. Use the Remote Management menu to accomplish the tasks you want.

- **Connection** – View the connection settings used to communicate with the device. Create a direct connection if needed.
- **Retry** – Use this option to reattempt a connection with the device.
- **UI Control** – Start here to view and control the client computer remotely. A representation of the device displays with a tool bar. Use the toolbar to adjust the screen depth and size. Use the Save As button to take a picture. Use the other buttons to take videos and create macros. The red button on the far right releases UI control.

  The bit depth determines the color of the window that displays the client computer. Options range from a 2-bit window display that shows a black and white screen to a 32-bit display that shows a full color window. Choose what is best for performance based on your connection.

- **File Manager** – Manage the device file system remotely to view, create, copy, move, and delete files and directories. The file system on the device is represented at the top of the window and the host machine is at the bottom of the window. Open folders by double-clicking on them. Move files by copy and pasting them.
- **Processes** – Use the activity monitor for the device. Right-click to stop, kill, or refresh processes, and to see active users. Right-click and select **Options** to add more columns for sorting.

  Processes do not refresh by default. Right-click to set up a periodic interval for refreshing.
- **Command Manager** – Use the macOS Terminal, from which you can run scripts and commands.
- **Configuration** – Configure and save the settings for the remote management applet and the log. The default stored location is the home directory.
  - If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



- **About** – On the host computer, view the version information about the remote management applet in use.

5. When you are finished with your remote management session, select **Cancel** at the bottom of Remote Management window to close the connection.

Known Issues

Known issues with taking UI control

- Remote management only works if the end user is logged in to the client device.
- If the login window is displayed on the device, a connection cannot be made.
- The connection drops if the end user attempts to switch users and displays the login window.

Known issues with viewing the UI

- The window that displays the client's computer cannot be resized or seen as a full screen.
- Mouse or trackpad scrolling on the client window does not work. Admins must use the scroll bar on the side of the window.
- Control is only available for the client's main display monitor.
- Recordings are saved in AVI format and cannot be watched using Apple's QuickTime. Instead, these files must be viewed using a multi-platform media Player.

Configure Remote Management v3.0 for QNX

Remote Management allows you to control a device directly to troubleshoot it, or to ensure that a device is properly provisioned. Configure the remote management settings for the macOS AirWatch Agent.

Prerequisites

- Java installed on the admin computer to run the remote management applet

Procedure

To configure Remote Management.

1. Navigate to **Devices > Device Settings > QNX > Agent Settings**.
2. Under the Remote Management section, complete the following settings related to the use of Remote Management.

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.

Setting	Description
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

3. Select **Save**.

Use the QNX Remote Management v3.0 Viewer

To manage QNX devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage QNX devices.

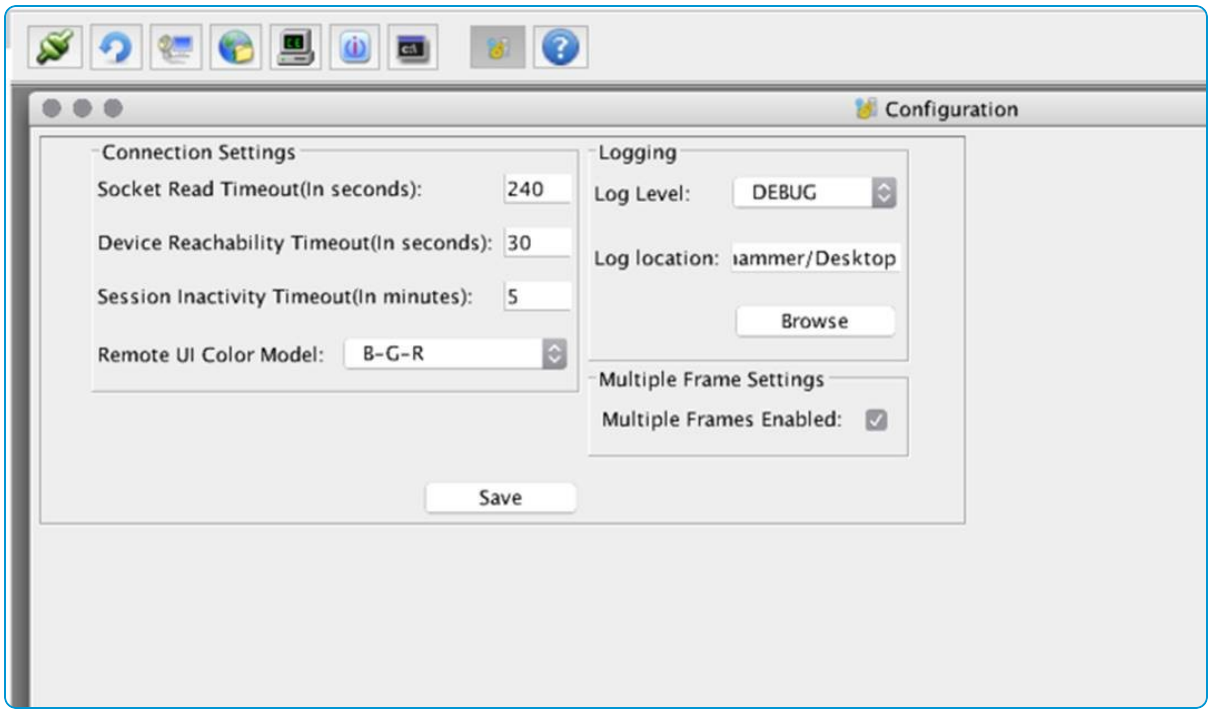
To use Remote Management.

1. Navigate to **Devices > List View** and select QNX.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish the following tasks.
   - **Connection** – Shows the connection settings used to communicate with the device.
   - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share** toolbar also allows you to adjust the view depth and size. The toolbar also allows you to take and save screenshots and videos to your computer. You can also record a sequence of actions (macros) that you can use later.

   - **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. You can also drag files and directories between the file system on the device and the remote control admin's machine.
   - **Command Prompt** – Displays the DOS-like command prompt. For a full list of supported commands and details, type 'help' into the command prompt and press enter.
   - **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management applet and the log.

- If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



5. When finished with your remote management session, select the **Cancel** button located below the applet window to close the connection.

Configure Remote Management v3.0 for Windows Desktop

Remote Management allows you to control a device directly to troubleshoot it, or to ensure that a device is properly provisioned. Configure the remote management settings for the Windows AirWatch Agent.

Prerequisites

- Java 7+ installed on the admin computer to run the remote management applet
- AirWatch Protection Agent installed on the end-user device

Procedure

Consider configuring these settings in the Global organization group. Child OGs inherit the settings configured at the Global OG.

To configure Remote Management:

1. Navigate to **Devices > Device Settings > Windows > Windows Desktop > Agent Settings**.
2. Under the Remote Management section, configure the following settings related to the use of Remote Management:

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

3. Download the AirWatch Agent onto the Windows Desktop device and enroll to begin using remote management.

Use the Windows Desktop Remote Management v3.0 Viewer

To manage Windows Desktop devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage Windows Desktop devices.

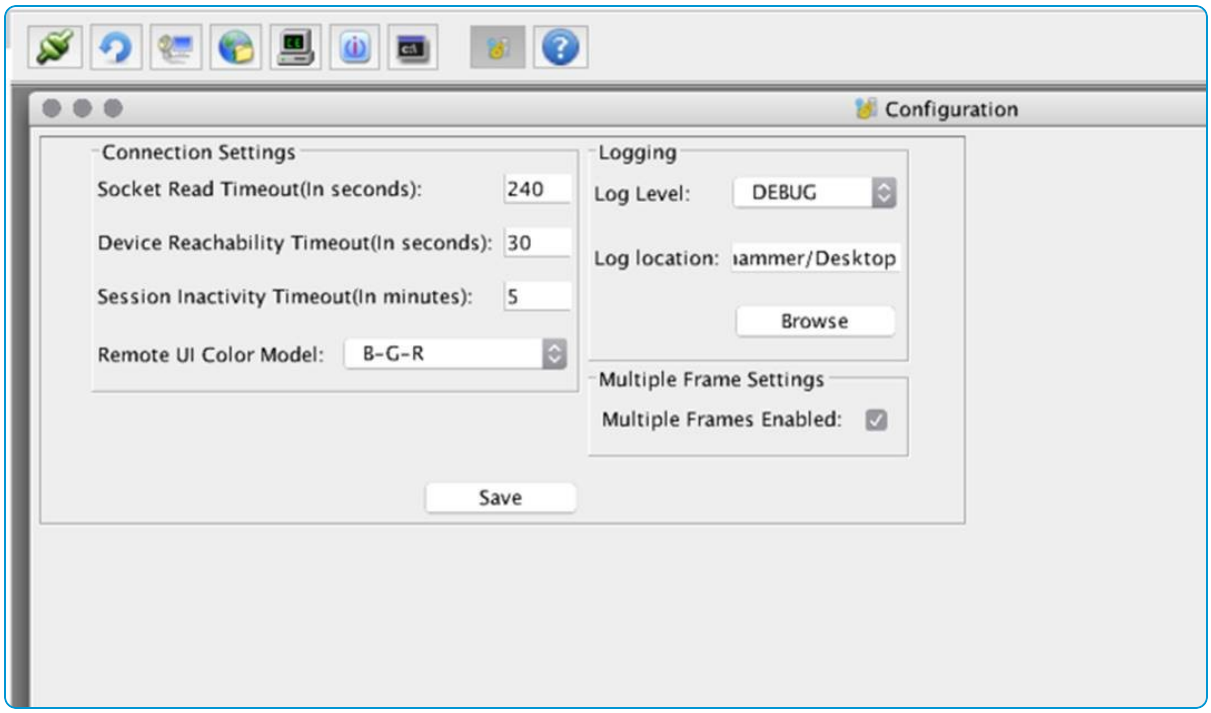
To use Remote Management.

1. Navigate to **Devices > List View** and select a device you want to manage.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish tasks.
   - **Connection** – Shows the connection settings used to communicate with the device.
   - **Retry** – Attempts to make a connection with the device again.
   - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share** toolbar also allows you to adjust the view depth and size. The toolbar also allows you to capture and save screenshots and videos to your computer. You can also record sequences of actions as macros that you can use later.

   - **Registry Manager** – Displays the device registry so you can remotely manage by viewing, creating, editing, and deleting registry keys and values.
   - **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. You can also drag files and directories between the file system on the device and the remote control admin's machine.
   - **Task Manager** – Displays a list of the processes currently running on the device. You can stop or kill a process by selecting that process from the list. You can also start an executable on the device by entering the full path and any parameters to be passed.
   - **Registered DLL List** – Displays a list of the registered.DLLs on the device. Select a .DLL to unregister by right-clicking. Load and register a .DLL from your local machine to a directory on the device.
   - **Device Info** – Displays the information about the device from the remote management applet instead of returning to the Dashboard.
   - **Applications** – Displays a list of any applications currently managed by the OS on the device. Uninstall a managed application by right-clicking on an entry. You can also load a managed application from your local machine and install it to a specified directory on a device.
   - **Display/ Volume Settings** – Displays the configurable display and volume settings on the device.

- **Send Message** – Displays a prompt for a message to be entered that displays on the device-user's screen.
- **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management applet and the log.
  - If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



- **About** – Displays the version information about the remote management applet in use.

5. When finished with your remote management session, select **Cancel**, located below the applet window, to close the connection.

Configure Remote Management v3.0 for Windows 7

Remote Management allows you to control a device directly to troubleshoot or ensure that a device is properly provisioned. Configure the remote management settings for the Windows AirWatch Agent.

Prerequisites

- Java 7+ installed on the admin computer to run the remote management applet
- AirWatch Protection Agent installed on the end-user device

Configuring Remote Management for Windows 7 devices

1. Navigate to **Devices > Device Settings > Windows > Windows 7 > Agent Settings**.
2. Under the Remote Management section, configure the following settings related to the use of Remote Management.

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

3. Download the AirWatch Agent onto the Windows 7 device and enroll to begin using remote management.

Use the Windows 7 Remote Management v3.0 Viewer

To manage Windows 7 devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage Windows 7 devices.

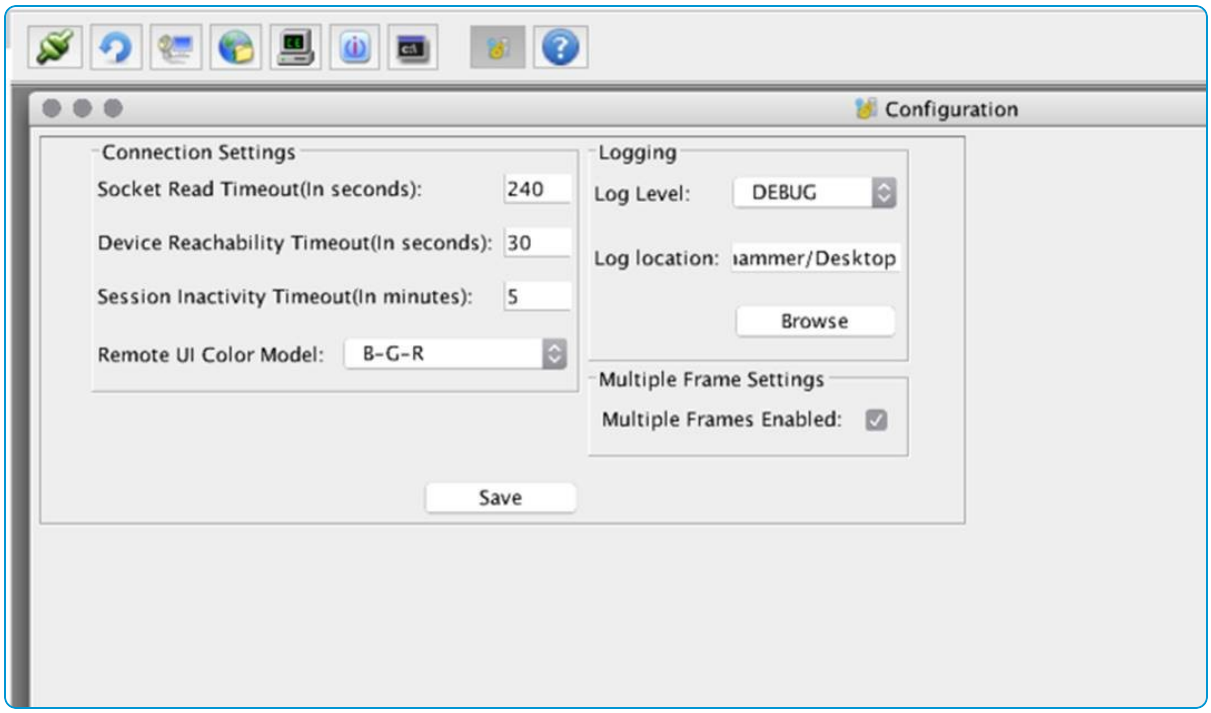
To use Remote Management.

1. Navigate to **Devices > List View** and select a device you want to manage.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens, listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish the tasks you want.
   - **Connection** – Shows the connection settings used to communicate with the device.
   - **Retry** – Attempts to make a connection with the device again.
   - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share** toolbar also allows you to adjust the view depth and size. The toolbar also allows you to take and save screenshots and videos to your computer. You can also record a sequence of actions (macros) that you can use later.

   - **Registry Manager** – Displays the device registry so you can remotely manage by viewing, creating, editing, and deleting registry keys and values.
   - **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. Files and directories can also be dragged and dropped between the file system on the device and the remote control admin's machine.
   - **Task Manager** – Displays a list of the processes currently running on the device. You can stop or kill a process by selecting the process from the list. You can also start an executable on the device by entering the full path and any parameters to be passed.
   - **Registered DLL List** – Displays a list of the registered DLLs on the device. Select a DLL to unregistered by right-clicking. Load and register a DLL from your local machine to a directory on the device.
   - **Device Info** – Displays the information about the device from the remote management applet instead of returning to the Dashboard.
   - **Applications** – Displays a list of any applications currently managed by the OS on the device. Uninstall a managed application by right-clicking on an entry. You may also load a managed application from your local machine and install it to a specified directory on a device.
   - **Display/ Volume Settings** – Displays the configurable display and volume settings on the device.

- **Send Message** – Displays a prompt for a message to be entered that displays on the device-user's screen.
- **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management applet and the log.
  - If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



- **About** – Displays the version information about the remote management applet in use.

5. When you finish your remote management session, select **Cancel** below the applet window to close the connection.

Configure Remote Management v3.0 for Windows Rugged

Remote Management allows you to control a device directly to troubleshoot or ensure that a device is properly provisioned. Configure the remote management settings for the Windows Rugged AirWatch Agent.

Prerequisites

- Java 7+ installed on the admin computer to run the remote management applet.

Configuring Remote Management for Windows Rugged devices

1. Navigate to **Devices > Device Settings > Windows > Windows Rugged > Agent Settings**.
2. Under the Remote Management section, configure the following settings related to the use of Remote Management:

Setting	Description
Download Remote Control Cab	Select this link to download the cabinet (CAB) installer file for Workspace ONE UEM Remote Management.
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	
Remote Management Port	Enter the port used to communicate between the Remote Management Agent and the Tunnel Agent on the end-user device. This port is responsible for caching the different frames on the device for use with the screen sharing function. The default port is 7775. Consider leaving the default setting unless port 7775 is in use for other uses in your organization.
Device Log Level	Set the Device Log Level to control the verbosity of the remote management application on the device.
Log Folder Path	Define the Log Folder Path where the application saves the remote management log file on the device.
Display Tray Icon	Enable Display Tray Icon to show the remote management applet on the device.
Max Sessions	Enter the maximum number of concurrent sessions allowed on a device.
Number of Retries	Enter the number of retries allowed before communication attempts stop.
Retry Frequency (Seconds)	Enter the amount of time between attempts to communicate.
Heartbeat Interval (Seconds)	Enter the amount of time (in seconds) that passes between status updates that are sent from the device.
Connection Loss Retry Frequency (Seconds)	Enter the amount of time (in seconds) that passes between attempts to reestablish the connection.

3. Using a product provisioning, upload the Windows Mobile Remote Management CAB file as a file/action and either:
   - Add it to a staging configuration as an Install file/action manifest item.
   - Add it to a product as an Install file/action manifest item.

Download the Windows Mobile Remote Management CAB file after creating the Remote Management Service Configuration package. If you must download the CAB file again, select **Reconfigure** on the **System > Enterprise Integration > Remote Management** settings page and navigate to the Summary screen.

4. Stage the device or push the product to download and install the application onto the device.

Use the Windows Rugged Remote Management v3.0 Viewer

To manage Windows Rugged devices remotely, start the remote management viewer Java applet. The viewer contains various functions to control and manage Windows Rugged devices.

To use Remote Management.

1. Navigate to **Devices > List View** and select a device you want to manage.
2. On the **Device Details View**, select the **More** option ( ) to display an expanded list of management options.
3. Select **Remote Management**. A new window opens listing the device details and showing the Remote Management window.

4. Use the Remote Management window to accomplish the tasks you want.
   - **Connection** – Shows the connection settings used to communicate with the device.
   - **Retry** – Attempts to make a connection with the device again.
   - **Screen Share** – Displays the device's screen so you can remotely view and control the device screen and receive any actions performed by the device user. The **Screen Share** toolbar also allows you to adjust the view depth and size. The toolbar also allows you to take and save screenshots and videos to your computer. You can also record a sequence of actions (macros) that you can use later.

   - **Registry Manager** – Displays the device registry so you can remotely manage by viewing, creating, editing, and deleting registry keys and values.
   - **File Manager** – Displays the device file system so you can remotely manage by viewing, creating, copying, moving, and deleting files and directories. You can also drag files and directories between the file system on the device and the remote control admin's machine.
   - **Task Manager** – Displays a list of the processes currently running on the device. You can stop or kill a process by selecting the process from the list. You can also start an executable on the device by entering the full path and any parameters to be passed.
   - **Registered DLL List** – Displays a list of the registered DLLs on the device. Select a DLL to unregistered by right-clicking. Load and register a DLL from your local machine to a directory on the device.

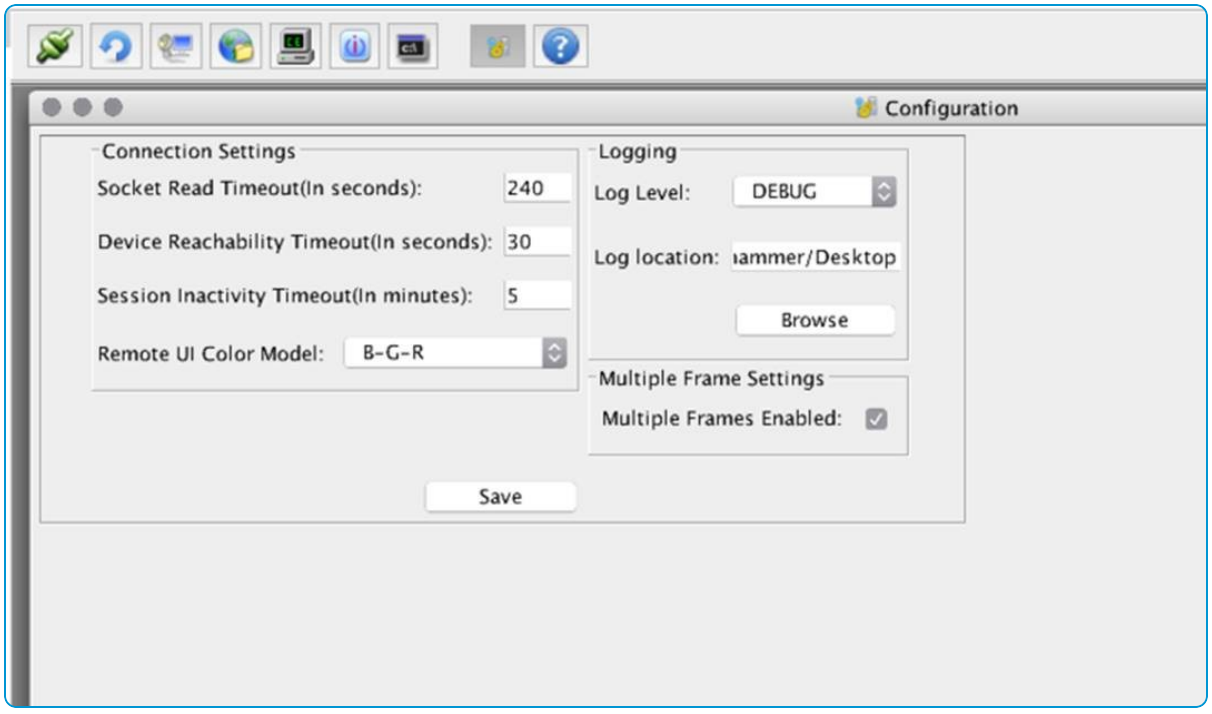
- **Device Info** – Displays the information about the device from the remote management applet instead of returning to the Dashboard.
- **Applications** – Displays a list of any applications currently managed by the OS on the device. Uninstall a managed application by right-clicking on an entry. You can also load a managed application from your local machine and install it to a specified directory on a device.
- **Display/ Volume Settings** – Displays the configurable display and volume settings on the device.
- **Send Message** – Displays a prompt for a message to be entered that displays on the device-user's screen.
- **Command Prompt** – Displays the DOS-like command prompt. For a full list of supported commands and details, type "help" into the command prompt and press enter.

  When running AWS scripts using the command prompt, you must always follow the syntax.

```
Start "\Program Files\AirWatch\awscriptrun.exe" "" "\temp\actual.aws"
```

  You must separate the first portion from the second portion by a space followed immediately by the full file path including AWS script filename. You must surround the AWS script filename with double quotes.

- **Applet Display and Log Settings** – Allows you to configure and save the settings for the remote management applet and the log.
  - If you want to see multiple frames at the same time while using remote management, you must select the **Multiple Frames Enabled** check box.



- **About** – Displays the version information about the remote management applet in use.

5. When finished with your remote management session, select **Cancel** located below the applet window to close the connection.

Configure Remote Management v1.0 Settings

Configure the legacy settings for the on-premises Remote Management Tunnel Server. Consider using the Remote Management Server in WebSocket mode for your remote management business needs.

Installing and configuring the Tunnel Server

1. As part of the AirWatch Installer, select the **Tunnel Server** as a feature to install.
2. Enter the Internal and External ports used to communicate between the Tunnel Server and the AirWatch Console.

Configuring Legacy Agent Settings

The following settings are used to configure platforms to use the legacy remote management system.

1. Navigate to the AirWatch Agent settings for the supported platforms.
   - Rugged Android
   - Rugged Windows
   - QNX
2. Under the Remote Management section, complete the following settings related to the use of Remote Management.

Setting	Description
Mode	Define how the remote management applet and the device communicate over the network. • **Off** – Communication happens directly between the applet and the device. This mode is used when the computer with the applet and the device you want to manage remotely are on the same network or virtual network. • **Inbound** – Communication flows from the applet to the device. There is no direct connection available between the applet and the device. The applet initiates a connection with the tunnel server and the tunnel server communicates with the tunnel agent on the device to establish a connection. This option requires that the device and the tunnel server are on the same network. • **Outbound** – Communication flows from the device to the applet. There is no direct connection available between the applet and the device. The applet and the device both establish connections with the tunnel server proactively.
Enable Encryption	Encrypt the data using AES 128-bit encryption.
Passphrase	Enter a passphrase for the encryption.

Setting	Description
Seek Permission	Enable Seek Permission if you want to prompt the end user to accept or decline the remote management request from the admin. • Enter a **Seek Permission Message** that the end user sees when a remote request is sent. • Enter the **Yes Caption** message for the accept button the end user sees on the Seek Permission request. • Enter the **No Caption** message for the decline button the end user sees on the Seek Permission request.
Advanced	Choose extra configuration options.
Remote Management Port	Enter the Remote Management Port used to communicate between the applet and the device.
Tunnel Agent Port	The port used for communication from the applet to the device. This setting is available when **Inbound** is selected as the **Mode**.
Max Sessions	Enter the maximum number of sessions allowed through Remote Management.
Number of Retries	The number of retries allowed before communication attempts stop. This setting is available when **Outbound** is selected as the **Mode**.
Retry Frequency (Seconds)	The amount of time between attempts to communicate. This setting is available when **Outbound** is selected as the **Mode**.
Heart Beat Interval (Seconds)	The amount of time (in seconds) that passes between status updates are sent from the device. This setting is available when **Outbound** is selected as the **Mode**.
Connection Loss Retry Frequency (Seconds)	The amount of time (in seconds) that passes between attempts to reestablish a connection. This setting is available when **Outbound** is selected as the **Mode**.

3. If you are using **Inbound** or **Outbound** mode, a tunnel server configuration must be defined. Navigate to **Settings > Systems > Advanced > Site URLs**.

   Under the **Remote Management** section, complete the following settings related to the use of Remote Management based on the Mode selected.

   - **Enable Remote Management Server** to allow the applet and the device to communicate with each other.
   - Enter the **Legacy Remote Management External URL** that communicates with device. The URL must be a public facing URL. This URL is used only for an outbound communication where the device must communicate with the tunnel server on a public IP.

- Enter the **Legacy Remote Management External Port** that communicates with device. The default port value is 7779. This port is used only for an outbound communication where the device must communicate with the tunnel server on a public IP.
- Enter the **Legacy Remote Management Internal URL** that communicates with the computer the applet is running on. The URL can be internal or external depending on the networks the applet and the tunnel servers use. This URL is used for both inbound and outbound modes since the applet establishes the connection with the tunnel server in both cases.
- Enter the **Legacy Remote Management Internal Port**that communicates with the computer on which the applet is running. The default value of the port is 7778. This port is used for both inbound and outbound modes, since the applet establishes the connection with the tunnel server in both cases.

4. Select **Save**to complete the configuration.

For information on using remote management, see the specific platform section in AirWatch Agent Configuration for Remote Management v3.0 on page 23.