

VMware AirWatch Upgrade Guide

Upgrading your version of AirWatch

AirWatch v9.3

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Revision Table

The following table displays revisions to this guide since the release of AirWatch v9.3.

Date	Reason
March 2018	Initial upload.

Table of Contents

Chapter 1: Overview	5
Introduction to the AirWatch Upgrade Guide	6
Before You Begin Tasks	6
Before You Begin Notes	8
Upgrade Procedure Checklist	10
Chapter 2: Prepare for Your Upgrade	12
Overview	13
Verify AirWatch Configurations	13
Workspace ONE Install Validation Tool	17
Perform SQL Preparations	17
Stage Upgrade Files	20
Chapter 3: Create Backups for Database and App Servers	21
Overview	22
Back up the AirWatch Database	22
Back up the AirWatch Console and Device Services Servers (if virtualized)	23
Chapter 4: Upgrade VMware Identity Manager	25
Upgrading VMware Identity Manager	26
Upgrade VMware Identity Manager Application Server	26
Upgrade an Identity Manager Server with SQL Server Availability Groups	26
Chapter 5: Start Production Upgrade	28
Overview	29
Disable the World Wide Web Publishing Service	29
Start the AirWatch Application Installer	29
Chapter 6: Upgrade the AirWatch Database	31
Overview	32
Upgrade Database	32

Chapter 7: Upgrade the AirWatch Console and Device Services Servers	36
Overview	37
Upgrade AirWatch Application Servers	37
Chapter 8: Validate the Upgrade	38
Verify AirWatch Services are Running	39
Verify the Upgrade	39
Appendix: Complete the Post Upgrade Checklist	42
Appendix: Performing a Feature Pack Update for AirWatch	45
Procedure	45
Accessing Other Documents	46

Chapter 1:

Overview

- Introduction to the AirWatch Upgrade Guide6
- Before You Begin Tasks 6
- Before You Begin Notes8
- Upgrade Procedure Checklist 10

Introduction to the AirWatch Upgrade Guide

This document discusses how to upgrade your AirWatch infrastructure regardless of your specific topology model. In order to take advantage of the latest features available in AirWatch, you must keep your AirWatch environment up to date with the latest version. As new versions of AirWatch are introduced to the marketplace, you must go through a standard upgrade procedure on your existing AirWatch infrastructure.

Before You Begin Tasks

Complete the preparations below before you begin the upgrade procedure.

Obtain the Latest Version of this Document

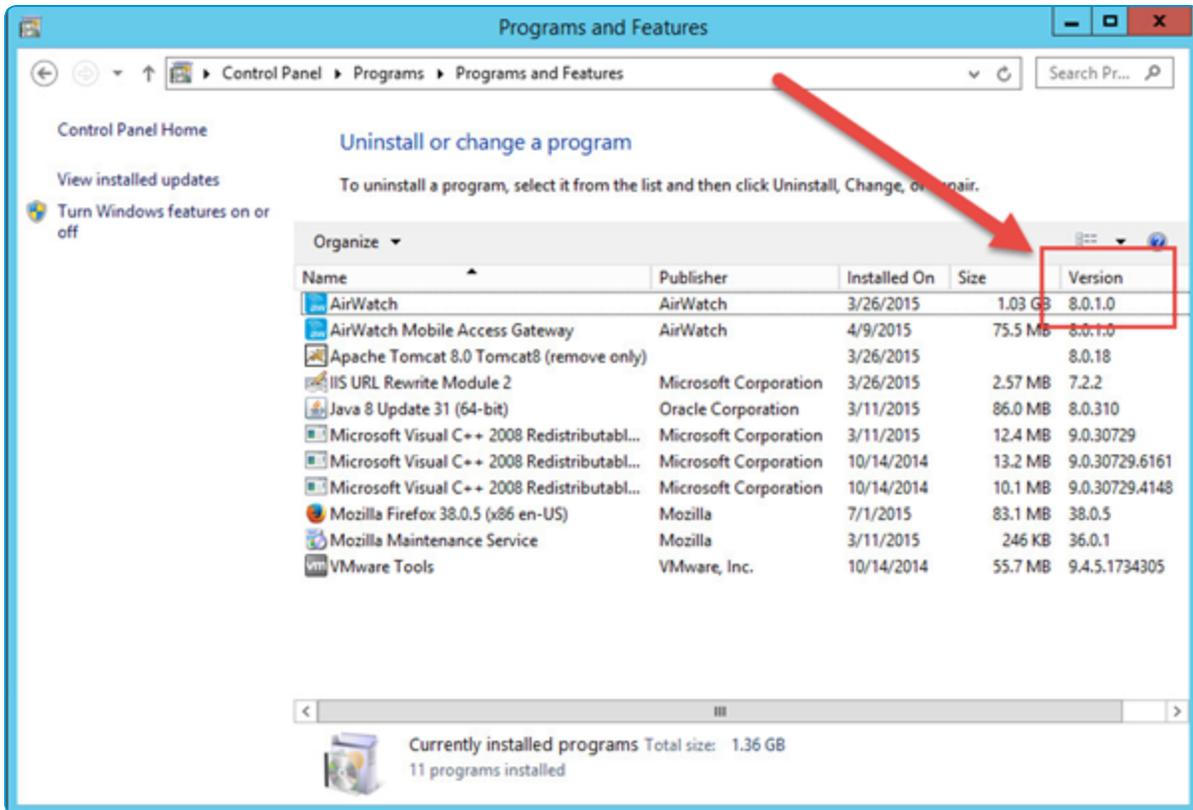
Ensure you are using the latest version of this guide by downloading the latest copy of the document from the AirWatch Resources Portal (<https://resources.air-watch.com>). AirWatch will make updates to these documents from time to time, and having the latest version ensures you are following the AirWatch recommended practices and procedures.

Determine Your AirWatch Version

Determine what version of AirWatch you are running so you can follow the version-dependent instructions in this guide. To determine your version of AirWatch:

1. Log in to the server where AirWatch is installed.
2. Navigate to **Start > Control Panel > Programs and Features** and locate AirWatch in the program list.

The version you are running is listed in the **Version** column.



Your database version, which you may need to know as part of the upgrade process, should be the same as your AirWatch version.

To verify your database version, run the following SQL query: `select * from dbo.databaseversion.`

The screenshot shows a SQL query execution window with the following results:

	MajorVersion	MinorVersion	Revision	Description	VersionDate	Hotfix	CommitID	BuildKey
1	9	2	0	AirWatch 9.2 FP03	2017-11-28 00:00:00.000	3	NULL	NULL

Obtain the Upgrade Package Files

Next, ensure you have downloaded the upgrade package files from AirWatch that are required to perform the upgrade procedure. To do this:

1. Navigate to <https://my.air-watch.com/>.
2. Open the hamburger menu in the top-left corner.

3. Select **Software** and then select **Console**.
4. Search for the installer using the following format: "9.2.X", where X is the FP you want to download. Download both the Patch Installer and the Full Installer packages for the version you have entered.

Note: If you are on AirWatch v9.0 or below: Navigate to **Software > Upgrades** and download the database upgrade package needed to bring the database version up to v9.1. For example, if you are on AirWatch v8.3, download the v8.3 to v9.1 database upgrade package.

Note: AirWatch highly recommends that you retain the latest installer files.

Meet the Requirements

You should meet all of the requirements needed for an AirWatch installation, which are outlined in the **VMware AirWatch Recommended Architecture Guide**. This is because requirements may have changed since you originally installed AirWatch. In addition, if your device count has changed since performing the initial installation please reference this document to ensure your systems are still compatible.

Note: As of AirWatch Version 9.2 we have changed our supported SQL versions. Please check the latest list of prerequisites in the **Recommended Architecture Guide** to ensure your current version is supported.

Note: While it is not required on your database server, .NET is required to run the installer. If you would like to avoid installing .NET on your database server and a potential reboot you can run the installer from one of the AirWatch application servers.

Prepare for Downtime

During the upgrade process, the AirWatch Console, enrollment, and device management will be down. For change window request purposes, the upgrade process typically takes a minimum of four hours. This time may vary based on the size of the database and the number of application servers you are upgrading.

Contact Your On-Call Resources

Before you begin, ensure you have the proper on-call resources available should you need them. This would include technical resources such as the Database Analyst, Change Manager, Server Administrator, Network Engineer and MDM System Administrator.

Before You Begin Notes

Review the information in this section before you begin the upgrade procedure.

Feature Pack Upgrades

If you are performing a feature pack upgrade (for example, from AirWatch v9.2.0 to AirWatch v9.2.1), then refer to the [Performing a Feature Pack Update for AirWatch appendix](#). Otherwise, read the system requirements below and then

proceed with [Prepare for Your Upgrade](#).

Server Topologies

In order to streamline the AirWatch Upgrade Procedure, the document refers to both AirWatch Console Servers and AirWatch Device Services Servers. Before proceeding, it is important to understand each of these components and what they mean to your specific topology model.

- The **AirWatch Console Application Server** refers to the component of AirWatch that renders and displays the AirWatch Console. It is designed to present and send data to the database directly from the AirWatch UI. By default, the API is installed on this server.
- The **AirWatch Device Services Application Server** refers to the component of AirWatch that communicates with all the managed devices. This server executes all processes involved in receiving and transmitting information from devices to other components of the system. By default, AWCM is installed on this server. The Application Server is the AirWatch end-point.
- **For deployments with dedicated API and AWCM servers:** Dedicated API and AWCM servers are considered application servers, similar to the AirWatch Console and Device Services. You should therefore perform the steps below on these servers if you have dedicated servers for these components.

Upgrade Note for Smart Groups

Note that if you have smart groups with over 500 devices when using the **Select Devices and Users** option for smart groups then you will not be able to upgrade until these groups have been limited to a maximum of 500 individual devices. If you encounter a scenario where you must add more than 500 devices while utilizing the **Select Devices or Users** option, consider instead enabling the **Select Criteria** option for that main bulk of devices that share a general criteria and, if required, create multiple **Select Devices or User** smart groups for those devices that fall outside of the general criteria.

Upgrade Note for AWCM

For customers upgrading from Legacy AWCM (AirWatch v6.4–v7.0) to AWCM 6.x (AirWatch v8.0-9.2) and wanting to use explicit clustering, please refer to the following KB article: <https://support.air-watch.com/articles/115001665788>.

For more information about configuring AWCM clustering, see the VMware AirWatch Installation Guide (VMware provides this document to you as part of the on-premises installation process) and the Appendix – Deployment Options section of the **AWCM Guide**.

Upgrade Note for VMware Enterprise Systems Connector

The VMware Enterprise Systems Connector replaces the AirWatch Cloud Connector.

The VMware Enterprise Systems Connector auto-update feature does not function correctly until your VMware Enterprise Systems Connector server is updated to .NET Framework 4.6.2. The VMware Enterprise Systems Connector auto-update feature will not update the .NET Framework automatically. Please install .NET 4.6.2 manually on the VMware Enterprise Systems Connector server before performing an upgrade.

SEG and VMware Tunnel Servers

The VMware Tunnel server requires communication with AWCM to authenticate devices. Because of this requirement, end user devices cannot use the VMware Tunnel during the upgrade process. Because the SEG server is an auxiliary component of the AirWatch architecture that does not communicate with the AirWatch database, it is neither affected

by, nor needs to be altered during the AirWatch Upgrade process. That said, all devices that communicate through the SEG to receive mail will continue to receive mail during the upgrade, provided that the SEG is installed on its own server. Refer to the **VMware AirWatch Secure Email Gateway (SEG)** and **VMware Tunnel** guides for additional information, which are available on [AirWatch Resources](#).

Troubleshooting

You can find several troubleshooting knowledge base articles on myAirWatch by executing the search parameter 'Troubleshooting Upgrades' at the following link: <https://support.air-watch.com/kb/>. The articles you find with this search may help you address issues you encounter during the upgrade.

Upgrade Procedure Checklist

Use this checklist to track your progress as you perform the upgrade steps.

Status (Mark Complete as Needed)	Task
Step 1: Prepare for Your Upgrade	
	Take Note of AirWatch Configurations
	Task: Verify Site URLs
	Task: Validate Directory Service Connectivity
	Task: Check validity of your APNs Certificate
	Task: Verify Reports Functionality
	Task: Verify Require Google Account is Checked at Global
	Verify Hardware Requirements
	Perform SQL Preparations
	Task: Enable Full-Text Search Component (if upgrading from below v7.0)
	Task: Verify SQL User Permissions
	Task: Stage your Installer files on all servers
Step 2: Stop All Websites and Services on All Console and Device Services Servers	
	Stop Application Server Services
Step 3: Backup the AirWatch Database and VM Snapshot the Device Services and Console Servers	
	Back up the AirWatch Database
	Back up the AirWatch Console and Device Services Server (if your servers are virtualized)
	Run the App Server Installer until the "IIS and all services are stopped" prompt appears on each application server
Step 4: Upgrade Your AirWatch Database	

Status (Mark Complete as Needed)	Task
	Upgrade to AirWatch database v8.4, if applicable
	Upgrade to AirWatch database v9.0, if applicable
	Upgrade to AirWatch database v9.1, if applicable
	Upgrade to AirWatch database v9.2
Step 5: Upgrade Each AirWatch Console and Device Services Server	
	Run the AirWatch Application Installer
Step 6: Validate the Upgrade	
	Verify AirWatch Services are Running
	Verify the Installation
	Run any applicable seed scripts.
	Task: Validate Custom Administrator Roles
	Task: Verify Directory Service Settings
	Task: Verify the Site URLs
	Task: Validate GEM Functionality
	Task: Disable Services on Multiple Console Servers
	Complete the Post Upgrade Checklist

Chapter 2:

Prepare for Your Upgrade

Overview	13
Verify AirWatch Configurations	13
Workspace ONE Install Validation Tool	17
Perform SQL Preparations	17
Stage Upgrade Files	20

Overview

The first step of the upgrade process is to take note of your existing AirWatch Console configurations to ensure everything is set up and functioning properly before the upgrade procedure. This also includes verifying you meet the minimum hardware and software requirements and have the appropriate SQL permissions.

Meet the Hardware and Software Requirements

You can find the hardware, software and network requirements in the VMware AirWatch Recommended Architecture Guide. If your device count has changed since performing the initial installation, reference this document to ensure your application and database servers still meet the minimum requirements.

Other prerequisite steps are outlined in the VMware AirWatch Installation Guide (VMware provides this document to you as part of the on-premises installation process).

Important: Do not uninstall current versions of VMware AirWatch software, including Identity Manager and the AirWatch Console. The upgrade process overwrites the relevant files. Uninstalling existing versions deletes previous configurations from your deployment.

Verify AirWatch Configurations

Perform these steps to verify that your AirWatch environment is ready to upgrade.

Task: Verify Site URLs

1. Log in to the AirWatch Console and navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs**
2. Verify the following Site URLs are correct:
 - The **Console URL** should be "https://{CONSOLE_URL}, where {CONSOLE_URL} is the URL of your AirWatch Console Server.
 - The **Device Services URL** should be "https://{AW_DS_URL}/DeviceServices, where {AW_DS_URL} is the URL of your Device Services server.
 - The **REST API** should be "https://{AW_API_URL}/API, where {AW_API_URL} is the URL of your API server.

- For a typical configuration, nothing should appear as "localhost" except for the Google Play Service URL.

System > Advanced >

Site URLs ?

Current Setting Inherit Override

Console URL*	https://acme.mdm.com
MDM Enrollment URL*	https://acme.mdm.com/DeviceManagement/Enrollment
Device Services URL*	https://acme.mdm.com/DeviceServices
Self-Service Portal URL*	https://acme.mdm.com/MyDevice
SAML Authentication URL*	https://acme.mdm.com/IdentityService
SOAP API URL*	https://acme.mdm.com/AirWatchServices
REST API URL*	https://acme.mdm.com/api
App Catalog URL*	https://acme.mdm.com/Catalog
Device Management URL*	https://acme.mdm.com/DeviceManagement
Google Play Service URL*	http://localhost:9001/

Task: Validate Directory Service Connectivity

3. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
4. Select the **Test Connection** button to verify connectivity.

Bind Authentication Type* Anonymous Basic Digest Kerberos NTLM **GSS-NEGOTIATE**

Bind User Name

Clear Bind Password

Bind Password Show

Domain Server

[+ Add Domain](#)

> **Advanced**

Use Azure AD For Identity Services Enabled **Disabled**

Use SAML For Authentication Enabled **Disabled**

Child Permission Inherit Override Inherit or Override

[Save](#) [Test Connection](#) [Start Setup Wizard](#)

Task: Check the Validity of Your APNs Certificate

5. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > APNs for MDM**.
6. Double-check the expiration date of your APNs certificate and ensure it will not occur before the upgrade procedure.

Current Setting	<input type="radio"/> Inherit <input checked="" type="radio"/> Override
Certificate *	Certificate Uploaded
Type	Pfx
Issued to	[Redacted]
Issued by	C=US, O=Apple Inc., OU=Apple Certification Authority, CN=Apple Application Integration 2 Certification Authority
Valid From	3/2/2018
Valid To	3/2/2019
Thumbprint	[Redacted]
Apple ID	[Redacted]
Child Permission *	<input type="radio"/> Inherit only <input type="radio"/> Override only <input checked="" type="radio"/> Inherit or Override

Task: Verify Reports Functionality

7. Navigate to **Hub > Reports & Analytics > Reports > List View** and try running a report (for example, Admin User Roles) to ensure reports are working correctly.

Task: Verify Require Google Account Is Checked at Global

8. From your Global organization group, navigate to **Groups & Settings > All Settings > Devices & Users > Android > Agent Settings**.

9. Confirm that **Require Google Account** is Enabled.

Devices & Users > Android >

Agent Settings

Current Setting Inherit Override

General

Heartbeat Interval (min)*

Data Sample Interval (min)*

Data Transmit Interval (min)*

Profile Refresh Interval (min)*

Require Google Account Enabled Disabled

Require Phone Number Enabled Disabled

Block User Unenrollment Enabled Disabled

Workspace ONE Install Validation Tool

Before you begin the upgrade process, use the Workspace ONE Install Validation Tool to verify that your system and components are properly configured.

For more information about the Install validation tool, see the [VMware AirWatch Installation Guide](#).

Perform SQL Preparations

Perform these steps to verify that your AirWatch database is ready to upgrade.

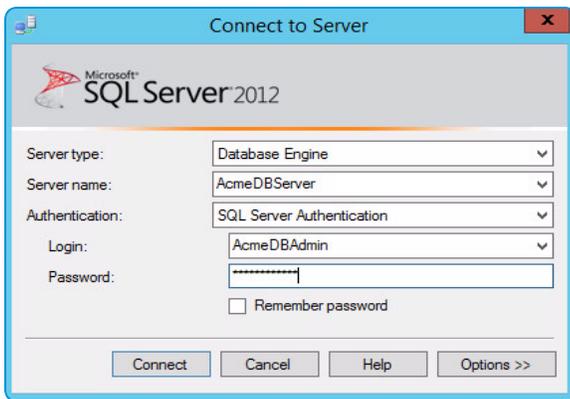
Task: Enable Full-Text Search Component (If upgrading from a version below 7.0)

If you are upgrading from AirWatch v7.0 or higher, then this feature should already be enabled. The Global search function of the AirWatch Console uses full text search indexes and requires the appropriate service to be running on the SQL server. Ensure this component is running on your SQL instance.

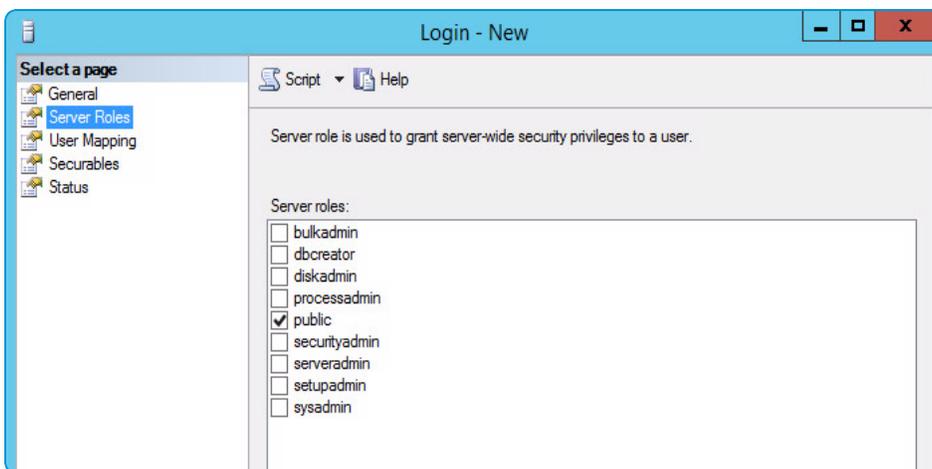
For instructions on enabling the Full-Text feature, see the 9.2 or earlier version of the VMware AirWatch Upgrade Guide .

Task: Verify SQL User Permissions

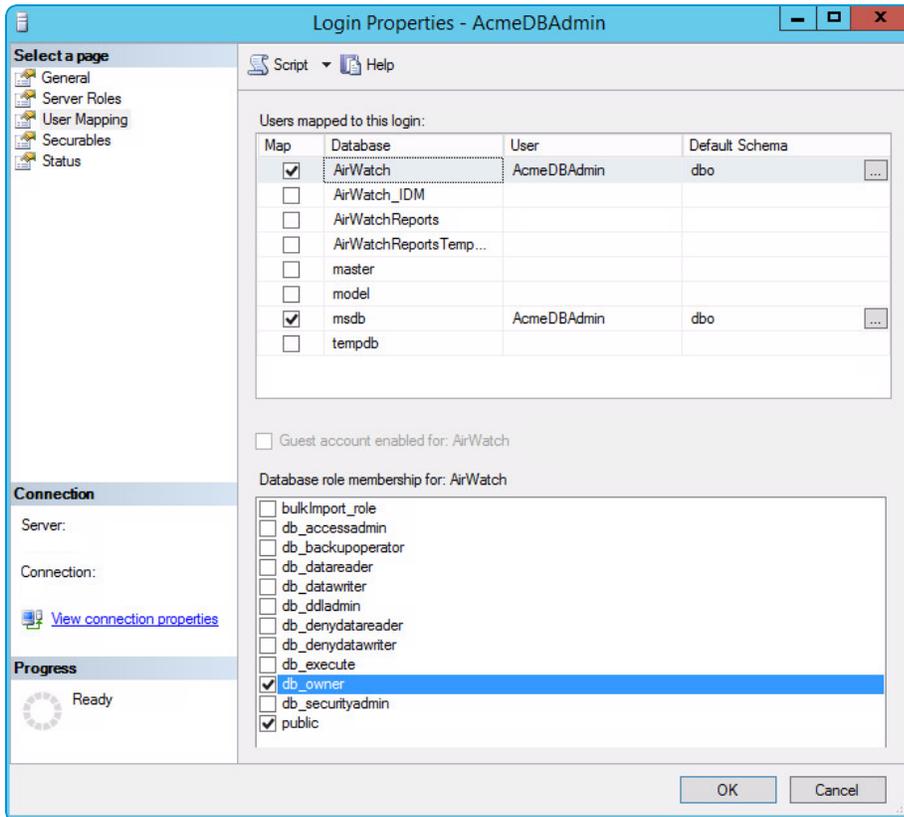
1. Open SQL Server Management Studio.



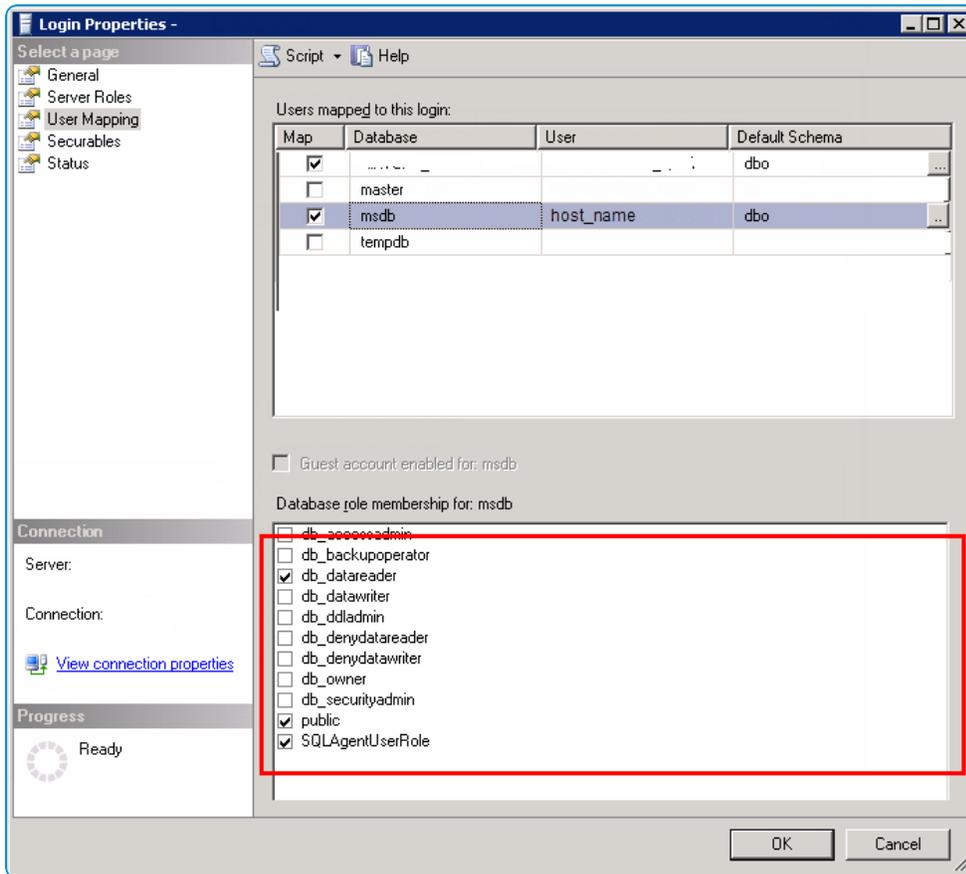
2. Log in to the DB server containing the AirWatch database.
3. Locate your DB user in the Object Explorer by navigating to **Security > Logins > {Your DB User}**, right-click, and select **Properties**.
4. Navigate to the **Server Roles** tab. Verify that the selected server role is **Public**.



5. Select **User Mapping**.
 - Select the AirWatch Database. Then, verify that the **db_owner** role is selected.
For a successful upgrade, you must ensure that the SQL User you are planning to run the AirWatch Database install with has the database **db_owner** role selected.



- Select the msdb database. Then, verify that the **SQLAgentUserRole** and **db_datareader** roles are selected.



Stage Upgrade Files

After performing the necessary preparatory steps, you can stage all the unzipped installer files on their appropriate servers. Place the files (in .zip format) that you downloaded from the Resources Portal on the following servers, then extract the contents:

- All AirWatch Application servers
- All AirWatch Database servers

Chapter 3:

Create Backups for Database and App Servers

- Overview 22
- Back up the AirWatch Database 22
- Back up the AirWatch Console and Device Services Servers
(if virtualized) 23

Overview

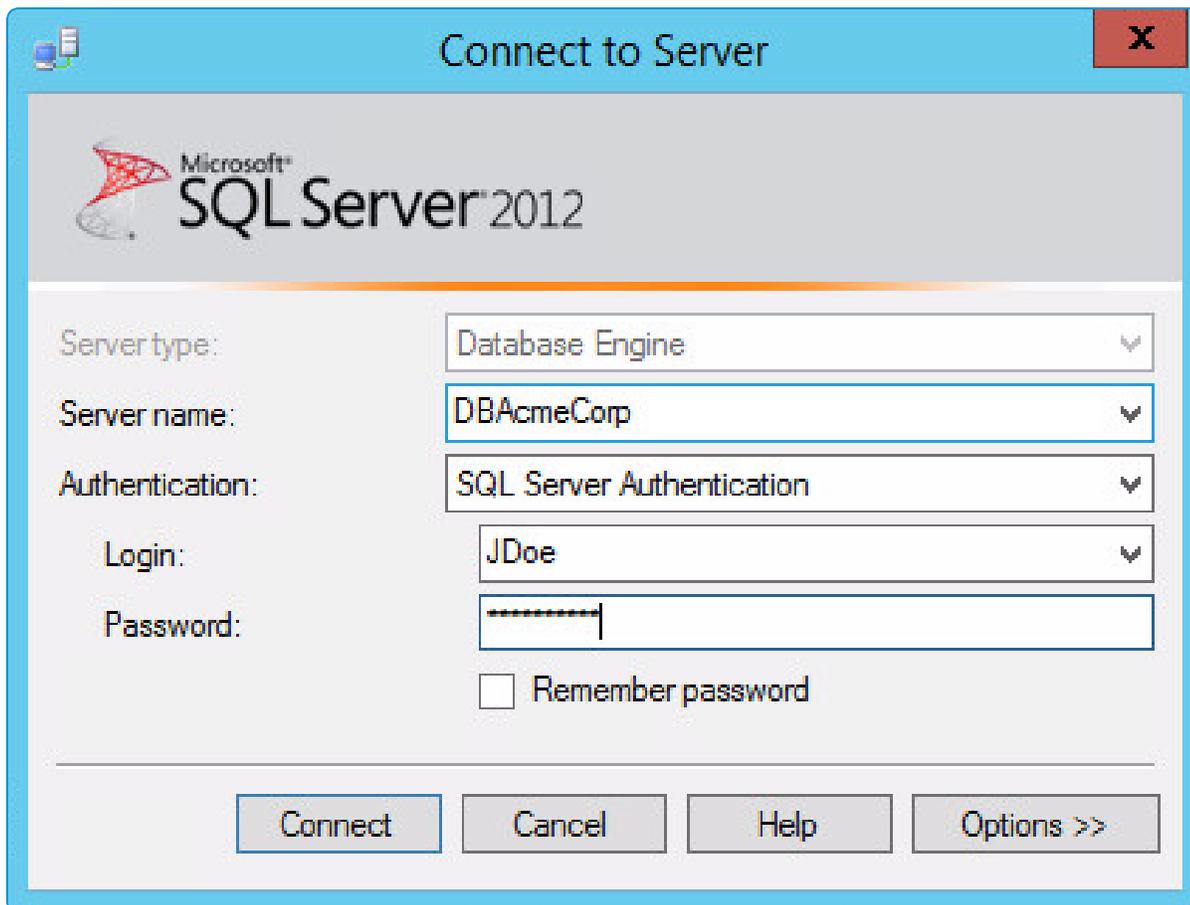
After stopping the appropriate services, you are ready to perform a back-up of your components. This ensures you have an effective restore point should you need to roll back your deployment at any time.

Caution: AirWatch does not automatically back up your servers as part of the upgrade process. Please contact your server vendor to follow the best recommended practice for backing up your servers. The following sections offer some basic guidance but your procedures may vary. You are responsible for creating backups of your AirWatch servers. Failure to do so can result in unrecoverable data loss.

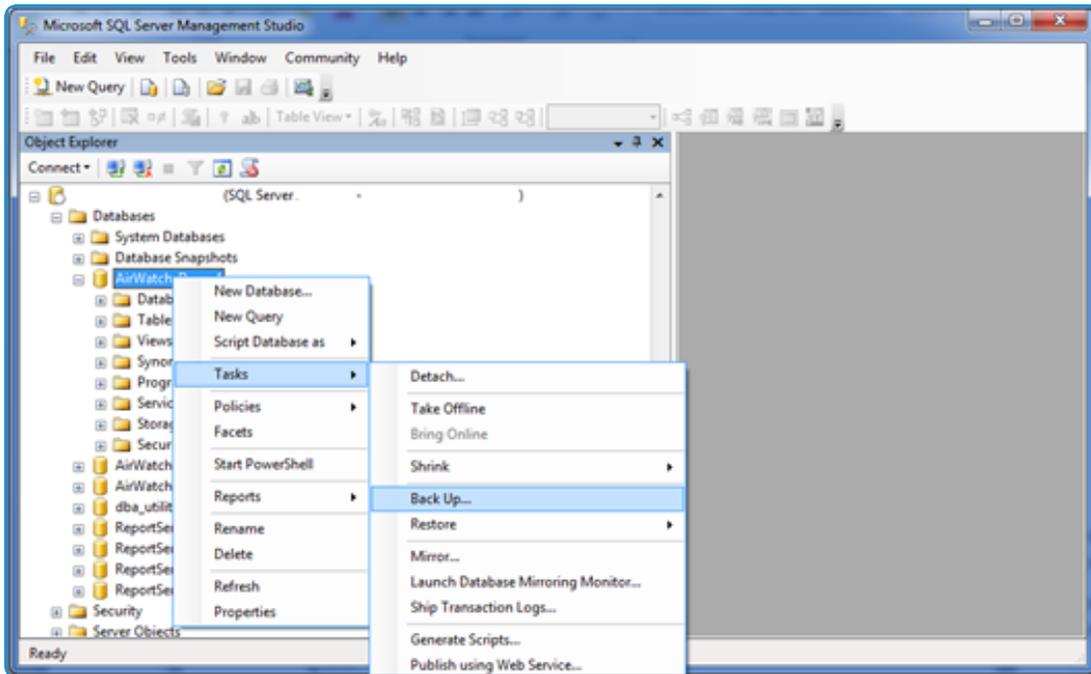
Back up the AirWatch Database

Perform a database backup in case your upgrade fails or you need to restore it later.

1. Make sure to [stop all the AirWatch services and websites](#).
2. Open the **SQL Server Management Studio**.



3. Log into the DB server containing the AirWatch database.
4. Find the AirWatch database in the Object Explorer on the left, right-click and choose **Tasks > Backup**.



5. Specify a backup location and type, and then select OK to complete the database backup.

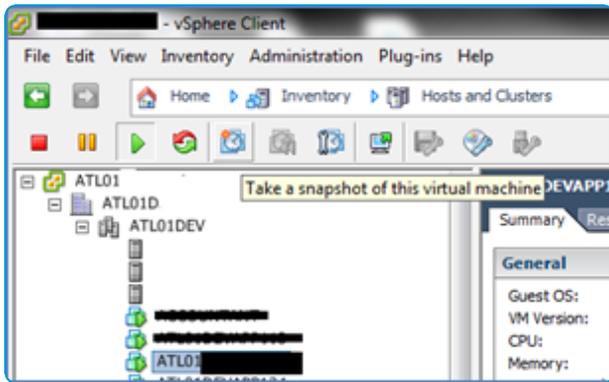
Back up the AirWatch Console and Device Services Servers (if virtualized)

Perform an app server backup in case your upgrade fails or you need to restore them later.

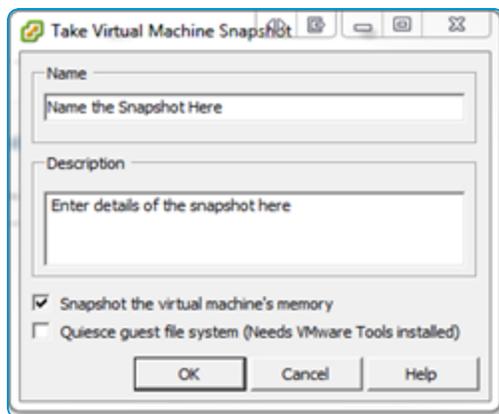
1. Open up the **VMware vSphere Client** and log-in.



2. Locate and select the AirWatch Console or DS server on the left, then press the **Take a Snapshot** button at the top.



- Specify a snapshot name, description, and then make sure:
 - **Snapshot the virtual machine's memory** is checked
 - **Quiesce guest file system** is unchecked



Chapter 4:

Upgrade VMware Identity Manager

Upgrading VMware Identity Manager	26
Upgrade VMware Identity Manager Application Server	26
Upgrade an Identity Manager Server with SQL Server Availability Groups	26

Upgrading VMware Identity Manager

To maintain version compatibility between VMware Identity Manager and VMware AirWatch, upgrade your Identity Manager Application server to the latest version.

You can upgrade the Identity Manager Application Server to the latest version (3.1) directly from version 2.9.1 (included in AirWatch v9.1 package).

For specific compatibility information, see https://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php.

These topics cover upgrading application servers running Windows. For information about upgrading VMware Identity Manager on Linux, go to <https://docs.vmware.com/en/VMware-AirWatch/9.2/identitymanager-upgrade.doc/GUID-58C1E237-86CF-4DD8-ACC6-0D761218E15B.html>.

Upgrade VMware Identity Manager Application Server

If your deployment includes VMware Identity Manager, upgrade this component first using the following steps.

1. Stop Windows Identity Manager Services for all the servers in your cluster.
2. On the first server in the cluster, run the **AirWatch Application 9.2.X Full Install.exe** by right-clicking and running as administrator. The installer detects a previous version of Identity Manager and prompts you to upgrade it.

This upgrade also upgrades the Identity Manager database simultaneously. Wait for this step to complete before proceeding.

To complete the Identity Manager upgrade:

- Provide the SQL database username and password.
 - Confirm the External and Internal hostnames for ports are correct, and adjust if necessary.
 - If you are using a Windows User to run the service, provide the password to confirm any changes.
3. Once the Identity Manager upgrade is complete on the first server, run the upgrade on subsequent servers using the process in Step 2.

You can run upgrades on multiple servers simultaneously once the first server upgrade is complete.

4. Restart one server at a time using a Windows reboot until all the servers are restarted.

Upgrade an Identity Manager Server with SQL Server Availability Groups

To upgrade a VMware Identity Manager Server equipped with SQL Server availability groups, you must disable availability groups before you upgrade the server. After the upgrade, you must re-enable availability groups.

1. Before you install the Identity Manager upgrade, log in to the SQL server as **sysadmin** and disable availability groups using the following command:

```
USE master;
ALTER AVAILABILITY GROUP avlgrp REMOVE DATABASE vIDm;
```

2. Upgrade the Identity Manager Server as usual.

For more information about installing the Identity Manager Server, see [Upgrade VMware Identity Manager Application Server on page 26](#).

3. Once the installation is complete, log in to the SQL server as **sysadmin** and re-enable availability groups using the following command:

```
USE master;  
ALTER AVAILABILITY GROUP avlgrp ADD DATABASE vIDM;
```

4. Run the following command to resync all the secondary nodes.

```
ALTER DATABASE [TestDB] SET HADR AVAILABILITY GROUP = [TestAG];
```

Chapter 5:

Start Production Upgrade

Overview	29
Disable the World Wide Web Publishing Service	29
Start the AirWatch Application Installer	29

Overview

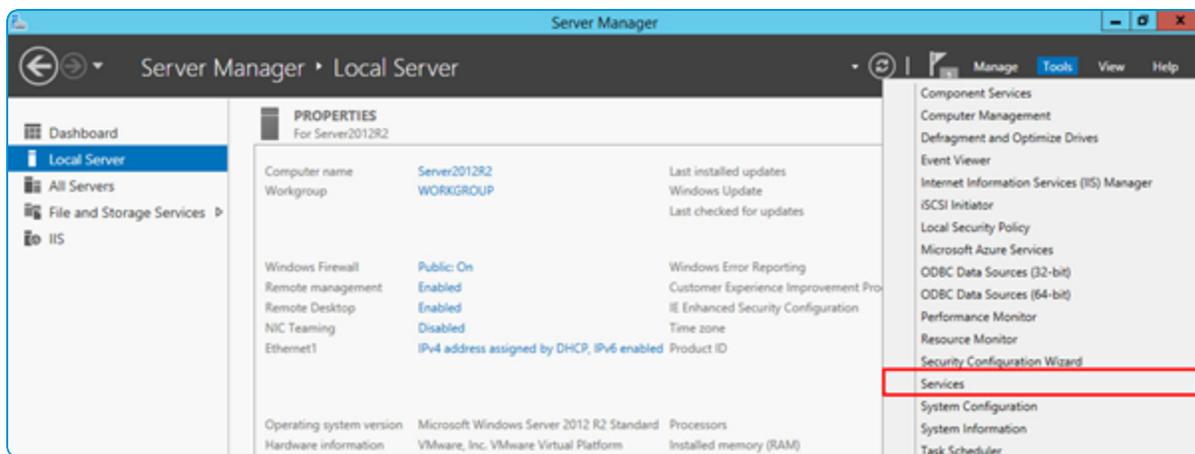
After staging the appropriate files, and backing up your servers, you are almost ready to install the upgrade.

Verify that all the AirWatch Services are stopped, and disable Internet Information Services (IIS) websites on each Application and Device Services server. By disabling these, AirWatch will effectively be down and the database will be able to be upgraded without interference. **Note that SEG, VMware Tunnel and VMware Enterprise Systems Connector are considered auxiliary components and you do not need to stop their services as part of this step.**

Disable the World Wide Web Publishing Service

Before starting the upgrade process, you must stop and disable the World Wide Web Publishing Service.

1. Open the **Server Manager**.
2. Navigate to **Tools > Services**.



3. Scroll to the bottom until you see the **World Wide Web Publishing Service**.
4. Right-click **World Wide Web Publishing Service** and select **Stop**.
5. Select **Properties** and verify that the Service Status displays **Stopped**.
6. From the **Properties** menu, set the **Startup Type** as **Disabled**. Select **Apply** and **Save**.

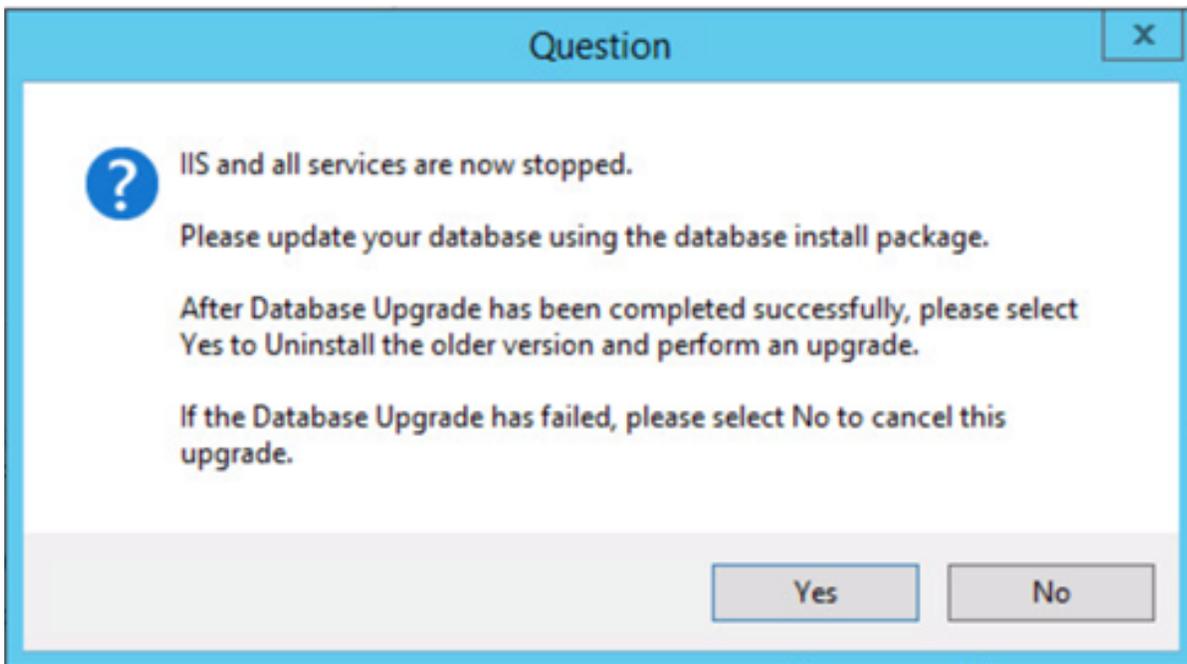
After disabling the World Wide Web Publishing Service, run the AirWatch Application Installer on all of your AirWatch application servers. The installer stops all the services on the App server automatically. For more information, see [Start the AirWatch Application Installer on page 29](#).

Start the AirWatch Application Installer

After stopping and disabling the World Wide Web Publishing Service, start the AirWatch Application Installer on all of your AirWatch application servers. The installer stops all the services on the App server automatically.

To start the installer:

1. On each application server, open the **9.2 Application** folder and run the **AirWatch Application 9.2.X Full Install.exe**. Execute the AirWatch installer from an account with administrator privileges. If you do not have administrative privileges, right-click and choose **Run as Administrator** to run the installer.
2. The installer installs pending server prerequisites, if any.
Certain software components you might be prompted to download, such as .NET and TLS, require a reboot. Proceed with the installer until finished and reboot when you are done.
3. If requested, reboot the server. Once the server reboots, the AirWatch Application Installer restarts automatically. If not, please restart the installer to continue
The installer continues installing any prerequisites. When finished, a prompt displays asking you to update your AirWatch database.



Important: Complete these steps on each application server before continuing. After reaching the database prompt on each application server, upgrade your AirWatch Database. For more information, see [Upgrade Database](#) on page 32.

Chapter 6:

Upgrade the AirWatch Database

Overview 32

Upgrade Database 32

Overview

In this step you will run the actual database installers according to your current AirWatch version.

Caution: Before continuing with the following steps, ensure you have properly backed up your AirWatch database. If you have not properly backed up your database server and an error occurs during the upgrade process, you could lose all of your AirWatch data and you must start your deployment of AirWatch from scratch.

Follow the applicable procedure below to upgrade to AirWatch 9.2 depending on your current AirWatch version. You can find out which version of AirWatch you are running by opening the AirWatch Console and selecting **About AirWatch** from the bottom left hand corner of any page.

If you are on a database version older than the versions listed here and require instructions to upgrade the database, then you should reference previous versions of the VMware AirWatch Upgrade Guide (available to partners and existing customers at: <https://resources.air-watch.com/view/xm92c772sbl39zg658k9>), which include instructions for older versions.

Upgrade Database

Perform the following steps to upgrade your database to the current version.

1. Verify that all AirWatch and IIS services are [stopped](#).
2. [Verify that your AirWatch Application Servers and AirWatch Databases are backed up](#).
3. Upgrade the database using the step-by-step instructions below under [How To Execute the Database Setup Utility](#). First, verify which utilities you will need to run:
 - a. If the current database version is 8.4,
 - Run the 9.0 database installation; proceed to step b.
 - b. If the current database version is 9.0,
 - Run the 9.1 database installation; proceed to step c.
 - c. If the current database version is 9.1,
 - Run the 9.2 database installation.

How To Execute the Database Setup Utility

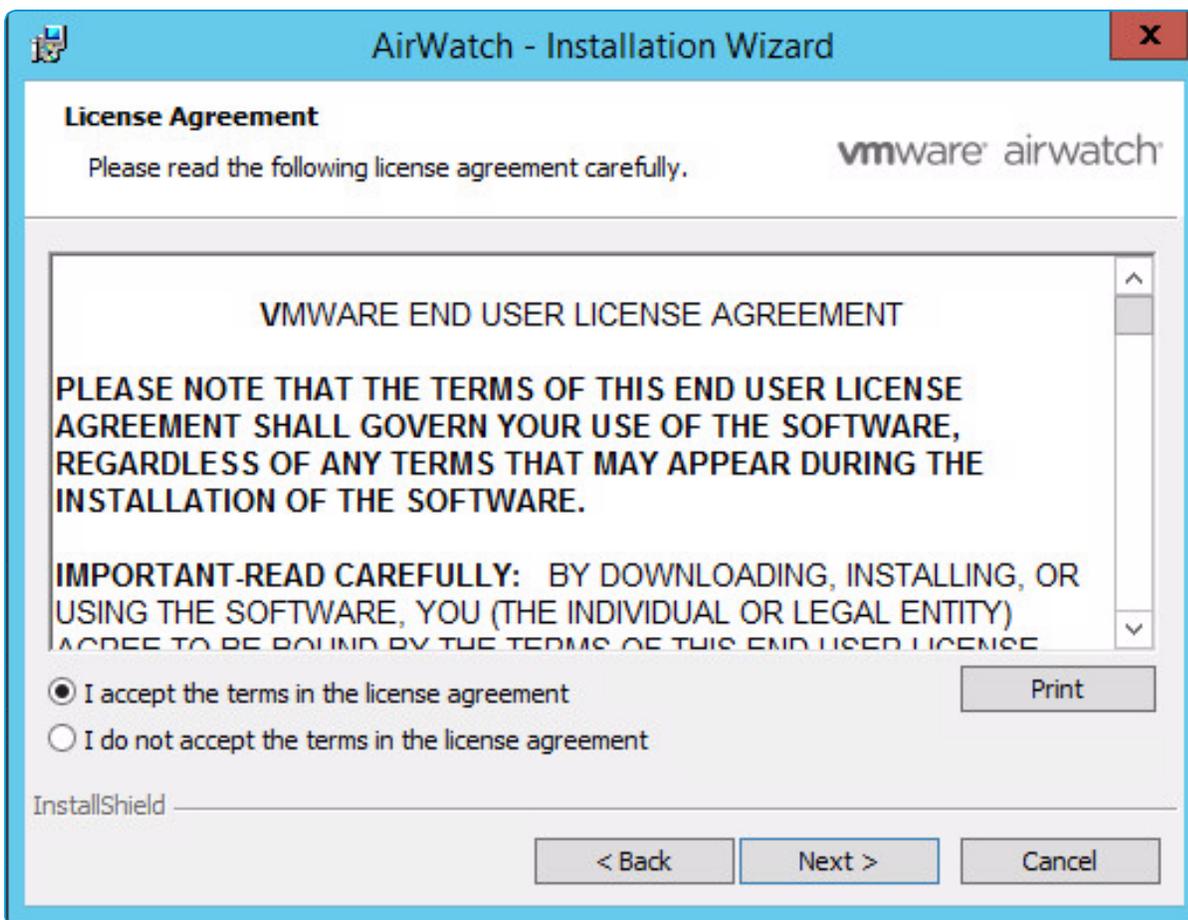
Use the following step-by-step instructions to perform the necessary database upgrades for each AirWatch version as applicable to your setup. For example, upgrading from 8.3 to 9.2 will require you to follow the procedure below four times – 8.3 to 8.4, 8.4 to 9.0, 9.0 to 9.1, and 9.1 to 9.2. The procedure itself is the same for each incremental upgrade, but it must be performed for each version until you reach 9.2.

If you use the Windows authentication credentials of the current user to connect to the database you are installing to, either:

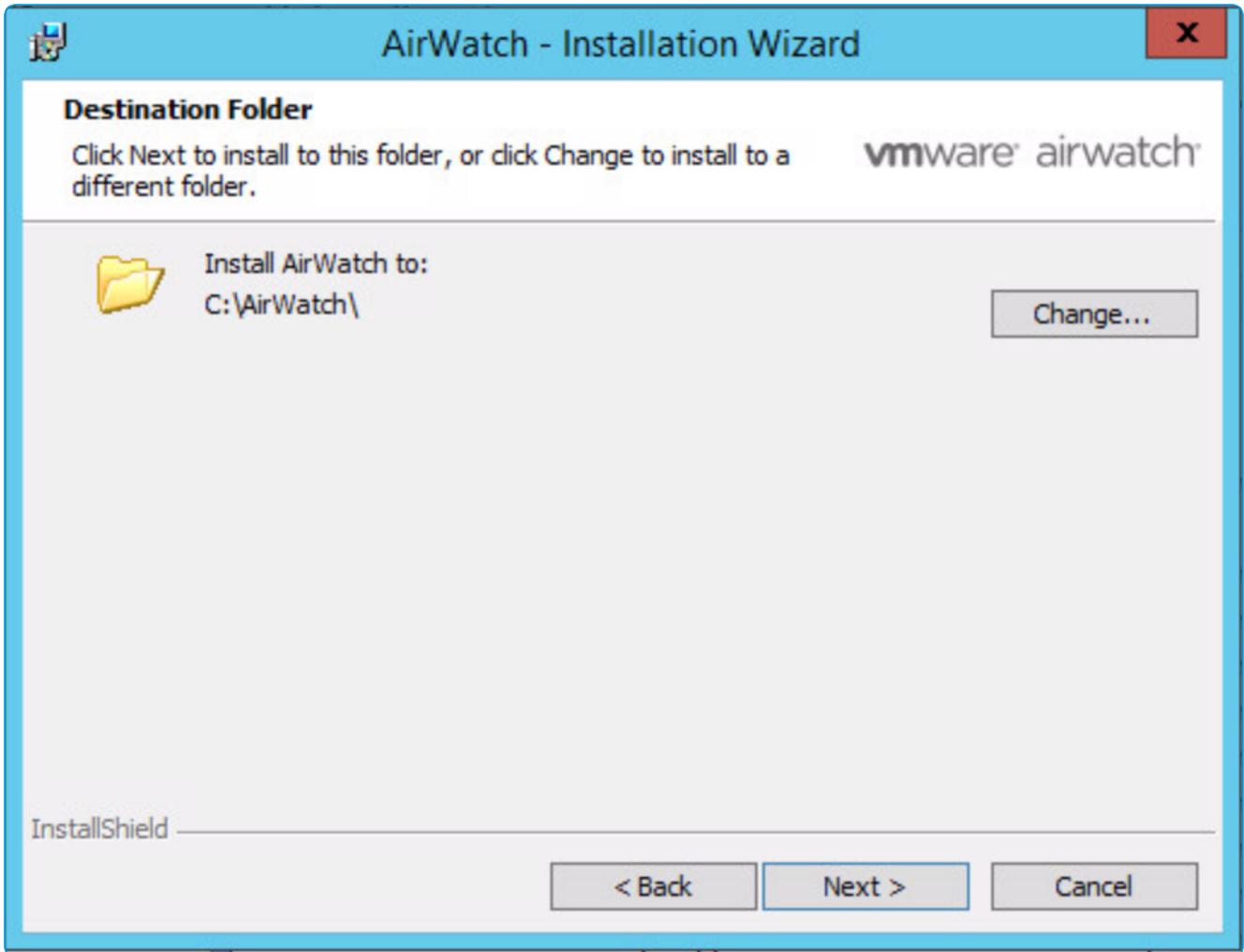
- Shift+right-click to run as a different user and log in as the Windows account you are using to authenticate.
- Log into the server as the Windows account you are using to authenticate, if you have not already.

From a server connected to the database, perform the following:

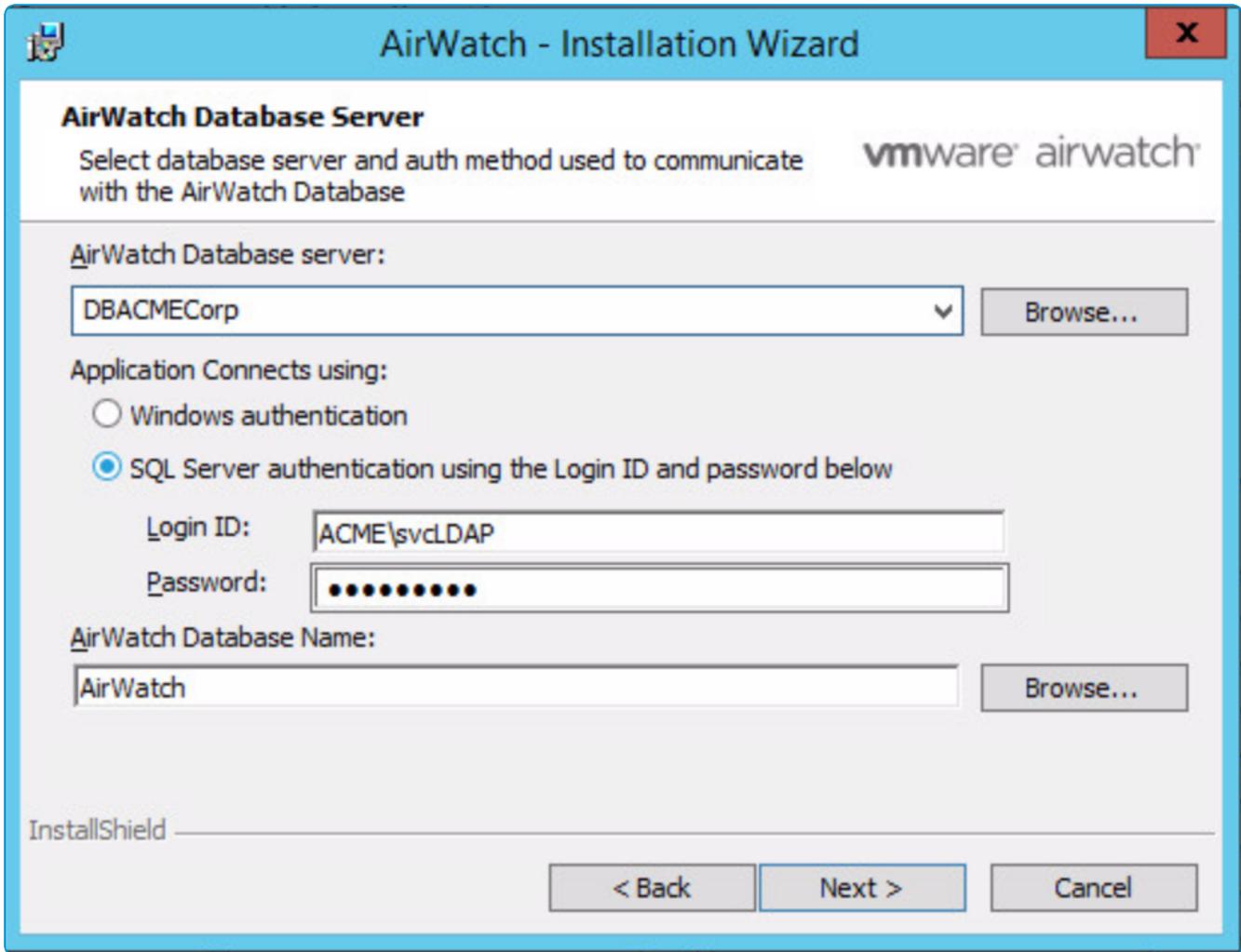
1. Verify that all AirWatch and IIS services are [stopped](#).
2. Open the **AirWatch Database 8.x/9.x Setup.exe** executable by right-clicking and running as administrator, where 8x/9.x is the next AirWatch version from the one you are running. (If you are currently on 9.1, you would run 9.2.)
Certain software components you might be prompted to download, such as .NET and TLS, require a reboot. AirWatch recommends proceeding with the installer until finished and rebooting when you are done.
3. If your server is missing any essential components, the DB installer will automatically prompt you to install them. The DB installer requires .NET 4.6.2 to run. If you do not want to install .NET on your SQL server, you can run the installer from the application server.
When complete, select **Next**.
4. Accept the AirWatch EULA and select **Next**.



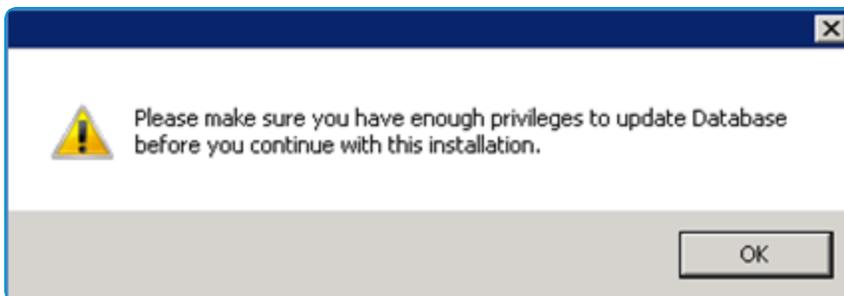
5. Select a location to upgrade the AirWatch Database Files. Best practice is to upgrade wherever the AirWatch folder exists on your system. For example, C:\AirWatch. Click **Next**.



- Next, review the information about the AirWatch database, specifically the server name, the user account with correct privileges, and the database name. Once complete, choose **Next**.



7. Before proceeding, you will be warned to make sure that your user account has enough permissions. Click **OK**.



8. Next, select **Install** to begin the database upgrade process.
9. Once the database upgrade process has completed, select **Finish**.

Chapter 7:

Upgrade the AirWatch Console and Device Services Servers

Overview	37
Upgrade AirWatch Application Servers	37

Overview

Once the database has been upgraded, the installer can be completed on each AirWatch Console and Device Services Server to finish up the upgrade process.

If you have previously started the installer to stop all websites and services, resume the installer on each server and complete the Wizard.

For deployments with dedicated API and AWCM servers:

Dedicated API and AWCM servers are considered application servers, similar to the AirWatch Console and Device Services. You should therefore perform the steps below on these servers if you have dedicated servers for these components.

Upgrade AirWatch Application Servers

Once your database is updated, upgrade your application servers to the latest version of VMware AirWatch.

On each of your Console and Device Services servers, continue to run the **AirWatch Application 9.2.X Full Install.exe**. The installer detects a previous version of AirWatch and prompts you to upgrade. During this process, the AirWatch Installer will stop IIS and all AirWatch services and prompt the administrator to update the AirWatch database. However, since you have already upgraded the database, you can continue without taking any extra actions.

The upgrade process does not differ significantly from the installation process. The values and settings you configured for your AirWatch installation should be automatically populated, meaning you can verify them and select Next through the installer. For specific details on each of these installer screens, refer to the VMware AirWatch Installation Guide (VMware provides this document to you as part of the on-premises installation process).

IMPORTANT: Do not change any of the pre-populated fields as part of your upgrade without first confirming with AirWatch, as this could adversely affect your deployment and in some cases prevent AirWatch from functioning.

SQL Server Availability Group Note

To upgrade a VMware Identity Manager Server equipped with SQL Server availability groups, you must disable availability groups before you upgrade the server. After the upgrade, you must re-enable availability groups.

For more information, see [Upgrade an Identity Manager Server with SQL Server Availability Groups on page 26](#).

Chapter 8:

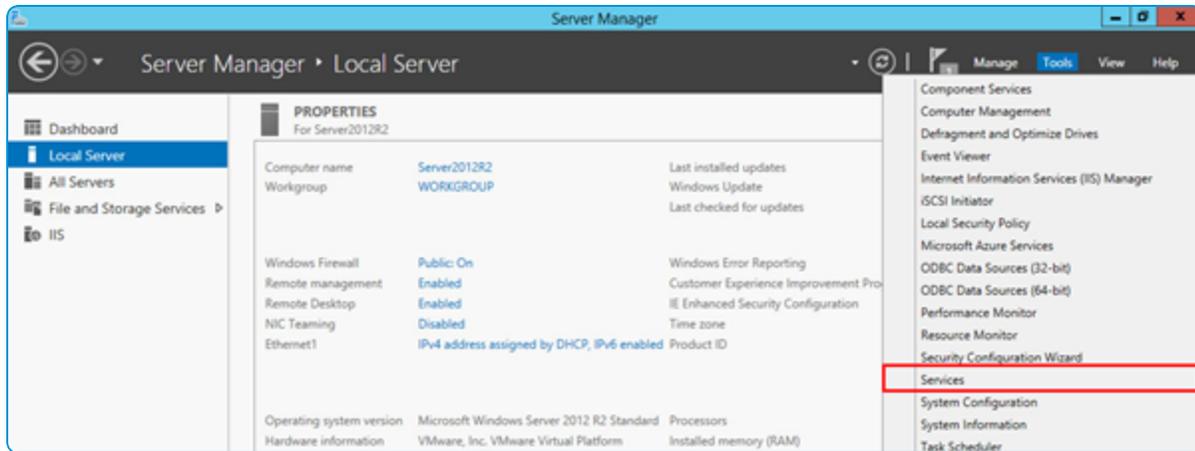
Validate the Upgrade

Verify AirWatch Services are Running	39
Verify the Upgrade	39

Verify AirWatch Services are Running

Verify AirWatch services are started before you perform the other validation tasks.

1. Open the **Server Manager**.
2. From the left pane, select your local server navigate to **Tools > Services**.



You will see all AirWatch Services at the top of the services list in alphabetical order. Each of these services start with AirWatch in the name.

3. Verify that each of these services show **Started** as the Status.
4. Verify the **World Wide Web Publishing** service is **Started** and that **Startup Type** is set to **Automatic**.

Verify the Upgrade

Perform the following verification steps to ensure you successfully upgraded AirWatch.

Task: Validate Customer Administrator Roles

1. Log in to the AirWatch Console and navigate to **Accounts > Administrators > Roles**.
2. Verify that the update did not remove any of your custom administrator roles. If they are missing, you will have to recreate them manually.

Task: Verify Directory Service Settings

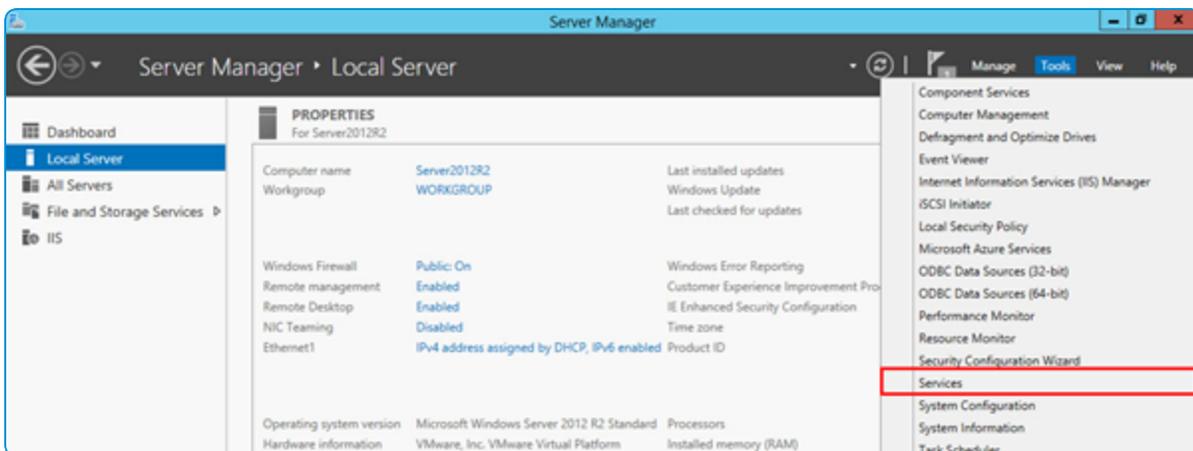
3. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**. Select the **User** tab.
4. Select **Show Advanced**. Verify that **Auto Merge** is checked. Select the **Group** tab.
5. Select **Show Advanced**. Verify **Auto Sync** and **Auto Merge** are checked.

Task: Verify the Site URLs

6. Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs**.
7. Verify the **REST API URL** and **Sync Appcast URL** are configured correctly:
 - The **Console URL** should be "https://{CONSOLE_URL}", where {CONSOLE_URL} is the URL of your AirWatch Console Server.
 - The **Device Services URL** should be "https://{AW_DS_URL}/DeviceServices", where {AW_DS_URL} is the URL of your Device Services server.
 - The **REST API** should be "https://{AW_API_URL}/API", where {AW_API_URL} is the URL of your API server.
 - The **Content Locker Sync Appcast URL** should be "https://{AW_DS_URL}/DeviceServices/AirWatchSyncAppcast.xml", where {AW_DS_URL} is the URL of your Device Services server.
 - The **MdmAgentAppcast URL** should be "https://{AW_DS_URL}/DeviceServices/AirWatchAgentAppcast.xml", where {AW_DS_URL} is the URL of your Device Services server.
 - The **Outlook Add-In Content Locker Appcast URL** should be "https://{AW_DS_URL}/DeviceServices/OutlookSCLAppcast.xml", where {AW_DS_URL} is the URL of the Device Services server.
 - The **Content Locker Appcast URL** should be "https://{AW_DS_URL}/DeviceServices/SCLAppcast.xml", where {AW_DS_URL} is the URL of the Device Services server.
 - Nothing should appear as "localhost" except for the Google Play Service URL.

Task: Validate GEM Functionality

8. On your Console server, open **Server Manager**.
9. From the left pane, select **Local Server** and navigate to **Tools > Services**.



10. You will see all AirWatch Services at the top of the services list in alphabetical order. Each of these services start with AirWatch in the name. For the **GEM Inventory Service**, right-click and select **Stop**.
11. Navigate to **C:\AirWatch\Logs\Services**. Delete the AirWatchGemAgent.log file.
12. Return to **Server Manager > Tools > Services**. For the **GEM Inventory Service**, right-click and select **Start**.

- Check your C:\AirWatch\Logs\Services\ folder to see if a log regenerates. If a log regenerates with errors, contact AirWatch Support for further assistance.

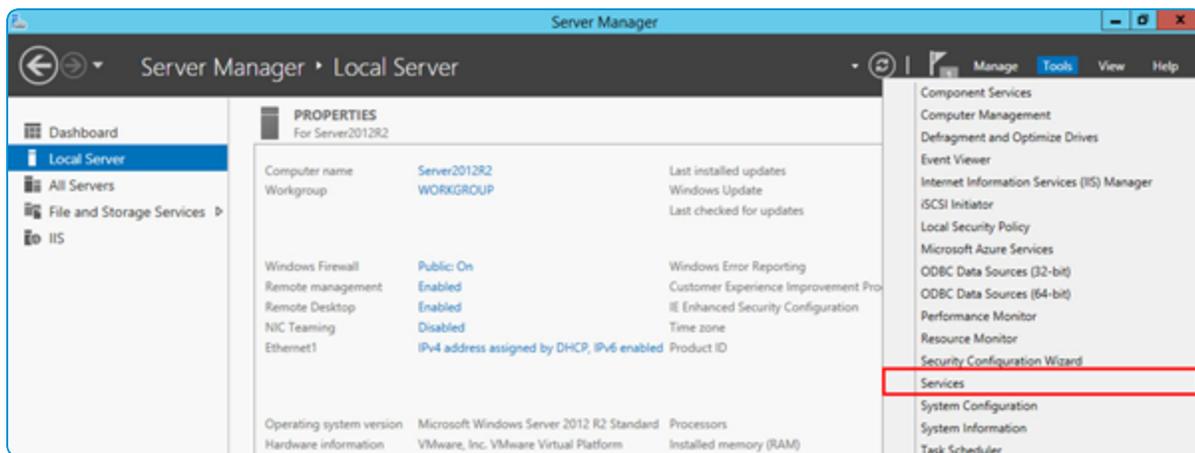
If you do not see a log file in this folder, then this is normal and you do not need to contact AirWatch Support.

Task: Disable Services on Multiple Console Servers

This task is only applicable if you have **multiple Console servers**.

The two services mentioned (AirWatch Device Scheduler and AirWatch GEM Inventory Service) must only be active on one primary Console server. Disable these services on any Console servers other than the primary by following the step-by-step instructions.

- On your non-primary Console servers, open the **Server Manager**.
- From the left pane, select Local Server and navigate to **Tools > Services**.



- You see all AirWatch Services at the top of the services list in alphabetical order. Each of these services starts with AirWatch in the name. For the **AirWatch Device Scheduler** and **AirWatch GEM Inventory Service**, right-click and select **Stop**.

Appendix:

Complete the Post Upgrade Checklist

In addition to the items in the previous section, use the following checklist to ensure your upgrade completed properly. For the following items, verify that the ones that are applicable to your deployment are working correctly.

Status	Functionality	Verification
AirWatch Console testing		
	Directory Services	Navigate to Groups & Settings > All Settings > System > Enterprise Integration > Directory Services and select Test Connection.
	Email (SMTP)	Navigate to Groups & Settings > All Settings > System > Enterprise Integration > Email (SMTP) and select Test Connection.
	AWCM	Attempt to access "https://<AWCM URL>:<port>/awcm/status", where <AWCM URL> is the URL of your AWCM and <port> is the port you configured it on. If functioning correctly you should see an "OK" status message.
	Devices are checking in	Verify on the Devices > List View page that devices are checking in by looking at the Last Seen column.
	Console Access using LDAP	Verify that AD or LDAP users work by logging into the Console with one (if applicable).
	Executing a Report	Try running an Admin User Roles report by navigating to Hub > Reporting & Analytics > Reports > List View.
	Content Management (if applicable)	Try downloading a piece of content from a device.
iOS device testing		
	Enrollment	Try enrolling an iOS device.
	Sending Commands (e.g. Device Lock)	Try sending a command to an enrolled iOS device.
	Create and Push Profile	Try creating and sending a profile from the Console to an iOS device.
	Create and Push Application	Try to create and send an application from the Console to an iOS device.
	Public Applications	Try to recommend a public application from the Console to an iOS device.
	Internal Applications	Try to push an internal application from the Console to an iOS device.

Status	Functionality	Verification
Android device testing		
	Enrollment	Try enrolling an Android device.
	Sending Commands (e.g. Device Lock)	Try sending a command to an enrolled Android device.
	Create and Push Profile	Try creating and sending a profile from the Console to an Android device.
	Create and Push Application	Try to create and send an application from the Console to an Android device.
	Public Applications	Try to recommend a public application from the Console to an Android device.
	Internal Applications	Try to push an internal application from the Console to an Android device.
Windows Rugged device testing		
	Device Check-In	Verify that Windows Mobile devices are checking in after the upgrade process.
	Create and Push Provisioning Product	Try to create and push a provisioning product to a Windows Mobile device.
	AWCM Testing	Verify on the Device Details page for a Windows Mobile device that AWCM is Connected.
	Remote Control	Try to activate Remote Control for a Windows Mobile device on the Device Details page. (Ensure Privacy Settings are enabled to allow you to do this.)
	Screenshot/Send Message	Try to take a screenshot or send a message Windows Mobile on the Device Details page.
Windows Phone device testing		
	Enrollment	Try enrolling a Windows Phone device.
	Sending Commands (e.g. Device Lock)	Try sending a command to an enrolled Windows Phone device.
	Create and Push Profile	Try creating and sending a profile from the Console to a Windows Phone device.

If Problems are Detected After the Upgrade

If during any of the verification steps listed above you are unsuccessful, check the following:

- If all AirWatch Services are up and running on the server with proper paths to the AirWatch 9.2 folder.
- If all AirWatch Websites are listed in IIS.
- If the Windows Application Log shows any errors originated from the AirWatch application.

- If any AirWatch logs show any errors that have occurred.
- If you are still having issues and need to contact AirWatch Support, then ensure you have the logs mentioned above to expedite resolution. Please include the log located at C:\AirWatch\AirWatch X.X\Database\AWDatabaseLog_MM-DD-YYYY_XX-XX-XX.txt.

Appendix:

Performing a Feature Pack Update for AirWatch

Procedure

Use the following step-by-step instructions to apply a Feature Pack to your version of AirWatch.

1. Stop all the AirWatch services and websites on AirWatch Console and Device Services servers.
2. Stopping and disable the World Wide Web Publishing Service.
3. Back up your AirWatch Application Servers and AirWatch Database.
4. Obtain the **AirWatch_Application_9.2.X_Install.exe**. and **AirWatch_Database_9.2.X_Setup.exe** files from AirWatch Resources (resources.air-watch.com).

These will be the full installer files, which you will run on your servers to apply the upgrade.

AirWatch recommends that you retain these *.exe install files.

5. Execute the **AirWatch_Application_9.2.X_Install.exe**. by right-clicking and running as administrator on each Console and Device Services server up until the point where all application servers state "IIS and all services are now stopped. Please upgrade your AirWatch database using the provided script", then immediately proceed to the next step.

AirWatch recommends that you retain these *.exe install files.

6. Run the **AirWatch_Database_9.2.X_Setup.exe** executable on the AirWatch database server.

AirWatch highly recommends that you retain these *.exe install files.

7. Finish running the installers on each Console and Device Services server.

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.