

VMware AirWatch Installation Guide

Installing AirWatch in on-premises environments

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 AirWatch Installation	6
Before you Begin Checklist	6
Installation Procedure Checklist	7
Chapter 2: Installation Preparation	10
Database Server Prerequisites	11
Application Server Prerequisites	12
VMware Identity Manager Service Prerequisites	14
Perform Optional Installs	15
Reports Prerequisites	15
Create the AirWatch Database	16
Create the AirWatch SQL Service Account and Assign DB Owner Roles	17
Create the VMware Identity Manager Service Database	20
Create the Identity Service SQL Service Account and Assign DB Owner Roles	21
Configure your Application Servers	24
Configure Your Internal DNS Record and Certificates	25
Configure Your External DNS Record and Certificates	29
Stage Install Files	35
Workspace ONE Validation Tool	35
Chapter 3: Database Installation	44
Run the AirWatch Database Setup Utility	45
Verify Proper Database Installation	46
Chapter 4: Application Server Installation	47
Run the AirWatch Installer on Each Application Server (Console and Device Services)	48
(Optional) Run the Installer on Additional Device Services Servers	61
Run the AirWatch Installer on the VMware Identity Manager Service	62
Chapter 5: Reports Installation	68
Reports Overview	69

Connect the Database to Reports Server	69
Configure the Service Account for SSRS	70
Configure the Web Service URL	72
Set up the Reporting Database	73
Verify the Report Manager URL and Web Service URL	74
Set up the AirWatch SSRS User	75
Add the SSRS User to IIS_IUSRS	77
Run the AirWatch Reporting Installer	78
Integrate Reports with the AirWatch Console	83
Reports Storage Overview	84
Chapter 6: Installation Verification	87
Verify Correct Site URL Population	88
Verify Connectivity	88
Verify Services Are Started	88
Validate GEM Functionality	89
(Optional) Disable Services on Multiple Console Servers	90
VMware Identity Manager Troubleshooting Overview	90
Chapter 7: Next Steps	96
Overview	97
Create a Corporate Apple ID	97
Run the Workspace ONE Wizard	97
Accessing Other Documents	98

Chapter 1:

Overview

- Introduction to AirWatch Installation6
- Before you Begin Checklist6
- Installation Procedure Checklist7

Introduction to AirWatch Installation

The AirWatch Windows Installer allows you to install AirWatch components onto application servers as needed to meet your AirWatch deployment needs. The installer handles the AirWatch Console server components, the Devices Services server components, and the VMware Identity Manager service.

Installing AirWatch requires following specific prerequisites and procedures to successfully deploy your AirWatch on-premises solution. Make sure to meet the prerequisites before proceeding with the installation instructions. Installing AirWatch on premises involves configuring servers for your database, application, any auxiliary components, and reports. AirWatch comprises several different components, which can be combined with application servers or installed on their own dedicated servers.

To review recommended architectures based on your deployment size, refer to the **VMware AirWatch Recommended Architecture Guide**, [available on AirWatch Resources](#).

Before you Begin Checklist

Be aware of several notes and caveats before attempting to install AirWatch on premises. Read through the following sections and ensure that you are fully prepared for following the steps in the remainder of this guide.

Obtain the Latest Version of this Document

Ensure that 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 frequently makes updates to documentation and having the latest version ensures that you are following the best practices and procedures.

Obtain the Install Package Files

Ensure that you have downloaded the installation package files. The link to these files is provided to you by your AirWatch consultant as part of the deployment process.

Meet the Requirements

Meet all the requirements needed for an AirWatch installation. Specific hardware and software requirements are outlined in the **VMware AirWatch Recommended Architecture Guide**, [available on AirWatch Resources](#). A list of other requirements can be found in the [Installation Preparation](#) section.

Note: As of AirWatch Version 9.1 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.

Verify your On-Call Resources

Ensure that you have the proper on-call resources available if you need them. These resources may include technical resources such as the Database Analyst, Change Manager, Server Administrator, Network Engineer, and MDM System Administrator.

Recommended Topologies

To streamline the AirWatch installation process, this document refers to both the AirWatch Console server and AirWatch Device Services server. Before proceeding, it is important to understand each of these components and what they mean to your specific topology model.

- The **AirWatch Console Server** refers to the component of AirWatch that renders and displays the AirWatch Console. It presents and sends data to the database directly from the AirWatch UI.
- The **AirWatch Device Services Server** refers to the component of AirWatch that communicates with all managed devices. This server runs all processes involved in receiving and transmitting information from devices to other components of the system.
- The **VMware Identity Manager Server** refers to the component of AirWatch that enables Workspace ONE functionality. This server provides services required for the Workspace ONE application and brand new functionality like mobile single sign-on and conditional access for third-party applications.
- The standard AirWatch deployment method involves installing multiple application servers for these components alongside a database. For each procedure in this guide that describes both the Console and Device Services components, complete the procedure on all AirWatch servers.
- This document assumes that you are using one of the recommended architectures as detailed in the **VMware AirWatch Recommended Architecture Guide**, [available on AirWatch Resources](#). If you are not using one of these architectures, contact AirWatch for additional assistance.

A Note About Screenshots in this Document

Where applicable, this document uses screenshots from Windows Server 2012. If you are using Windows Server 2008 or 2016, then perform the same actions documented in this guide, with the knowledge that the exact steps may slightly differ.

Installation Procedure Checklist

Use the following checklist to track your installation progress. Use the links provided to jump to a particular section, but ensure that you complete all the required steps.

Status Checklist	Requirement	Notes
Step 1: Prepare for Your Installation		
	Verify Database Server Prerequisites Are Met	See Database Server Prerequisites on page 11 .
	Verify Application Server Prerequisites Are Met	See Application Server Prerequisites on page 12 .
	Verify Identity Manager Service Server Prerequisites Are Met	See VMware Identity Manager Service Prerequisites on page 14 .
	Perform Optional Installs	See Perform Optional Installs on page 15 .
	Verify Reports Server Prerequisites Are Met	See Reports Prerequisites on page 15 .
	Create the AirWatch Database	See Create the AirWatch Database on page 16 .

Status Checklist	Requirement	Notes
	Assign AirWatch Database Roles	See Create the AirWatch SQL Service Account and Assign DB Owner Roles on page 17.
	Create the Identity Manager Database	See Create the VMware Identity Manager Service Database on page 20.
	Assign Identity Manager Database Roles	See Create the Identity Service SQL Service Account and Assign DB Owner Roles on page 21.
	Configure Application Servers	See Configure your Application Servers on page 24.
	Server Internal DNS and Certificate Requirements	See Configure Your Internal DNS Record and Certificates on page 25.
	Server External DNS and Certificate Requirements	See Configure Your External DNS Record and Certificates on page 29.
	Stage Install Files	See Stage Install Files on page 35.
Step 2: Perform the Database Installation		
	Run the AirWatch Database Setup Utility	See Run the AirWatch Database Setup Utility on page 45.
	Verify Proper Database Installation	See Verify Proper Database Installation on page 46.
Step 3: Perform Application Server Installation		
	Start the AirWatch Installer on Each Application Server	See Run the AirWatch Installer on Each Application Server (Console and Device Services) on page 48.
	(OPTIONAL) Run the AirWatch Installer on Any Additional Device Services Servers	See (Optional) Run the Installer on Additional Device Services Servers on page 61.
	(OPTIONAL) Run the AirWatch Installer on Identity Manager Server	See Run the AirWatch Installer on the VMware Identity Manager Service on page 62.
Step 4: Perform Reports Installation		
	Connect Database to Reports Server	See Connect the Database to Reports Server on page 69.
	Configure Service Account for SSRS	See Configure the Service Account for SSRS on page 70.
	Configure Web Service URL	See Configure the Web Service URL on page 72.
	Set up Reporting Database	See Set up the Reporting Database on page 73.
	Verify Report URLs	See Verify the Report Manager URL and Web Service URL on page 74.
	Set up AirWatch SSRS User	See Set up the AirWatch SSRS User on page 75.
	Add the SSRS User to IIS_IUSRS	See Add the SSRS User to IIS_IUSRS on page 77.
	Run the Reports Installer	See Verifying Reports Functionality on page 81.
	Integrate Reports with the Console and Enable Reports Storage	See Integrate Reports with the AirWatch Console on page 83 and Reports Storage Overview on page 84.

This guide does not cover post-install configuration, but does include a [Next Steps](#) section, which covers some of the essential procedures to get you started.

Chapter 2:

Installation Preparation

Database Server Prerequisites	11
Application Server Prerequisites	12
VMware Identity Manager Service Prerequisites	14
Perform Optional Installs	15
Reports Prerequisites	15
Create the AirWatch Database	16
Create the AirWatch SQL Service Account and Assign DB Owner Roles	17
Create the VMware Identity Manager Service Database	20
Create the Identity Service SQL Service Account and Assign DB Owner Roles	21
Configure your Application Servers	24
Configure Your Internal DNS Record and Certificates	25
Configure Your External DNS Record and Certificates	29
Stage Install Files	35
Workspace ONE Validation Tool	35

Database Server Prerequisites

Meet the database server prerequisites before installing the database server. The prerequisites listed here apply to any database you plan to install (for example, the AirWatch or AirWatch Identity Manager databases).

SQL Server Hardware Requirements

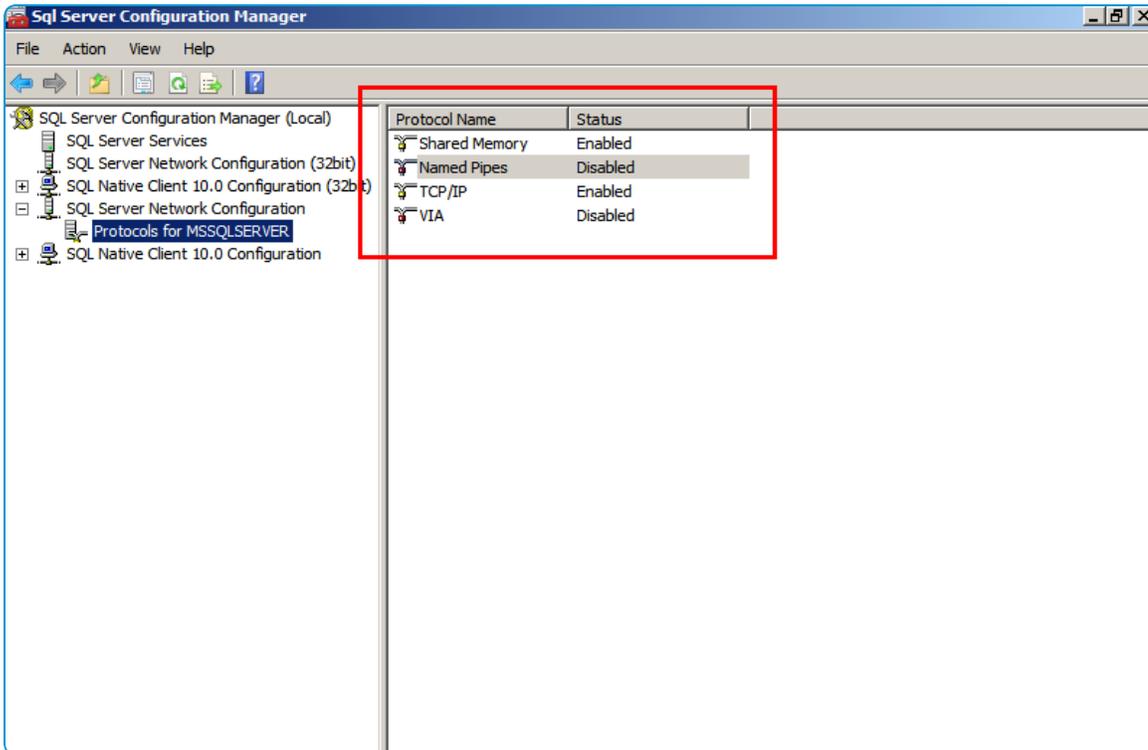
The exact specifications needed for your SQL server depend on the size and needs of your deployment. You may need to gather this information before proceeding so you size your servers correctly. Read through the **VMware AirWatch Recommended Architecture Guide**, available on [AirWatch Resources](#), for hardware sizing information and other technical details that ensure the smooth operation of your AirWatch database.

SQL Server Software Requirements

- SQL Server 2012, SQL Server 2014, or SQL Server 2016 with Client Tools (SQL Management Studio, Reporting Services, Integration Services, SQL Server Agent, latest service packs). Ensure the SQL Servers are 64-bit (OS and SQL Server). AirWatch does not support Express, Workgroup, or Web editions of SQL Server. These editions do not support all the features used in the AirWatch application. Currently only Standard and Enterprise Editions are supported.
- Microsoft SQL Server 2012 Native Client 11.3.6538.0 is required to run the database installer. If you do not want to install Microsoft SQL Server 2012 Native Client 11.3.6538.0 on to your database server, then run the database installer from another AirWatch server or a jump server where Microsoft SQL Server 2012 Native Client 11.3.6538.0 can be installed.
- .NET 4.6.2 is required to run the database installer. If you do not want to install .NET on to your database server, then run the database installer from another AirWatch server or a jump server where .NET can be installed.
- Ensure the SQL Server Agent Windows service is set to Automatic or Automatic (Delayed) as the Start type for the service. If set to Manual, it has to be manually started before database installation.
- You must have the access and knowledge required to create, back up, and restore a database.

TCP/IP is Enabled

Use TCP/IP to connect to the database and disable Named Pipes. In SQL Server Configuration Manager, navigate to SQL Server Network Configuration and select **Protocols for MSSQLSERVER**.



Identity Manager Database

The Identity Manager database supports Named Instances or Windows authentication.

Application Server Prerequisites

Meet the application server prerequisites before installing the application server. The prerequisites listed here apply to any application server you plan to install.

Hardware Requirements

An AirWatch installation can involve many servers, and the exact specifications depend on the size and needs of your deployment. You may need to gather this information before proceeding so you size your servers correctly. Read through the **VMware AirWatch Recommended Architecture Guide**, available on [AirWatch Resources](#), for hardware sizing information and other technical details that ensure the smooth operation of your AirWatch solution.

Network Requirements

Review all the network requirements as outlined in the **VMware AirWatch Recommended Architecture Guide**. These requirements include the firewall ports that must be opened for AirWatch to function properly.

Software Requirements

Ensure that you meet the following software requirements for the application servers:

- Internet Explorer 9+ installed on all application servers
- Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016

- 64-bit Java (JRE 1.8) server needed for the server AWCM is installed on
- 64-bit Java (JRE 1.8) installed on all app servers
- .NET Framework 4.6.2 required; .NET 4.7 is supported. The installer is packaged with the .NET Framework 4.6.2 installer and will install it if 4.6.2 or 4.7 is not already present.
- PowerShell version 3.0+ is required if you are deploying the PowerShell MEM-direct model for email. To check your version, open PowerShell and run the command `$PSVersionTable`. More details on this and other email models can be found in the **VMware AirWatch Mobile Email Management Guide**, [available on AirWatch Resources](#).
- Microsoft SQL Server 2012 Native Client 11.3.6538.0 is required to run the database installer. If you do not want to install Microsoft SQL Server 2012 Native Client 11.3.6538.0 on to your database server, then run the database installer from another AirWatch server or a jump server where Microsoft SQL Server 2012 Native Client 11.3.6538.0 can be installed.

Proxy Requirements

The AirWatch servers can be configured with a proxy / PAC file for outbound Internet access. Apple APNs traffic, however, is not HTTP traffic, and cannot be authorized through traditional HTTP proxies. This traffic must go straight out to the Internet or through an application/SOCKS proxy.

If you are performing outbound proxying of APNs messages, your proxy application must support SOCKS V5. SOCKS V4 and SOCKS V4a are not supported.

Install Role from Server Manager

Ensure that you meet the following IIS requirements, depending on your Windows Server version:

- IIS 7.0 (Server 2008 R2)
- IIS 8.0 (Server 2012 or Server 2012 R2)
- IIS 8.5 (Server 2012 R2 only)
- IIS 10.0 (Server 2016)

See additional information on the required roles and features under [Configure your Application Servers](#).

RDP and VM Access to Application Servers

You must have remote access to the servers that AirWatch is installed on. Verify this access before attempting to install AirWatch servers.

Remote Desktop Connection Manager can be downloaded from the following link:

<https://www.microsoft.com/en-us/download/details.aspx?id=44989>

Verify you can connect using RDP to your application servers or appropriate VM hosts.

1. Open Remote Desktop Connection:
 - Start > Run
 - Type `mstsc`

- Select **OK**
2. Enter the IP address of the server and select **Connect**.
 3. Log in using credentials for the server. Verify a successful log-in.

Permissions of AirWatch Service Accounts

The service account you create for AirWatch needs the appropriate permissions to integrate with your back end systems. This can be one service account that has all required access. Verify AD/LDAP connectivity between your AirWatch service account and your backend systems.

VMware Identity Manager Service Prerequisites

The VMware Identity Manager service must be installed in a new standalone server or cluster. Meet the following requirements before installation.

During installation, AirWatch installs the complete VMware Identity Manager service including the RabbitMQ Server and Erlang component. These components are necessary to use all the features and functionality of the VMware Identity Manager service.

Identity Manager Service Software Requirements

- Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016
- PowerShell 4.0 or higher
 - Active Directory module for PowerShell (RSAT-AD-PowerShell)
- JRE 1.8 installed (included in the application server installer)

If your JRE is an older version, the installer automatically updates it, but does not remove the existing JRE version, which must be manually uninstalled.
- RabbitMQ Server (included in the application server installer)
- Erlang (included in the application server installer)

Networking Requirements

To configure certificate authentication in a VMware Identity Manager on-premises DMZ deployment:

- Enable SSL pass-through on port 443 at the load balancer in front of VMware Identity Manager.
- Open port 6443 (HTTPS) on the load balancer or firewall.

Review all the network requirements as outlined in the **VMware AirWatch Recommended Architecture Guide**. These requirements include the firewall ports that must be opened for AirWatch to function properly.

VMware Enterprise Systems Connector

When you deploy the complete VMware Identity Manager service, you must deploy the VMware Enterprise Systems Connector as well. For more information, see the **VMware Enterprise Systems Connector Installation and**

Configuration Guide, available on AirWatch Resources here: <https://resources.air-watch.com/view/lmtqzhdn2v8vf2ft763j>.

If you are only using the VMware Identity Manager for the unified application catalog, you must use the AirWatch Cloud Connector of the VMware Enterprise Systems Connector to connect to Active Directory.

AlwaysOn

The SQL Server AlwaysOn capability is a combination of failover clustering and database mirroring/log shipping. It allows for multiple read copies of your database and a single copy for read-write operations. For more information, see <https://msdn.microsoft.com/en-us/library/ff877884.aspx>.

So long as you have the bandwidth to support the traffic generated, the Identity Manager database supports AlwaysOn.

Perform Optional Installs

Install optional software to ensure a smooth installation process and to make troubleshooting easier.

Supported Browsers

The AirWatch Console supports the latest stable builds of the following web browsers:

- Chrome
- Firefox
- Safari
- Internet Explorer 11
- Microsoft Edge

Note: If using IE to access the Console, navigate to **Control Panel > Settings > Internet Options > Security** and ensure you have a security level or custom security level that includes the **Font Download** option being set to **Enabled**.

If you are using a browser older than those listed above, AirWatch recommends upgrading your browser to guarantee the performance of the AirWatch Console. Comprehensive platform testing has been performed to ensure functionality using these web browsers. The AirWatch Console may experience minor issues if you choose to run it in a non-certified browser.

Notepad++

Download and install Notepad++ (<http://notepad-plus-plus.org/>). This application is helpful because it allows you to view many log files at once using the tabular format and allows for the auto-refresh of a log file if it is regenerated.

Reports Prerequisites

Meet the reports server prerequisites before installing the reports server.

Hardware Requirements

The exact specifications needed for your reports server depend on the size and needs of your deployment. You may need to gather this information before proceeding so you size your servers correctly. Read through the **VMware AirWatch Recommended Architecture Guide**, available on [AirWatch Resources](#), for hardware sizing information and other technical details that ensure the smooth operation of your AirWatch reports server.

Software Requirements

- Windows Server 2008 R2/2012, or 2012 R2 (32-bit or 64-bit) with the latest service packs and recommended updates from Microsoft (<http://www.update.microsoft.com>).
- Microsoft SQL Server 2012, SQL Server 2014, or SQL Server 2016 with Client Tools (SQL Management Studio, Reporting Services, Integration Services, SQL Server Agent, latest server packs).

Network Requirements

Inbound communications to this server:

- AirWatch Console and Device Services using HTTP (80) or HTTPS (443) or other custom port numbers as needed.

Outbound communications from this server:

- The SMTP Mail Relay using SMTP on ports 25 or 465.

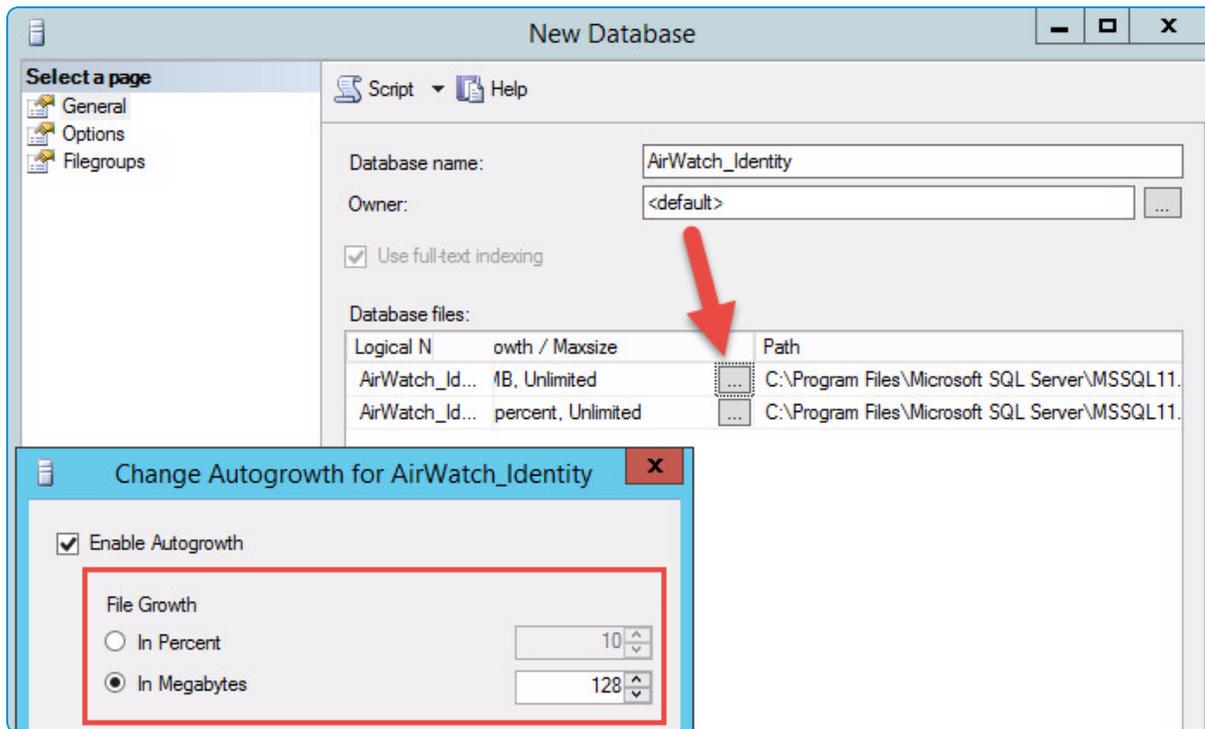
User Account Requirements

The Windows users running the Report installer must have access to both Report Manager and Report Database, as they are required to deploy the report files on the Report Server.

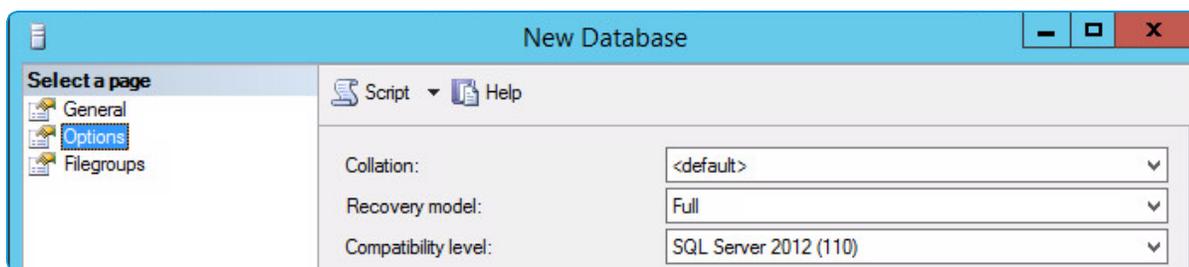
Create the AirWatch Database

To create the database, you must perform the following steps with an administrator account that has the correct read/write permissions.

1. On the SQL Server, open SQL Server Management Studio.
2. Log in using your user name and password.
3. Click **Connect**.
4. Right-click **Databases** and select **New Database**.
5. Enter **AirWatch** as the Database name.
6. Scroll to the right side of Database files, select the ... next to **Autogrowth for AirWatch**, and change **File Growth** to "In Megabytes" and the size to **128**, then select **OK**.



7. Select **Options**, and set the Collation to **SQL_Latin1_General_CP1_CI_AS**.

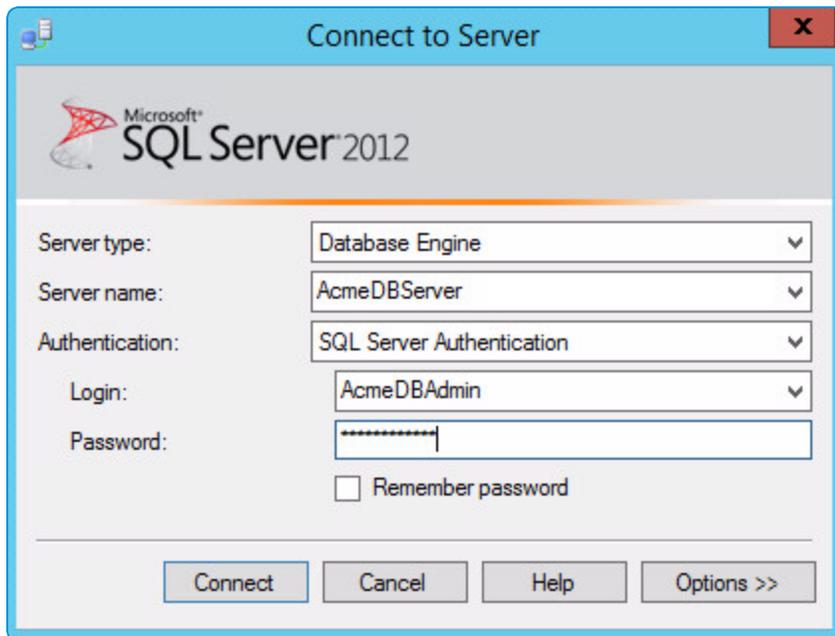


8. Select **OK** to create the AirWatch database.
9. Expand **Databases** and verify the AirWatch database is created.

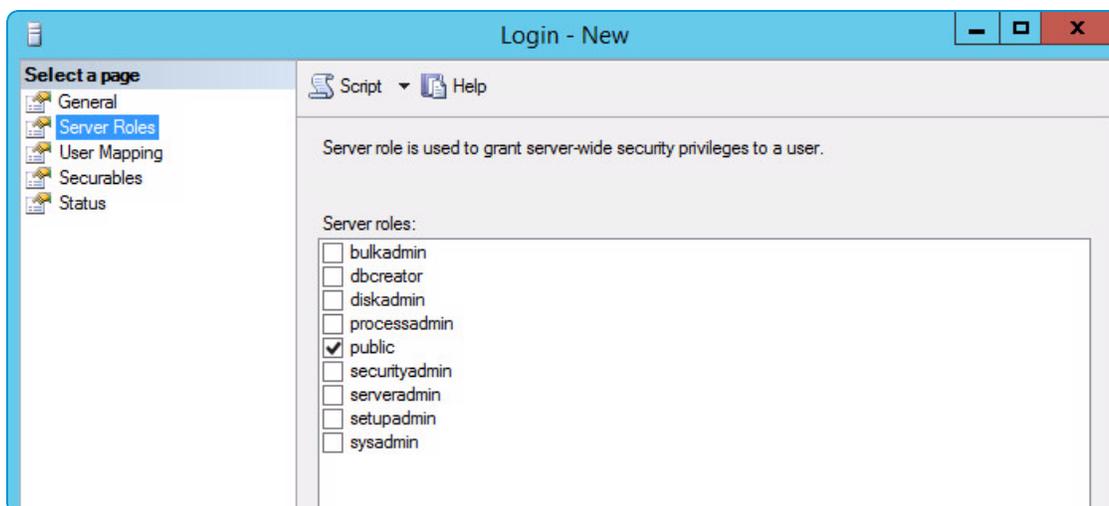
Create the AirWatch SQL Service Account and Assign DB Owner Roles

After you create the AirWatch database, you must configure the credentials of the SQL user that will run the AirWatch database setup utility.

1. Open SQL Server Management Studio.
2. Log in to the DB server containing the AirWatch database.

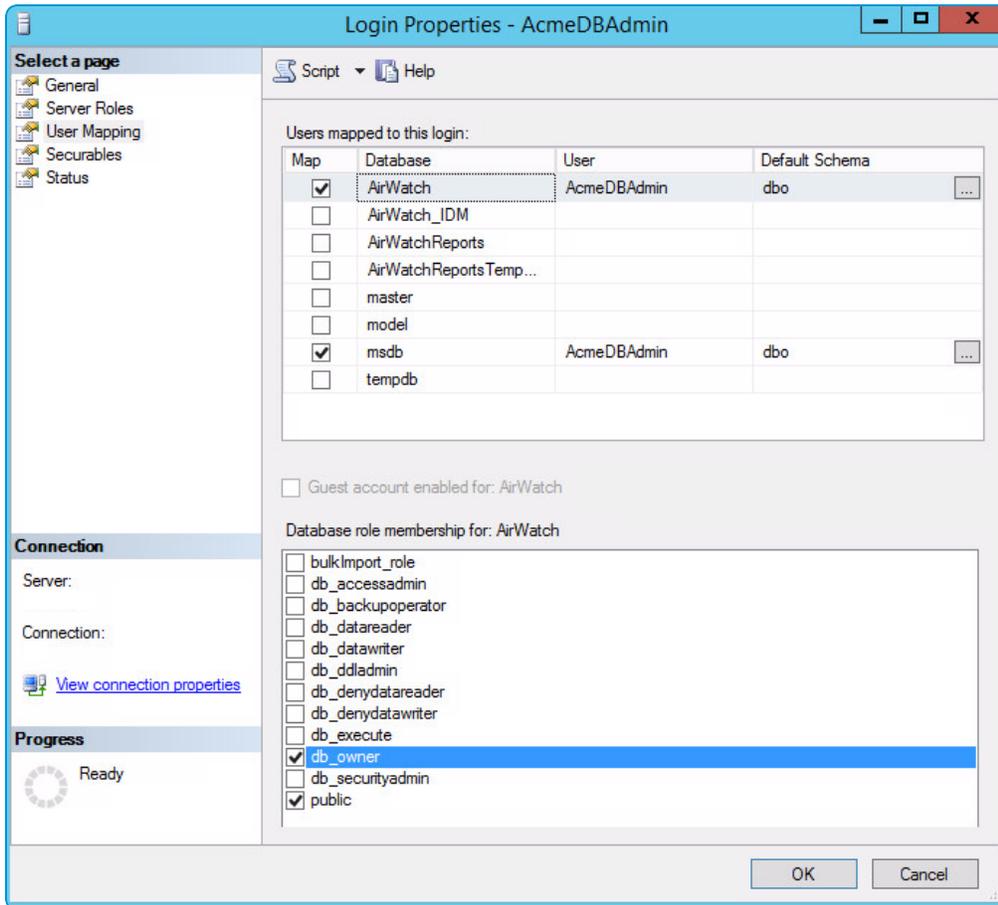


3. Navigate to **Security > Login**, right-click, and select **New Login**.
4. Select whether to use your **Windows** account or local **SQL Server** account for authentication. For SQL Server authentication, enter your user credentials.
5. Select the AirWatch database as the **Default database**.
6. Navigate to the **Server Roles** tab. Select server role as **Public**.

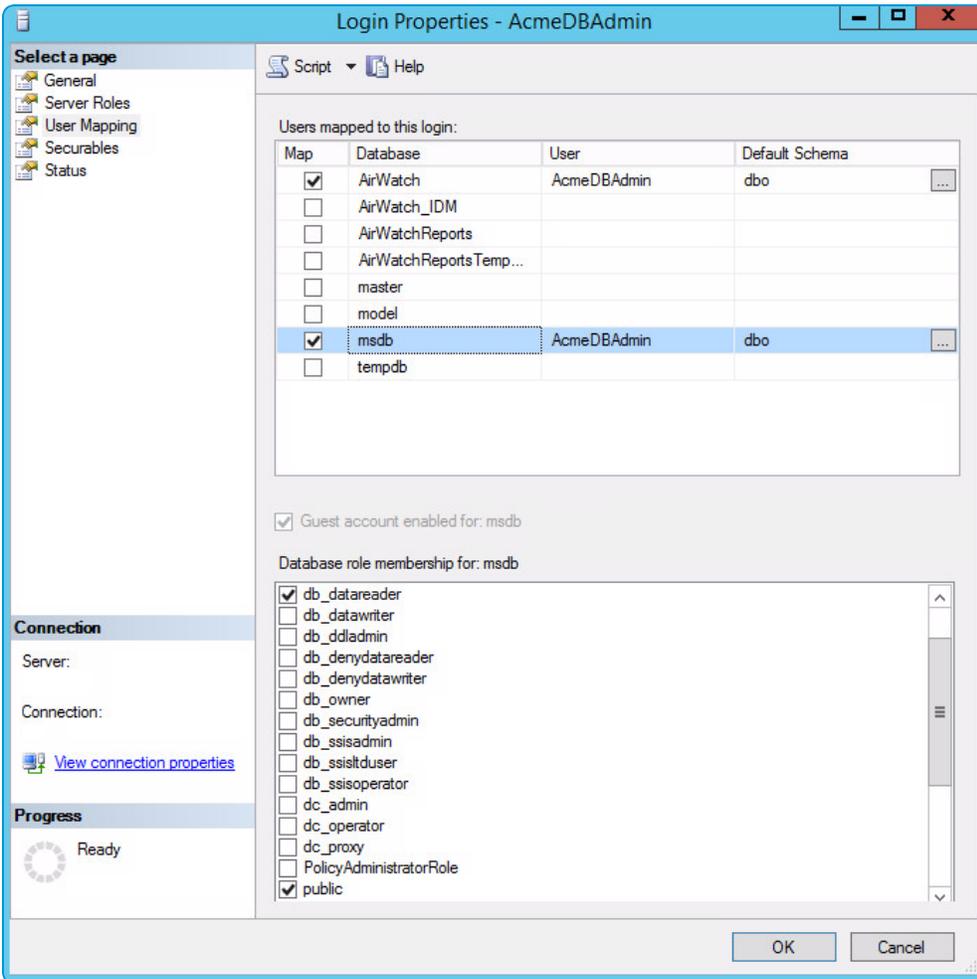


7. Select **User Mapping**.
 - Select the AirWatch Database. Then, select the **db_owner** role.

For a successful installation, you must ensure that the SQL User you are planning to run the AirWatch Database Script with has the database db_owner role selected.



- Select the msdb Database. Then, select the **SQLAgentUserRole** and **db_datareader** roles. SQLAgentUserRole is not pictured below due to space constraints.

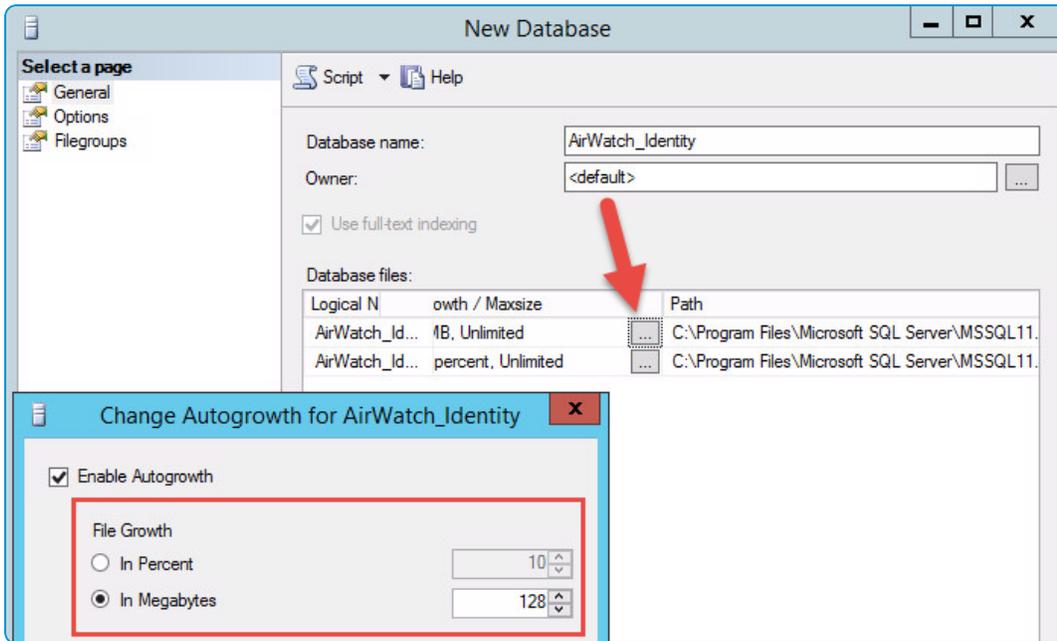


8. Select OK.

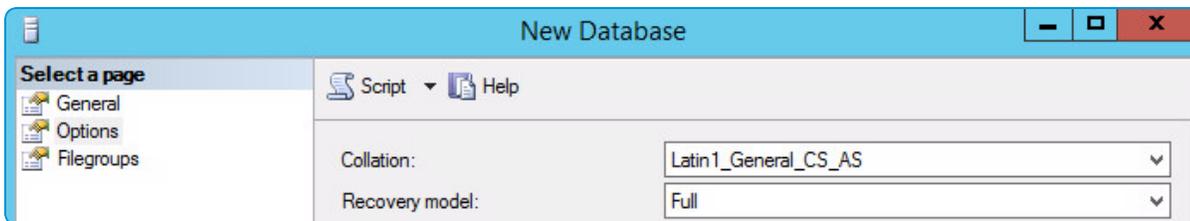
Create the VMware Identity Manager Service Database

If you are installing the VMware Identity Manager service as part of a Workspace ONE installation, then you must create a separate VMware Identity Manager services database.

1. On the SQL Server, open SQL Server Management Studio.
2. Log in using your user name and password.
3. Click **Connect**.
4. Right-click **Databases** and select **New Database**.
5. Enter **AirWatch_IDM** as the Database name.
You can customize the IDM database name. This guide uses **AirWatch_IDM** as the database name throughout.
6. Scroll to the right side of Database files, select the ... next to **Autogrowth**, and change **File Growth** to "In Megabytes" and the size to **128**, then select **OK**.



7. Select **Options**, and set the Collation to **Latin1_General_CS_AS**.

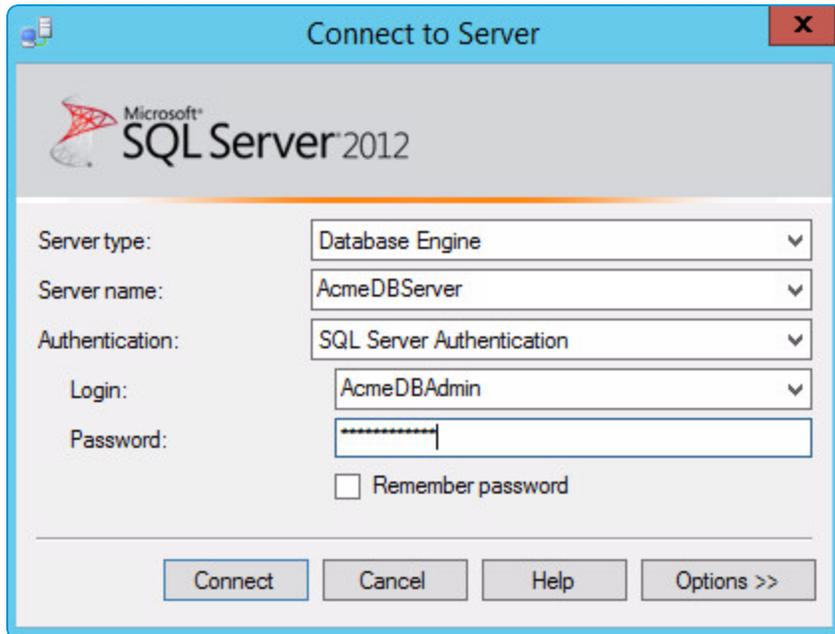


8. Under **Options**, set READ_COMMITTED_SNAPSHOT to **ON**.
9. Select **OK** to create the AirWatch_IDM database.
10. Expand **Databases** and verify the AirWatch_IDM database is created.

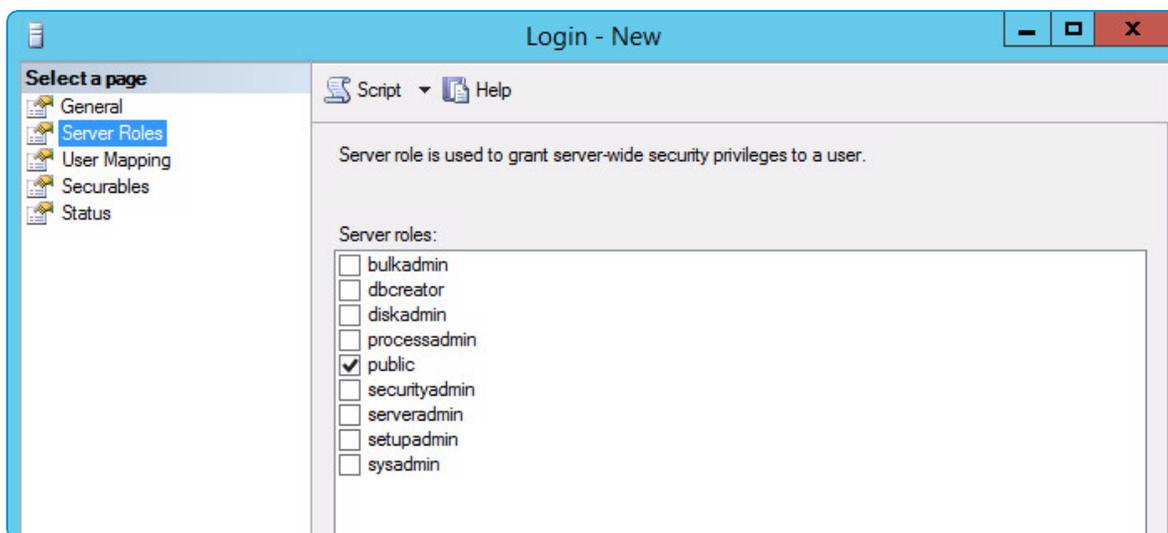
Create the Identity Service SQL Service Account and Assign DB Owner Roles

After you create the AirWatch Identity Service database, you must configure the credentials of the SQL user that will run the AirWatch database setup utility.

1. Open SQL Server Management Studio.
2. Log in to the DB server containing the AirWatch Identity Service database.

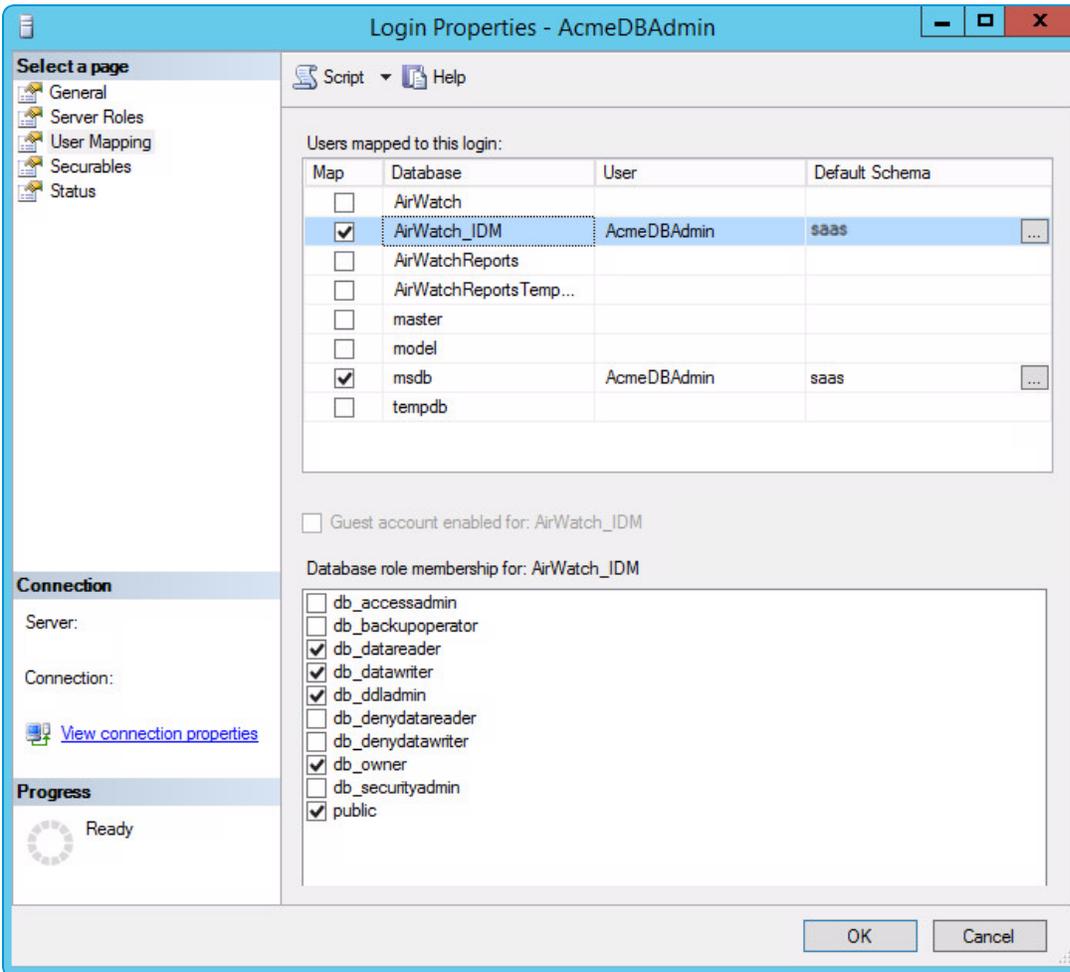


3. Navigate to **Security > Login**, right-click, and select **New Login**.
4. Enter your **SQL Server** account credentials for authentication.
5. Select the AirWatch_IDM database as the **Default database**. If **User must change password** is selected, then you must change the password before running the application server installer. To avoid this step, uncheck this option.
6. Navigate to the **Server Roles** tab. Select server role as **Public**.



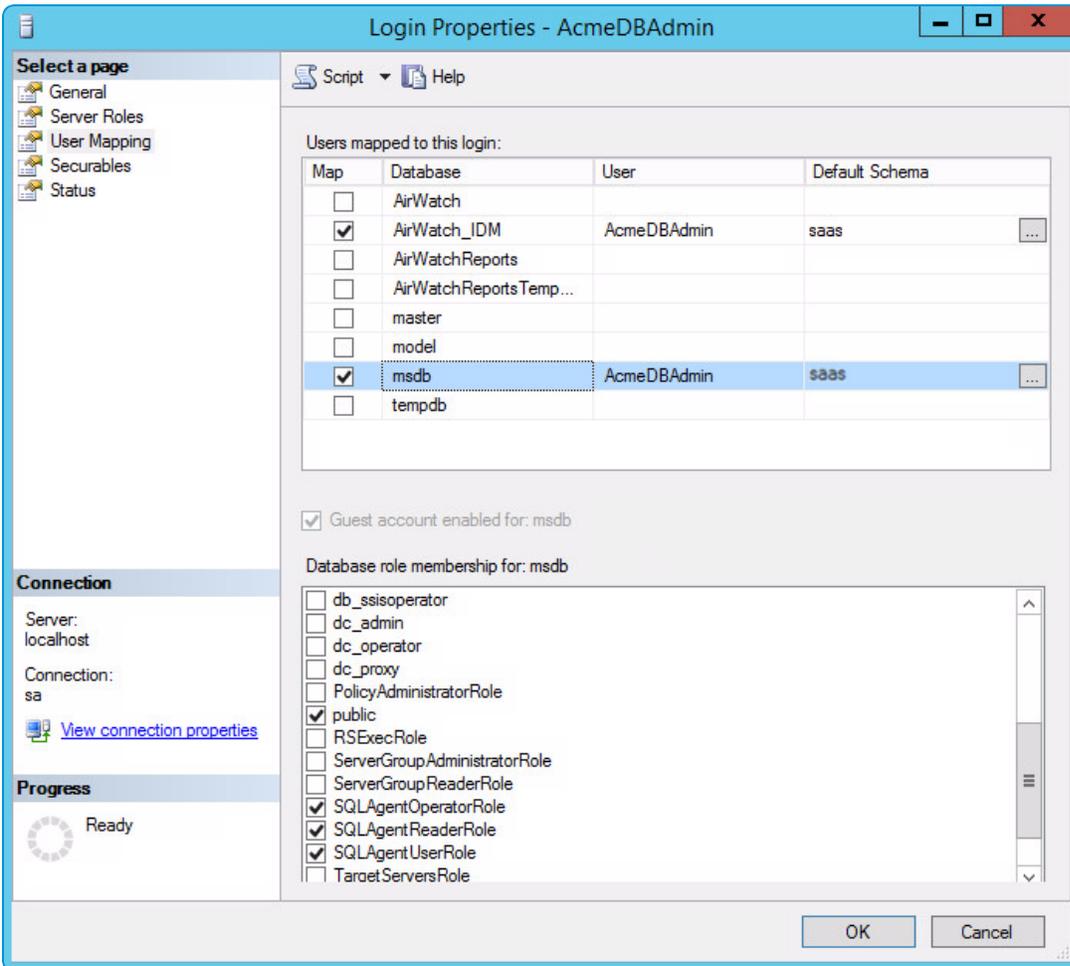
7. Select **User Mapping**.
 - Select the AirWatch_IDM database. Then, select the **db_owner**, **db_datareader**, **db_datawriter**, **db_ddladmin**, and **public** roles.

For a successful installation, you must ensure that the SQL User you are planning to run the AirWatch Database Script with has the database db_owner role selected.



Make sure that the AirWatch database default schema is set to **saas**. Only the saas schema can be used in the Identity Manager database.

- Select the msdb Database. Then, select the **public**, **SQLAgentUserRole**, **SQLAgentOperatorRole**, **SQLAgentReaderRole** and **db_datareader** roles. Note that **db_datareader** is not pictured below due to space constraints.



Make sure that the AirWatch database default schema is set to **saas**. Only the saas schema can be used in the Identity Manager database.

8. Select **OK**.

Configure your Application Servers

The AirWatch installer configures the following roles and permissions as part of the installation. If you prefer to configure these manually, or to verify them, you can use the procedure below.

1. On the **AirWatch Console Server** and **AirWatch Device Services Server**, from the Taskbar, open **Server Manager** and select **Manage > Add Roles and Features**. Click **Next** to advance to the **Server Roles** tab.
2. Expand Web Server (IIS), and under it expand Web Server.
3. Verify that the following role services are enabled (most may already be enabled):
 - **Common HTTP Features:** Static Content, Default Document, Directory Browsing, HTTP Errors, HTTP Redirection
 - **Application Development:** ASP.NET, .NET Extensibility, ASP, ISAPI Extensions, ISAPI Filters, Server Side Includes

When ASP.NET is selected, select Add Required Features to associate features with the ASP framework. Ensure that other required role services are enabled.

- **Health and Diagnostics:** HTTP Logging, Logging Tools, Request Monitor, Tracing
 - **Security:** Request Filtering, IP, and Domain Restrictions
 - **Performance:** Static Content Compression, Dynamic Content Compression
 - **Management Tools:** IIS Management Console and IIS 6 Metabase Compatibility
 - Ensure WebDAV is not installed.
4. Click **Next**.
 5. On the **Features** tab, verify the following required features are added:
 - **.NET Framework 4.6.2 Features:** Entire module (.NET Framework and WCF Activation)
When .NET is selected, select Add Required Features, to associate features with the .NET framework. Expand to verify every .NET/WCF feature is enabled. For a 2012 R2, .NET Framework 4.6.2 Features is required.
 - **Message Queuing:** Message Queuing Server (expand Message Queuing > Message Queuing Services to select)
 - **Telnet Client**
 6. Click **Next** and verify that the features which must be enabled have been so enabled.
 7. Select **Install**.
 8. When the installation is finished, verify that the Installed succeeded messages are shown, then select **Close**.

Install URL Rewrite Module 2.0

The URL Rewrite Module 2.0 cannot be installed until the IIS role is installed.

1. Navigate to <http://www.iis.net/downloads/microsoft/url-rewrite#additionalDownloads> and download the appropriate version for your install.
2. Run the installer and accept the defaults for installation.

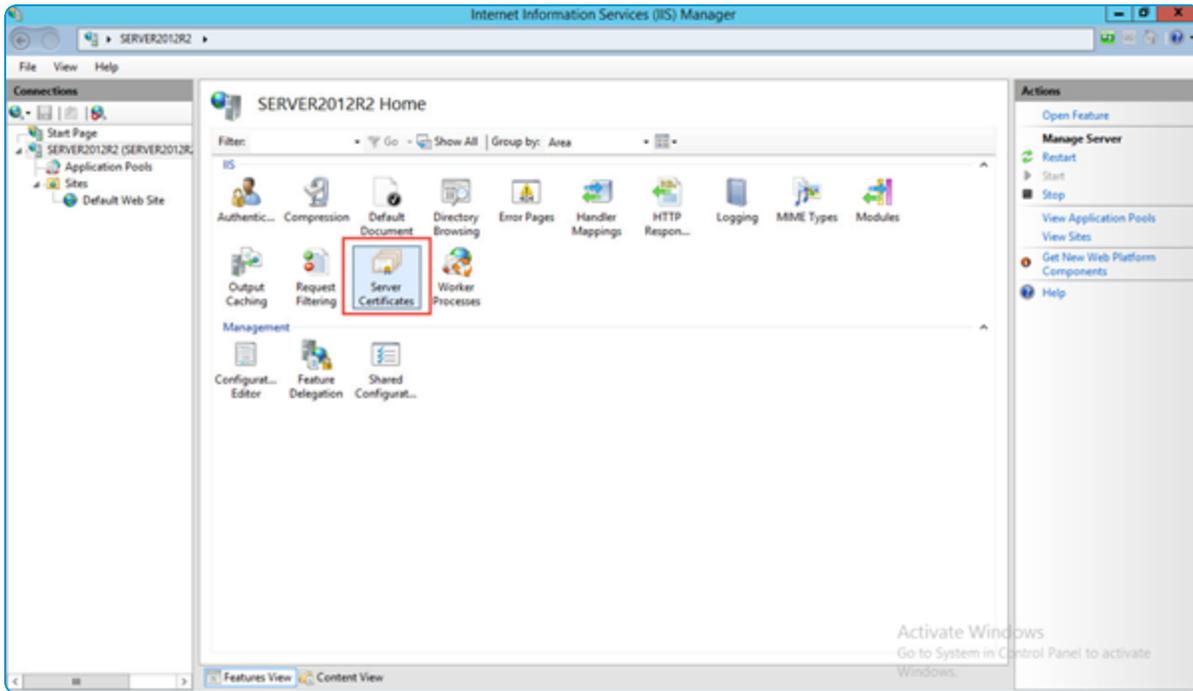
Configure Your Internal DNS Record and Certificates

An internally registered DNS record is for devices connecting over your organization's internal Wi-Fi network, and it tells them how to connect to AirWatch (specifically, the Device Services server). An internal DNS record must be registered on the internal domain server.

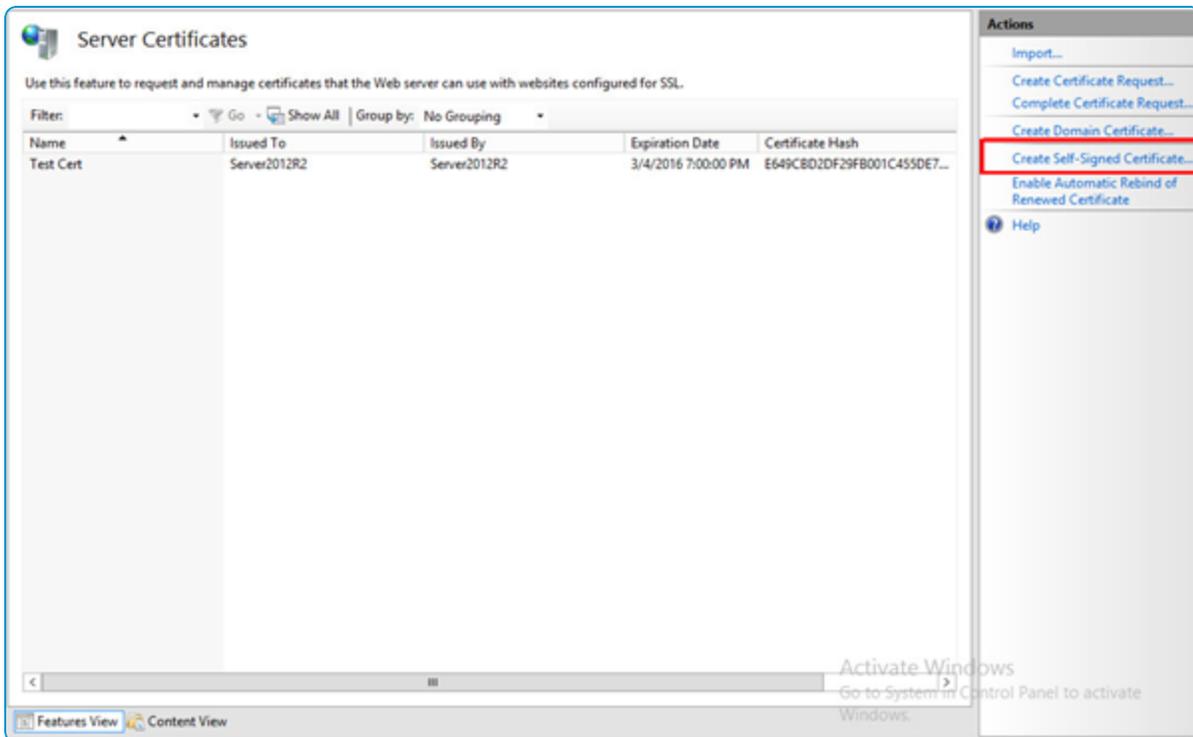
In the standard, multi-server deployment, you must generate a self-signed certificate for your Console server (or you can use an internally issued certificate).

The externally available URL of the AirWatch server must be set up with a trusted SSL certificate. A wildcard or individual Web site certificate is required.

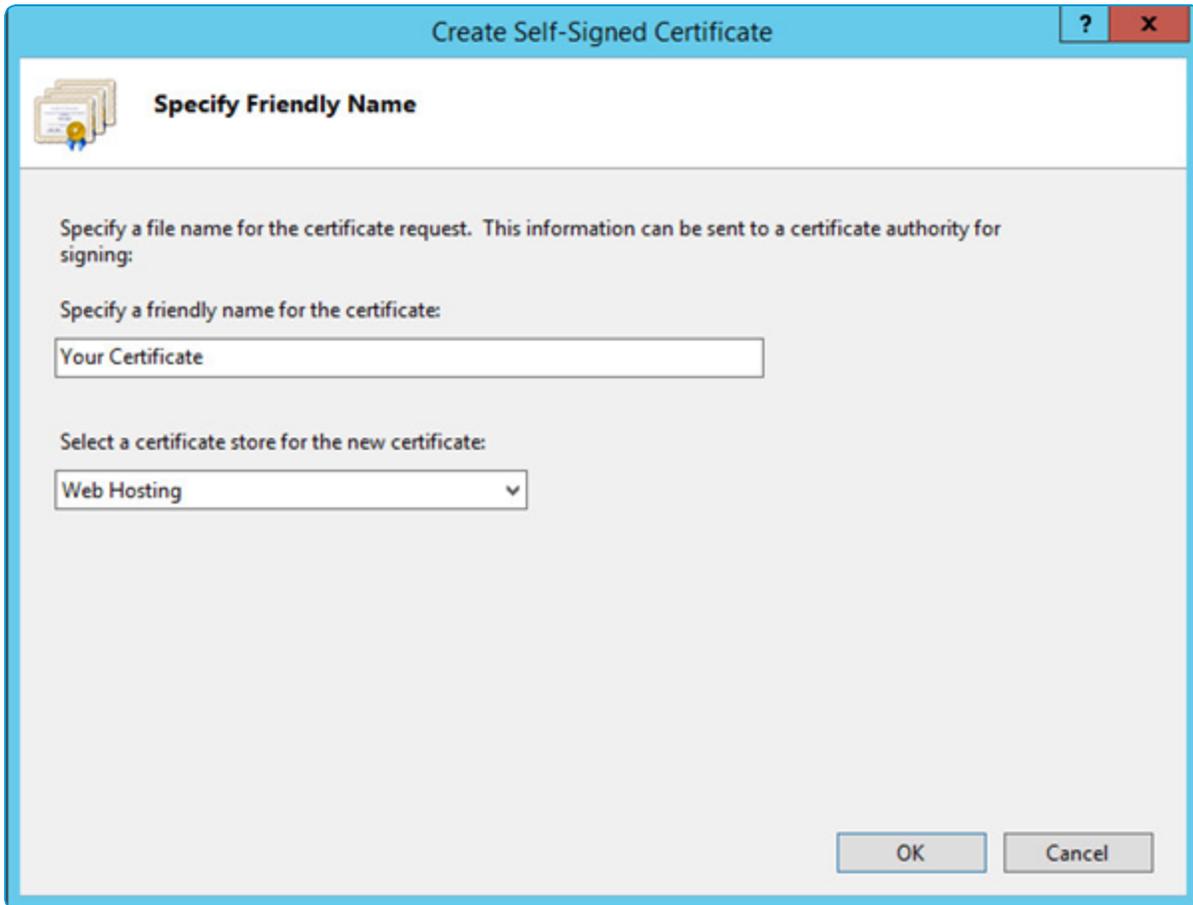
1. Open **Server Manager** and navigate to **Roles > Web Server (IIS)**.
2. Click the **Server Name**.
3. Double-click **Server Certificates**.



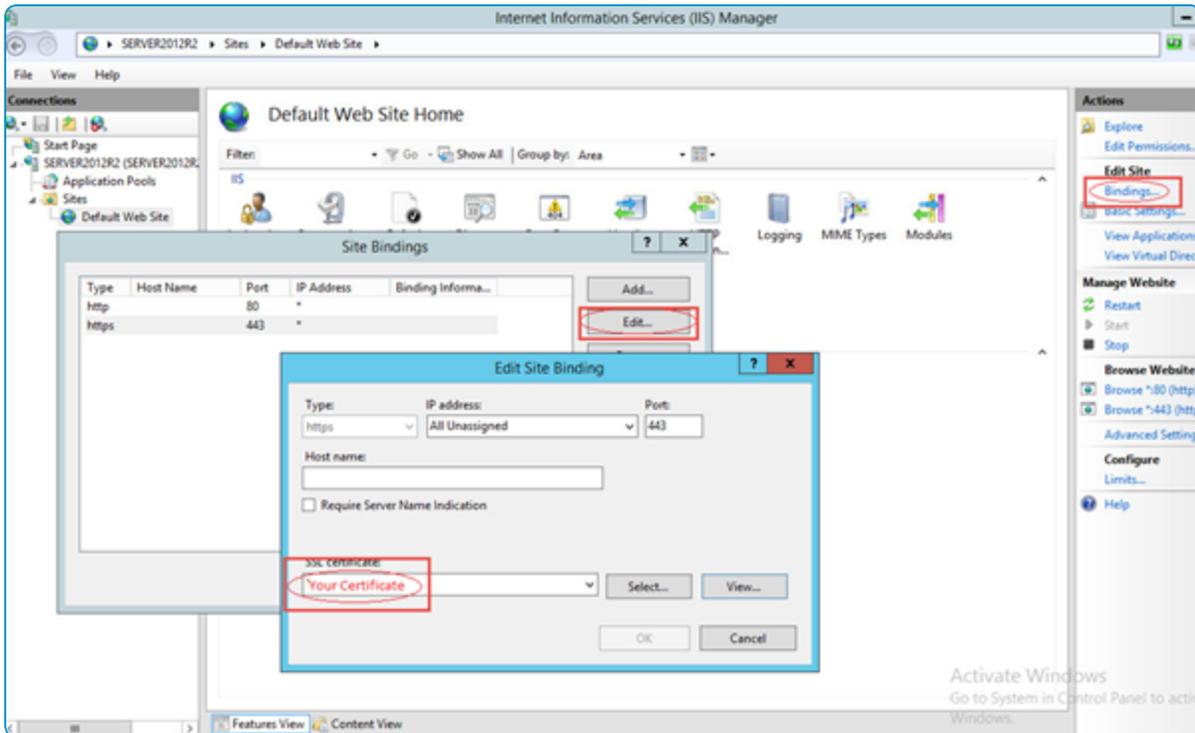
4. On the right, select **Create Self-Signed Certificate**.



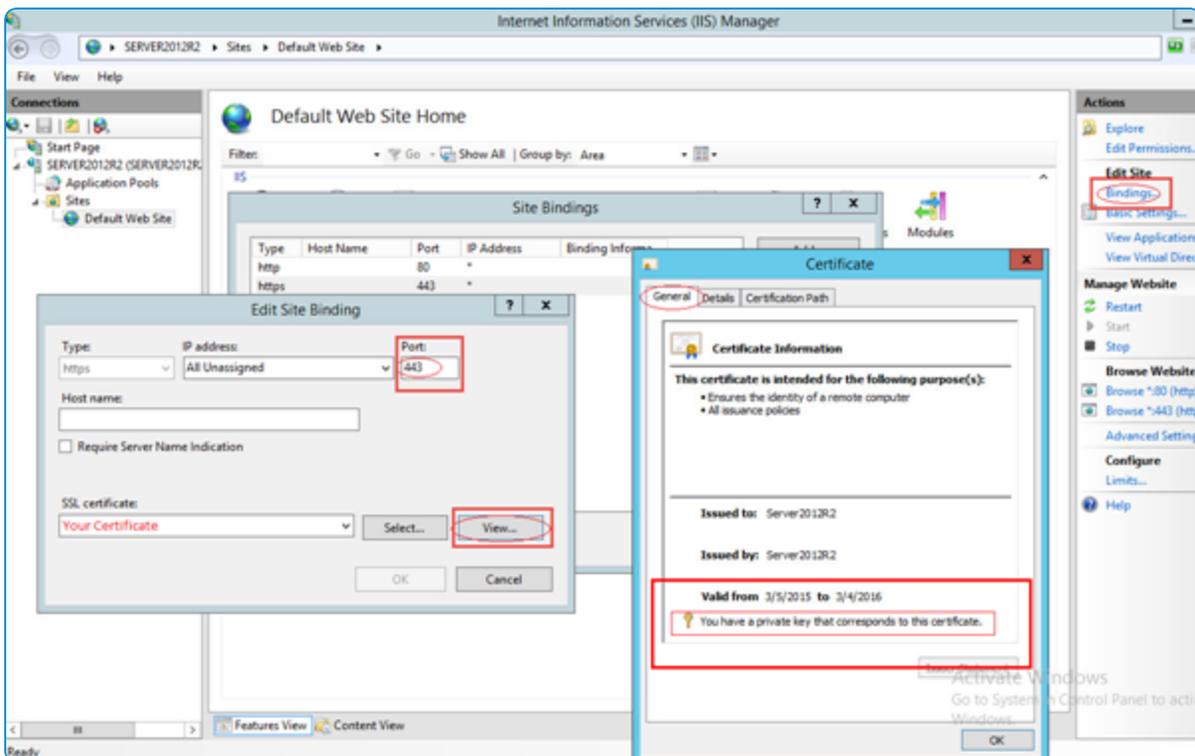
5. Enter the friendly name (FQDN) and select OK.



- Next you can add a 443 binding to the Default Web site in IIS. The bindings for a completed server look like the following. Your SSL certificate appears in the drop-down menu of available certificates.



7. Also verify that you have a private key that corresponds to your certificate.



Configure Your External DNS Record and Certificates

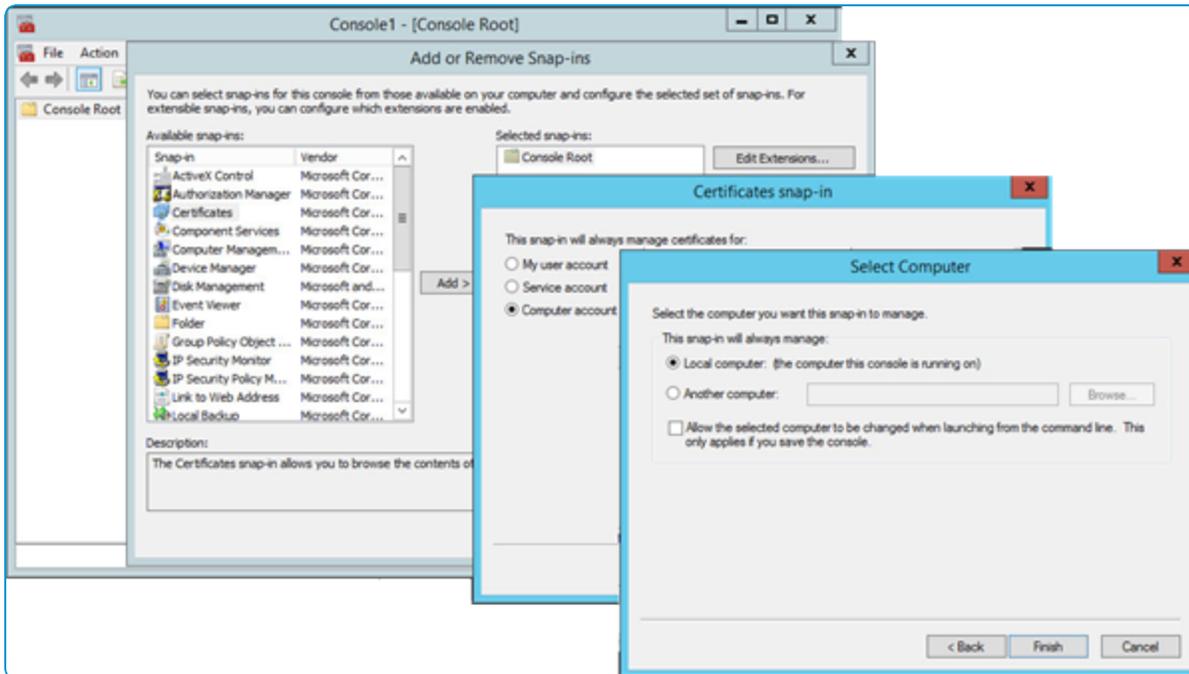
The two main components of AirWatch are the Device Services server and the Console server. In the standard deployment model, these components are installed on separate servers, and only the Device Services component requires an external DNS record, while the Console component can remain only internally available.

An externally registered DNS record is a friendly name that refers to the IP to tell external devices how to connect to AirWatch (the Device Services server). This externally available URL must be set up with a trusted SSL certificate that is trusted by all device types. For Apple, you can see a list of root certificates that are natively trusted by iOS on the Apple Support webpage. For other OEMs, check with the OEM to see which third-party certificate authorities are natively trusted. You can also typically retrieve this information from the device by looking for the Trusted Root CAs under Settings.

A wildcard or individual Web site certificate is required.

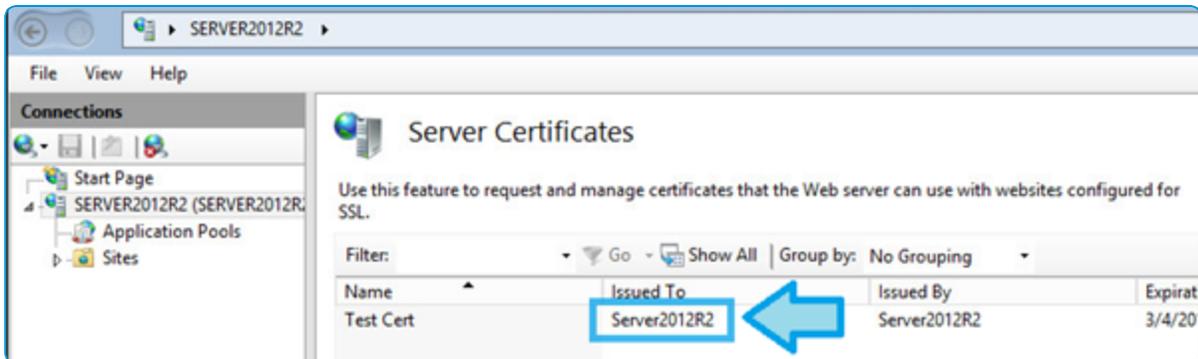
Important: Ensure that these steps are performed on both the AirWatch Console and Device Services servers.

1. Obtain SSL certificates for each of your external DNS entries. A list of root certificates natively trusted by iOS can be found here: <http://support.apple.com/kb/HT5012>
2. On the **AirWatch Console** and **Device Services Servers**, open **mmc**:
 - a. Start > Run
 - b. Type mmc
 - c. Select OK
3. In mmc, navigate to **File > Add/Remove Snap-in ...**
4. Select **Certificates** from the list of add-ins and select **Add**.
5. Choose **Computer account** and select **Next**.
6. Keep **Local computer** selected and select **Finish** and **OK**.



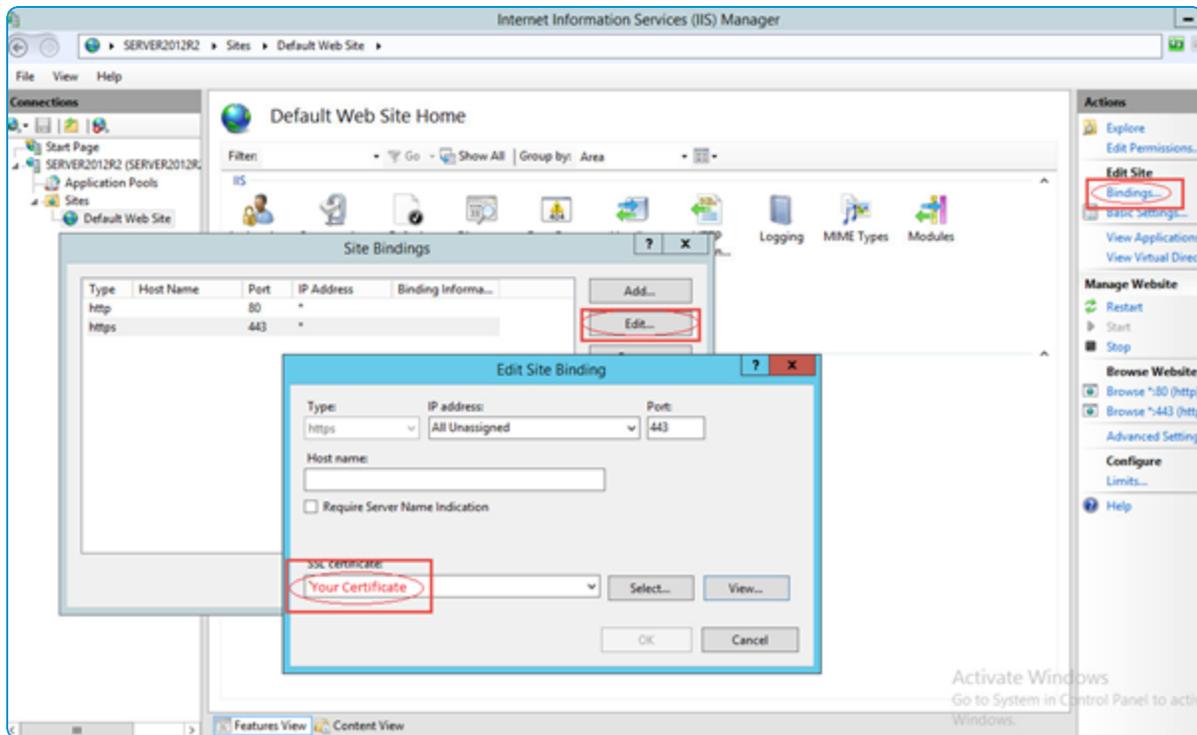
7. Expand the **Certificates** folder and right-click **Personal**.
8. Select **All Tasks** and choose **Import**.
9. In the **Certificate Import Wizard**, select **Next** and perform the following steps:
 - a. Click **Browse** and navigate to the **Cert** folder, which was staged earlier, and change the file type drop-down to **All Files**.
If the drop-down is not changed to All Files, the certificate cannot be selected for import.
 - b. Select the appropriate certificate and select **Open**.
In a standard, multi-server installation, this certificate is the external third-party certificate for the DS server and for the Console it can be a self-signed or internally issued certificate.
This certificate must be a PFX file.
 - c. Click **Next**, and complete the following settings:
 - Password: Your certificate password
 - Mark this key as Exportable: enable
This is optional and allows you to export the certificate from this server to use it on another server.
 - Include all extended properties: enable
 - d. Click **Next** and select **Finish**.
 - e. Select **OK** to close the “**The import was successful**” pop-up.
10. Expand the **Personal** folder to show the **Certificates** folder
11. Drag the **Root CA Certificate** into the **Trusted Root Certification Authorities** folder. Navigate to **Trusted Root Certification Authorities > Certificates** to verify that the move was successful.

12. Navigate back to the **Personal** folder to show the **Certificates** folder, and drag the **Intermediate CA Certificate** into the **Intermediate Certification Authorities** folder. Navigate to **Intermediate Certification Authorities > Certificates** to verify that the move was successful.
13. Select **File > Exit** to close mmc. Select **No** to save changes.
14. Open Server Manager, select **Roles** and expand: **Web Server (IIS) > Information Services (IIS) Manager**.
15. In the right pane, under **Connections**, select the server.
16. Under the IIS section, double-click on **Server Certificates** and verify that the certificate is located in the certificate list. An example is shown.



Once uploaded on your server you can use it to add a 443 binding to the Default Web site in IIS. Your SSL certificate appears in the drop-down menu of available certificates.

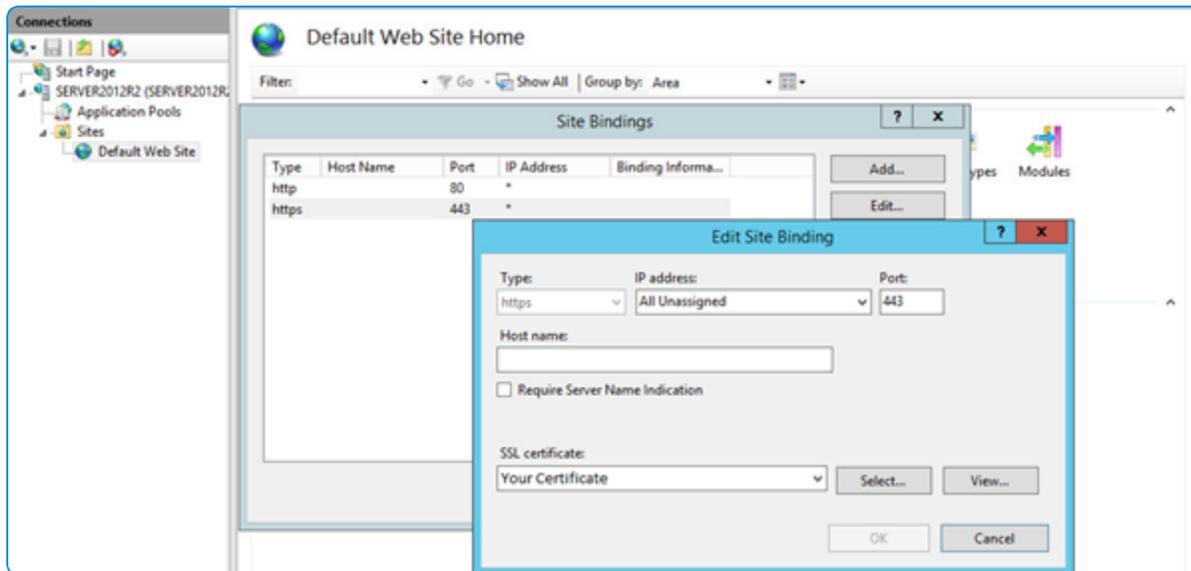
17. Under **Connections**, expand **Sites** and select **Default Web Site**.



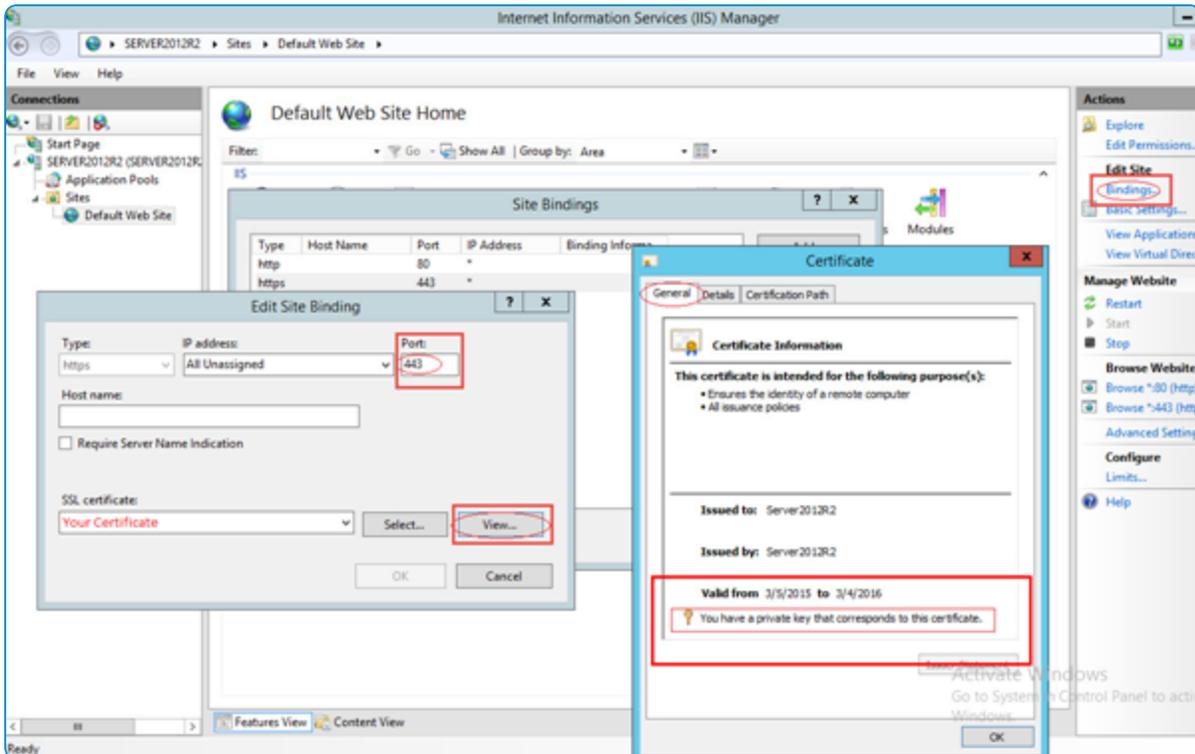
18. Under **Actions**, to the far right side, under **Edit Site**, select **Bindings** and select **Add...**

19. Configure the following settings:
 - Type: https
 - SSL certificate: Your certificate
20. Click **OK** and select to **Close**.

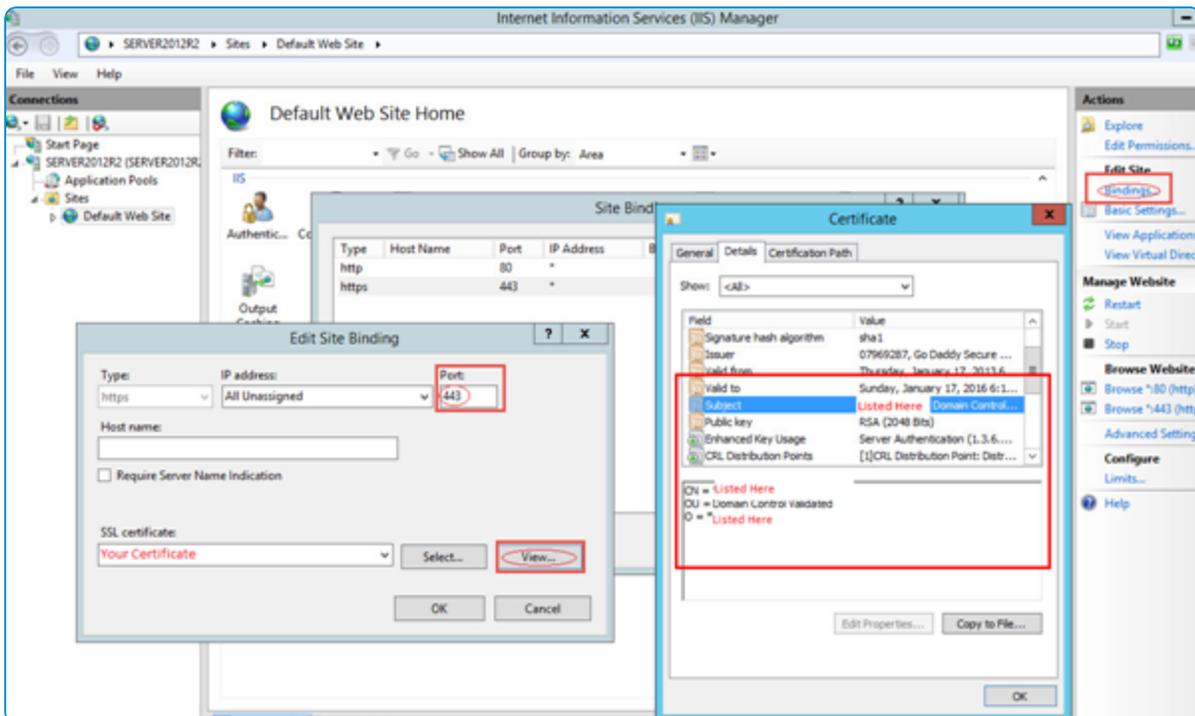
The IP address and Port are not altered. Do not populate the Hostname with an IP or DNS entry, since it affects the functionality of the SSL binding. A slight delay occurs when the certificate is bound to the Web site.



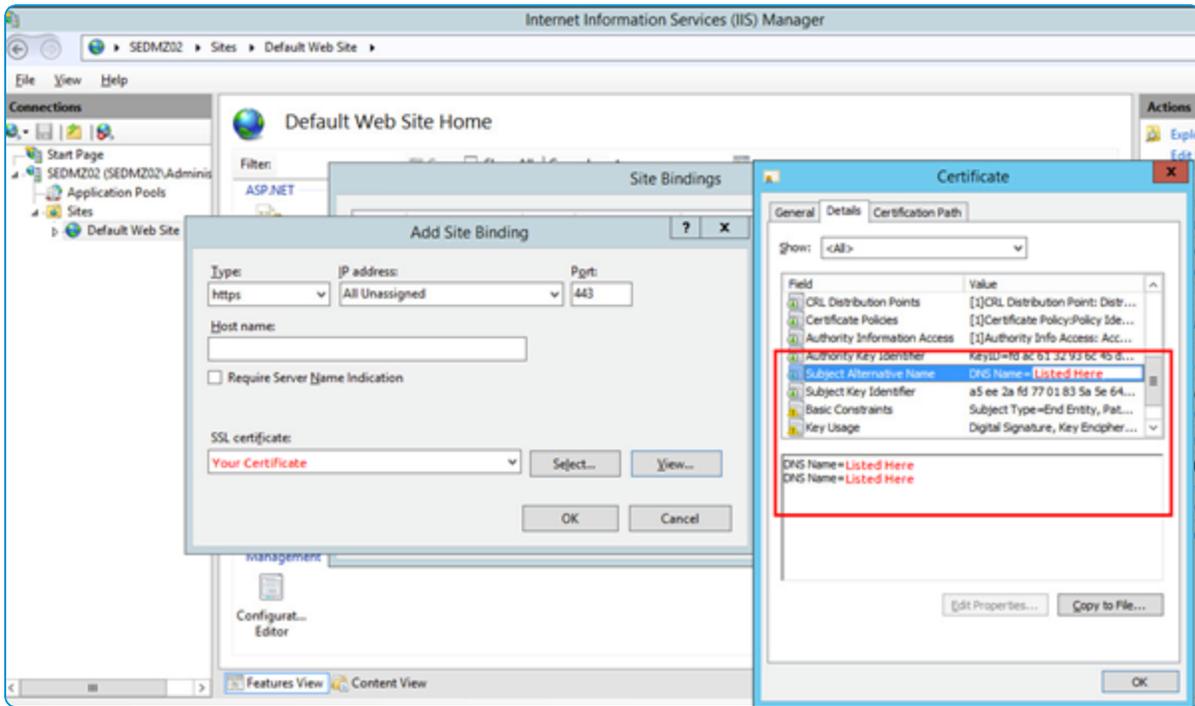
21. Click **OK** and select to **Close**.
22. Under **Actions/Browse Web Site**, verify **Browse *.443 (https)** is an available option.
23. Also verify that you have a private key that corresponds to your certificate.



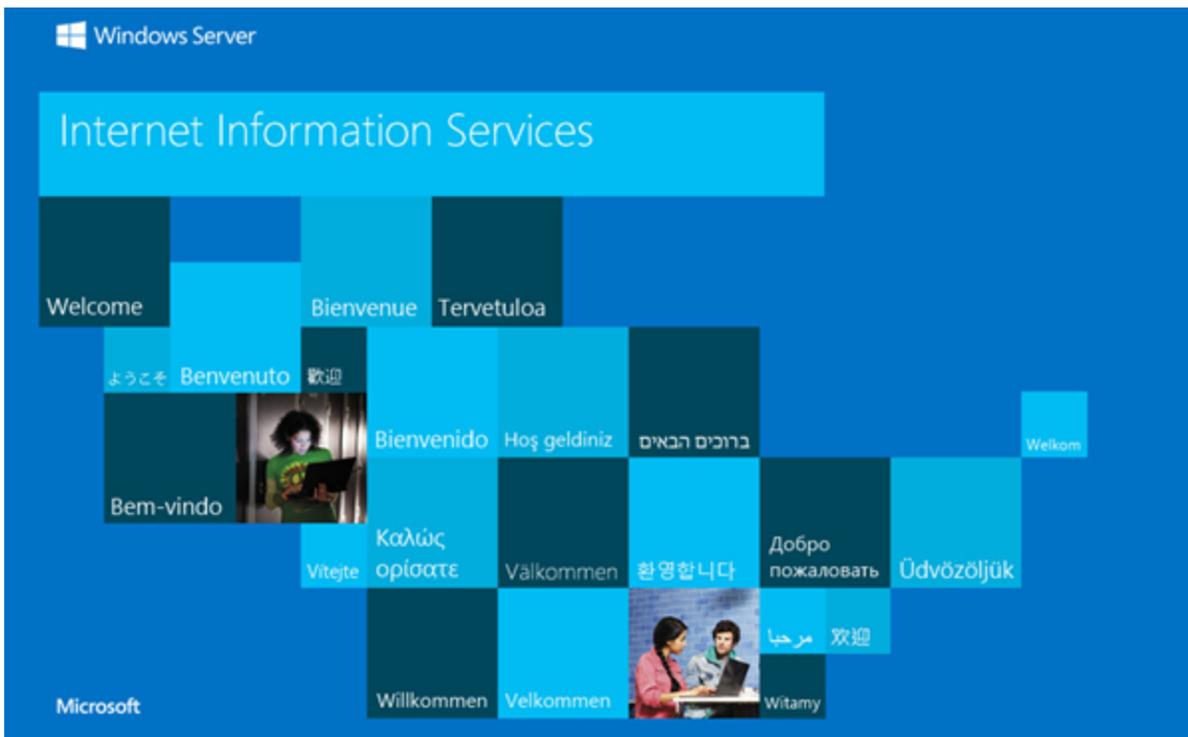
24. Verify that the certificate contains the common name in the subject.



25. Verify that your DNS name is listed in the Subject Alternative Name.



26. Validate that you can connect to the server over HTTPS (<https://yourAirWatchDomain.com>). At this point, the IIS splash page displays.



Important: If SSL is used for Admin Console access, ensure that FQDN is enabled or host file is configured.

Stage Install Files

After meeting the database and application server prerequisites and configuring your internal and external DNS, you can stage the install files on the appropriate Console, Device Services, and SQL servers.

To stage the install files:

1. Download the latest GA or Feature Pack Full Installer.zip file from the Resource Portal. Receive a direct link to the files from your AirWatch consultant as part of the deployment process.
2. Unzip the files on to the appropriate server.
3. Extract the contents.

Workspace ONE Validation Tool

Use the Workspace ONE Validation Tool to verify that your system and components are properly configured.

The Workspace ONE Validation Tool collects and analyzes configuration data from the target AirWatch and Workspace ONE environments to validate that your environment is ready for a successful SaaS or on-premises deployment.

The utility validates the Database, Console, Device Services, AirWatch Cloud Messaging, VMware Enterprise Systems Connector, Secure Email Gateway, and Email Notification Service. Each of these components has different software and networking requirements, such as OS, Database, CPU, RAM, JRE, network security, Server Manager, DNS, certificates, and Email infrastructure.

The tool generates a customized report that validates that the environment is deployment-ready.

You can check your configuration to perform:

- A system health check.
- A validation before or after an install or upgrade to your AirWatch version.
- Troubleshooting on network changes.
- A validation before or after a server migration.

To begin the installation validation, download the Workspace ONE Validation Tool from <https://resources.air-watch.com/view/vldrj3p3fb8mvzmrpj84>. Extract the ZIP file and open the InstallVerificationTool.exe file.

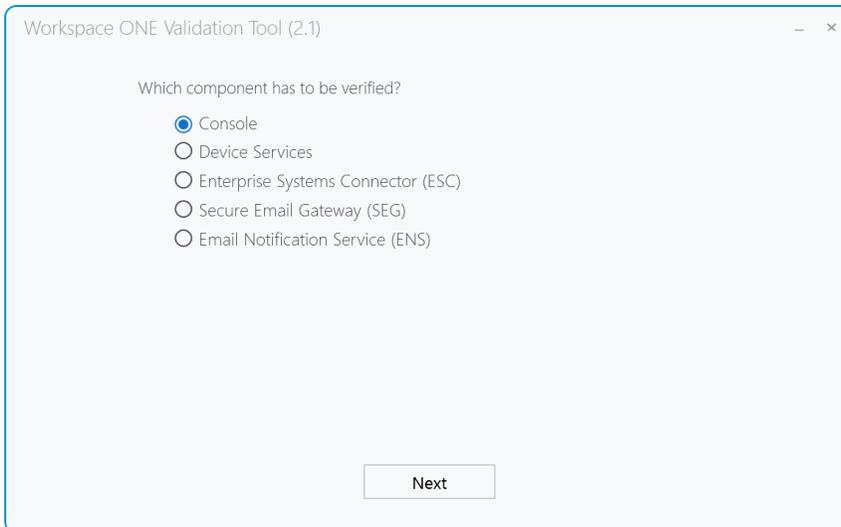
Next, select a component to validate:

- [Validate the VMware AirWatch Console on page 35](#)
- [Validate the VMware Device Services on page 37](#)
- [Validate the Email Notification Server on page 40](#)
- [Validate the VMware Enterprise Systems Connector on page 38](#)
- [Validate the Secure Email Gateway on page 40](#)

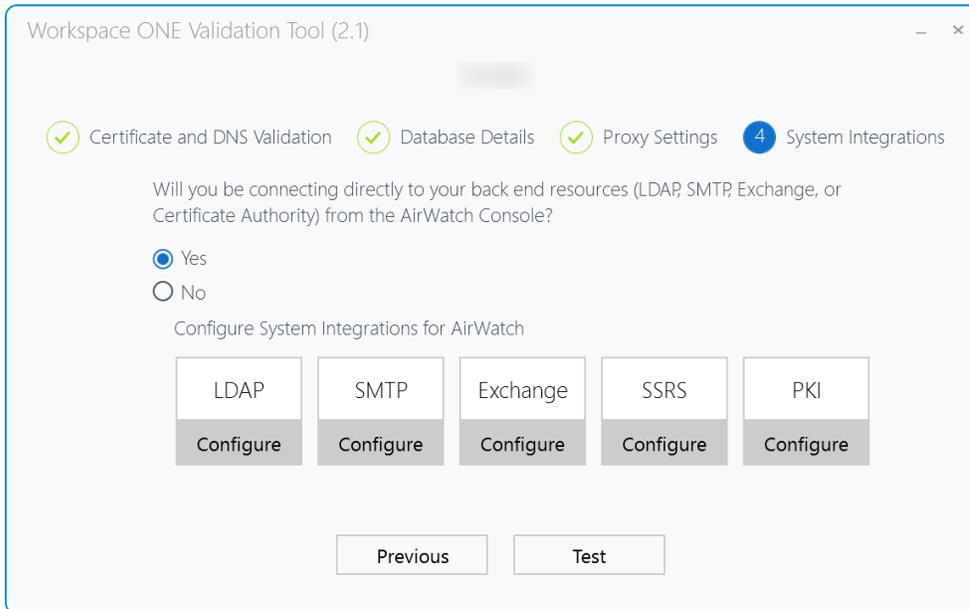
Validate the VMware AirWatch Console

Use the Workspace ONE Validation Tool to verify that your Windows machine is properly configured for a deployment of the VMware AirWatch Console.

1. Run the Workspace ONE Validation Tool. Select the **Console** option.



2. Enter the following Console information. Select **Next** at the end of each page.
 - a. Host URL
 - b. Database server
 - c. Database name
 - d. Authentication type: select **SQL Server** or **Windows**
 - e. Database user
 - f. Database password
 - g. Outbound connections by proxy: select **Yes** or **No**
 - If you select **Yes**, enter the **Proxy URL** and **Proxy port**, and select the **Authentication type**.
 - If your authentication type is **Password**, enter the **User name**, **Password**, and **Bypass List** information for your authentication strategy.
 - h. System integration configurations: select **Yes** or **No** to connect your back-end resources to the Console
 - If you select **Yes**, select the System Integration you want to configure, and enter the required integration information for your selection.



3. When you have entered all the required information, select **Test** to verify your Console configuration.
4. When the test results appear, you can **Export** the results or **Retry** the validation. For more information about using the results, see [Validation Tool Results on page 41](#).

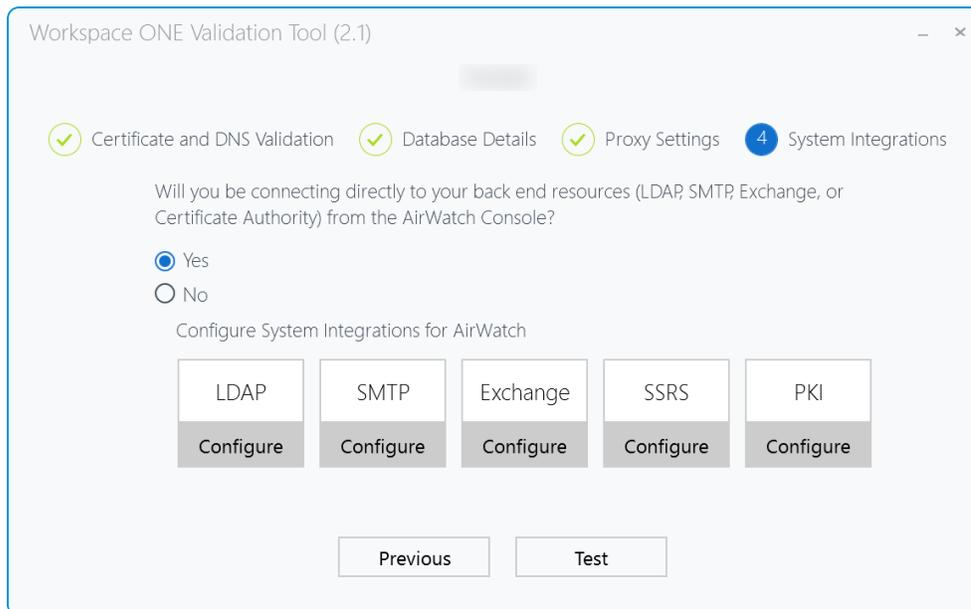
If the validation returns errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Validate the VMware Device Services

Use the Workspace ONE Validation Tool to verify that your instance of VMware Device Services is properly configured.

1. Run the Workspace ONE Validation Tool. Select the **Device Services** option.
2. Enter the following Device Services information. Select **Next** at the end of each page.
 - a. Host URL
 - b. Database server
 - c. Database name
 - d. Authentication type: select **SQL Server** or **Windows**
 - e. Database user
 - f. Database password
 - g. Outbound connections by proxy: select **Yes** or **No**
 - If you select **Yes**, enter the **Proxy URL** and **Proxy port**, and select the **Authentication type**.
 - If your authentication type is **Password**, enter the **User name**, **Password**, and **Bypass List** information for your authentication strategy.

- h. System integration configurations: select **Yes** or **No** to connect your back-end resources to Device Services
- o If you select **Yes**, select the System Integration that you want to configure and enter the required integration information for your selection.



3. When you have entered all the required information, select **Test** to verify your Device Services configuration.
4. When the test results appear, you can **Export** the results or **Retry** the validation. For more information about using the results, see [Validation Tool Results on page 41](#).

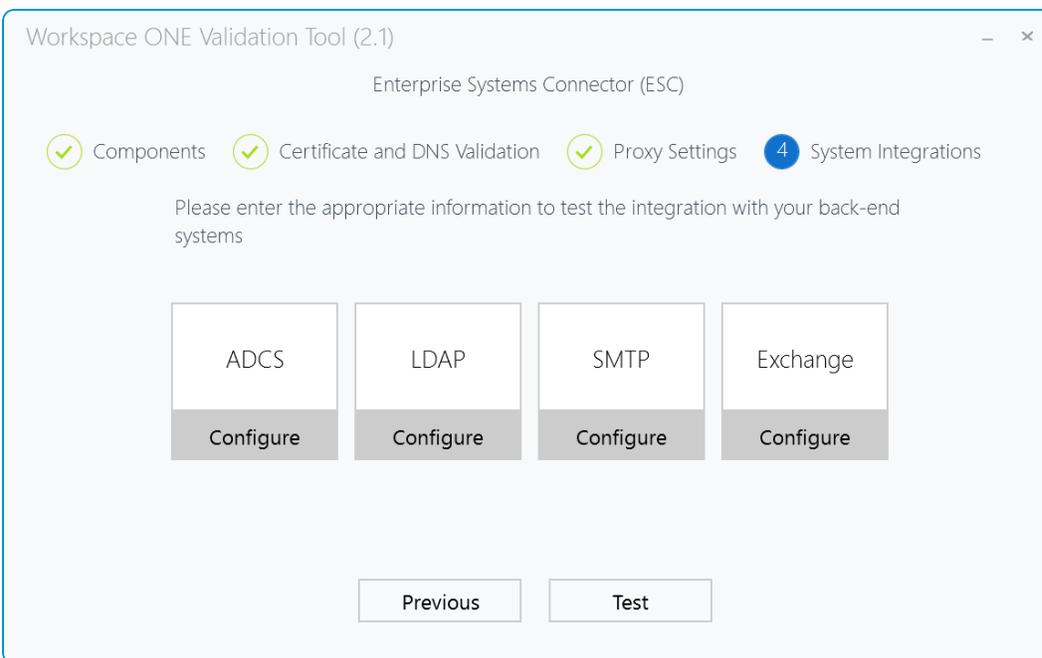
If the validation returns errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Validate the VMware Enterprise Systems Connector

Use the Workspace ONE Validation Tool to verify that your instance of VMware Enterprise Systems Connector is properly configured.

1. Run the Workspace ONE Validation Tool. Select the **Enterprise Systems Connector** option.
2. Select the components to test: **AirWatch Cloud Connector** and **VMware Identity Manager Connector**. You can select one or both components. Select **Next**.
3. Enter the following Certificate and DNS Validation information. The fields that appear depend on your selection in the previous page.
 - a. AirWatch Cloud Connector:
 - Enter the **Console URL**.
 - Enter the **AWCM URL**.
 - Enter the **API URL**.

- b. VMware Identity Manager Connector
 - Enter the **IDM URL**.
 - Enter the **ESC URL (FQDN)**.
 - Select **Yes** to integrate with **RSA SecureID** and enter the **RSA Server URL**.
 - Select **Yes** to integrate with **Horizon View** and enter the **Horizon View URL**.
 - Select **Yes** to integrate with **Citrix-published resources** and enter the **Citrix URL**.
4. Configure outbound connections by proxy.
 - Select whether your outbound configurations operate using a proxy.
 - If you select **Yes**, enter the **Proxy URL** and **Proxy port**, and select the **Authentication type**.
 - If your authentication type is **Password**, enter the **User name**, **Password**, and **Bypass List** information for your authentication strategy.
5. System integration configurations: select **Yes** or **No** to connect your back-end resources to Device Services
 - If you select **Yes**, select the System Integration that you want to configure and enter the required integration information for your selection.



6. When you have entered all the required information, select **Test** to verify your Enterprise Systems Connector configuration.
7. When the test results appear, you can **Export** the results or **Retry** the validation. For more information about using the results, see [Validation Tool Results on page 41](#).

If the validation returns errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Validate the Secure Email Gateway

Use the Workspace ONE Validation Tool to verify that your instance of VMware Secure Email Gateway (SEG) is properly configured.

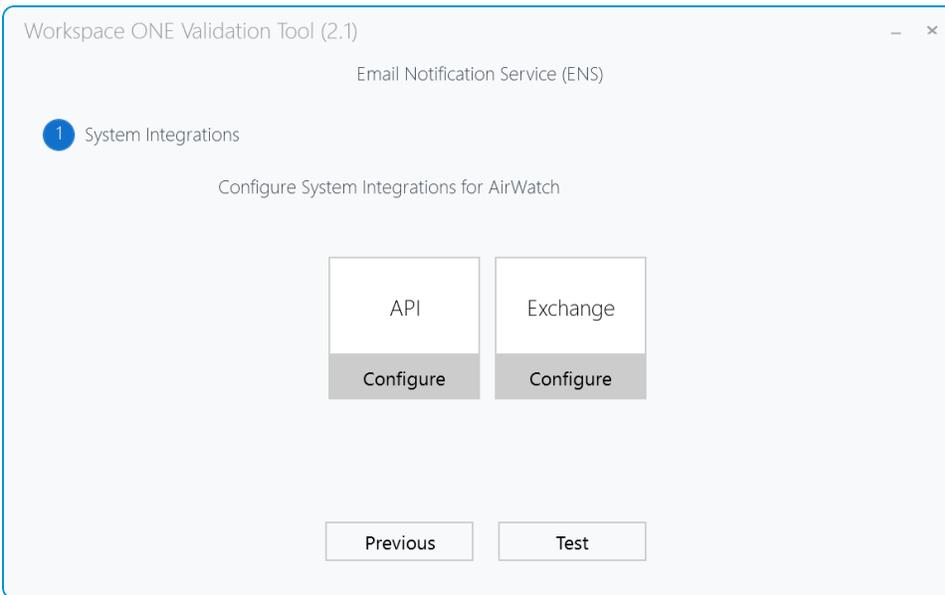
1. Run the Workspace ONE Validation Tool. Select the **Secure Email Gateway** option.
2. Select the SEG version (**Classic SEG** or **V2 SEG**) to test. Select **Next**.
3. Enter the following Certificate and DNS Validation information.
 - a. Enter the **Server URL**.
 - b. Enter the **AWCM URL**.
 - c. Enter the **API URL**.
4. Configure the system integration settings to test.
 - Select **Microsoft Exchange** and enter the required integration information.
5. When you have entered all the required information, select **Test** to verify your Secure Email Gateway configuration.
6. When the test results appear, you can **Export** the results or **Retry** the validation. For more information about using the results, see [Validation Tool Results on page 41](#).

If the validation returns errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Validate the Email Notification Server

Use the Workspace ONE Validation Tool to verify that your instance of VMware Email Notification Server (ENS) is properly configured.

1. Run the Workspace ONE Validation Tool. Select the **Email Notification Server** option.
2. Configure the system integration settings to test.
 - Select the System Integration you want to configure and enter the required integration information.



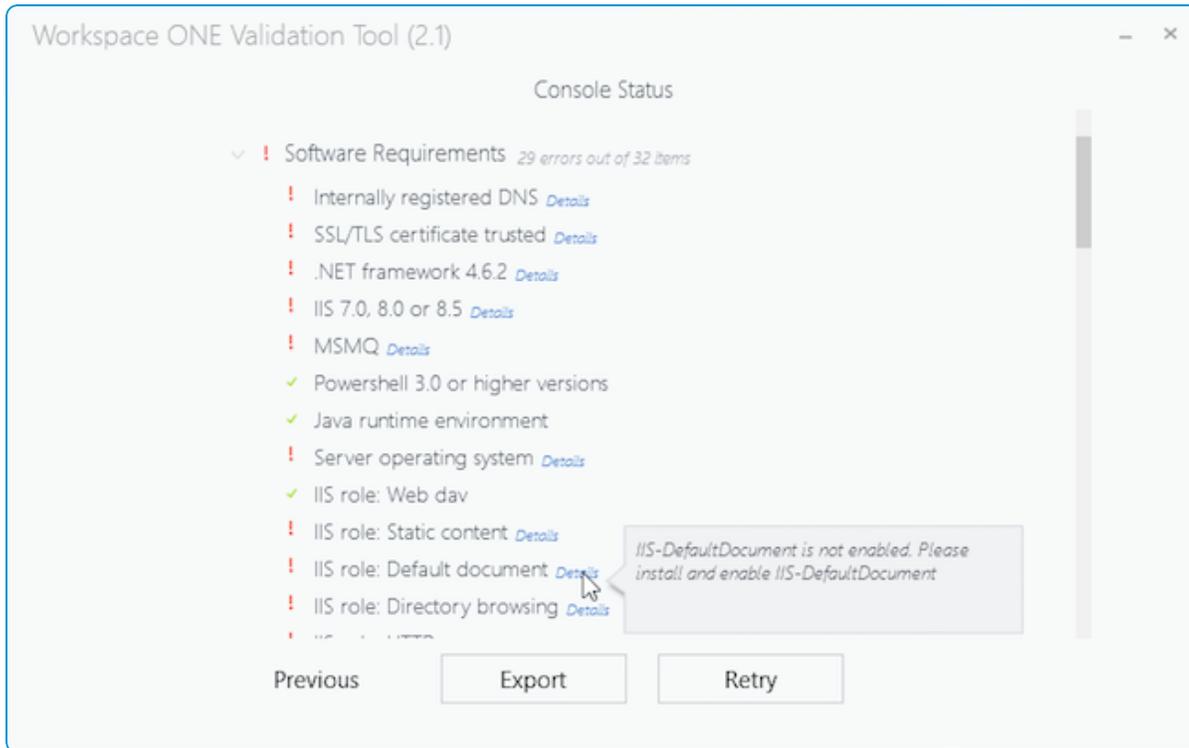
3. When you have entered all the required information, select **Test** to verify your Secure Email Gateway configuration.
4. When the test results appear, you can **Export** the results or **Retry** the validation. For more information about using the results, see [Validation Tool Results on page 41](#).

If the validation returns errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Validation Tool Results

Use the results from the VMware Workspace ONE Validation Tool to make necessary changes to your configuration to make sure that you are ready for a successful SaaS or on-premises deployment.

If the validation tool finds errors, your results include error details for your configuration. Additional information appears when you hover over an error in this view.



To view additional details for each error, select **Export** to download a Component Test Report. Use this report to troubleshoot your configuration.

Workspace ONE™		Validation Tool (2.1)	
Test component - Secure Email Gateway Classic			
Server Information			
Server Name :	AW		
OS Version :	Microsoft Windows Server 2012 R2 Standard		
OS Bit Version :	64-bit		
RAM Available:	2663MB		
Total RAM:	8192MB		
Number of Processors:	2		
Number of Cores:	2		
Disk Space Available:			
C:\	66GB		
D:\	0MB		
E:\	94GB		
Software Requirements			
Verification	Requirement	Status	Notes
1	Server operating system	TRUE	Success
2	Externally registered DNS	FALSE	Not registered to external DNS
3	Internally registered DNS	TRUE	Internally registered DNS
4	SSL/TLS certificate trusted	FALSE	This server's certificate is not trusted
5	IIS 7.0, 8.0 or 8.5	TRUE	Success
6	MSMQ	TRUE	Success
7	Telnet client	TRUE	Success
8	.NET framework 4.6.2	TRUE	Success
9	IIS 443 certificate binding	TRUE	IIS 443 is binded withhttps://aw.airwatch.com/AirWatchcertificate
10	IIS role: Web dav	TRUE	Success
11	IIS role: Static content	TRUE	Success
12	IIS role: Default document	TRUE	Success
13	IIS role: Directory browsing	TRUE	Success
14	IIS role: HTTP errors	TRUE	Success
15	IIS role: HTTP redirection	TRUE	Success
16	IIS role: ASP.NET	TRUE	Success
17	IIS role: .NET extensibility	TRUE	Success
18	IIS role: ASP	TRUE	Success
19	IIS role: ISAPI extensions	TRUE	Success
20	IIS role: ISAPI filter	TRUE	Success
21	IIS role: Server side includes	TRUE	Success
22	IIS role: IIS management console	TRUE	Success
23	IIS role: IIS 6 management compatibility	TRUE	Success
Network Requirements			
Verification	Requirement	Status	Notes
1	Exchange server	TRUE	Success
2	REST API	FALSE	Not able to connect.
3	AWCM endpoint	FALSE	Connection failed
4	m.google.com (Note: This is only required for Google Apps integration.)	TRUE	Successful ping

For more information on how to resolve errors, consult the **Pre-Installation Requirements Worksheet**, available at **AirWatch Resources**.

Chapter 3:

Database Installation

Run the AirWatch Database Setup Utility	45
Verify Proper Database Installation	46

Run the AirWatch Database Setup Utility

Run the AirWatch database executable once all prerequisites are met, such as creating the database and the AirWatch SQL account and assigning DB owner roles used for installation.

For the following procedure, if you are planning to use Windows authentication, then you must be logged in as the account you want to use or you must shift+right-click when you run the AirWatch database executable and select **Run as different user**. The installer can be run directly on the database server, or on an application server if you have security concerns.

Important: If there is an open connection to the AirWatch database, the population of the tables during the Database setup fails.

1. On either the AirWatch Console or Database Server, open the **9.2 DB** folder, right-click the AirWatch Database executable, and **Run as an administrator**.
2. The DB Installer automatically prompts you to install any essential missing components. When complete, select **Next**.
3. Accept the AirWatch **EULA**, and then select **Next**.
4. Select a location to install the AirWatch Database files, and then select **Next**. The best practice is to install wherever the AirWatch folder exists on your system. For example, C:\AirWatch.
The Database Server screen displays.
5. Click the **Browse** button next to the **Database** server text box and select your AirWatch database from the list of options.

If a custom port was used, do not select **Browse...** Instead, use the following syntax:
DBHostName,<customPortNumber> and then select **Browse...** to select the database server.

Select the **Server authentication use the Login ID and password below** radio button and enter the SQL Admin credentials. Click the **Browse** button next to the database catalog text box and select the **AirWatch database catalog**. Or, if you choose **Windows Authentication**, enter your Windows account. The Windows account must have access to the database server.

Note: The Windows account mentioned is only used for creating the database.

The AirWatch database installation user (the account used to install the database only) has DB owner privileges on the AirWatch Database and SQLAgentUserRole and db_datareader on the msdb database.

6. Click **Next**. A warning pop-up displays to ensure the account accessing the database has sufficient rights. Click **OK** and **Install**.
7. Click **Finish** once the database upgrade process completes.
8. On the **SQL Server**, open **SQL Server Management Studio**, expand the **AirWatch database** and verify AirWatch tables have been populated.

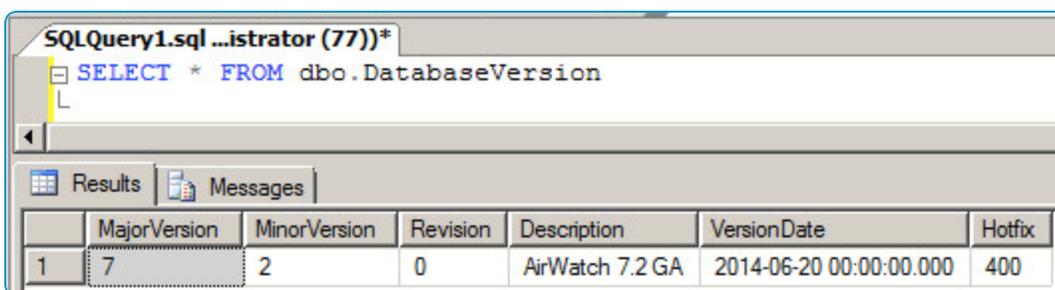
Verify Proper Database Installation

After running the database setup utility and completing installation, check to make sure that the installation was successful.

To verify a successful installation:

1. From SQL Server Management Studio, select your AirWatch instance and enter:


```
SELECT * FROM dbo.DatabaseVersion
```
2. Click **Execute**.
3. Verify the correct version displays in the Results window. (If performing an 9.2 GA release, you see MajorVersion 9, MinorVersion 2, and Description AirWatch 9.1 GA. Version 7.2 is shown as an example.)



	MajorVersion	MinorVersion	Revision	Description	VersionDate	Hotfix
1	7	2	0	AirWatch 7.2 GA	2014-06-20 00:00:00.000	400

Chapter 4:

Application Server Installation

Run the AirWatch Installer on Each Application Server (Console and Device Services)	48
(Optional) Run the Installer on Additional Device Services Servers	61
Run the AirWatch Installer on the VMware Identity Manager Service	62

Run the AirWatch Installer on Each Application Server (Console and Device Services)

Run the AirWatch executable file on your application servers to install the AirWatch Console and Device Services features.

For the following procedure, if you are planning to use Windows authentication, then you must be logged in as the account you want to use or you must shift+right-click when you run the installer EXE file and select **Run as different user**.

1. On the application server (which is either your Console or DS), open the **9.2 Application** folder and run the **AirWatch Application 9.2.X Full Install.exe**.

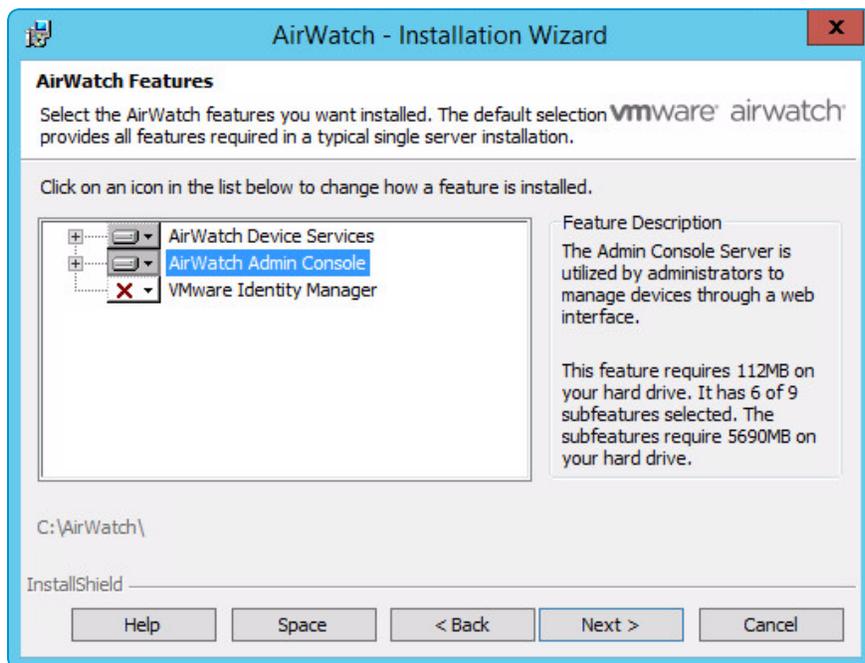
Execute the AirWatch installer from an account with administrator privileges. If you do not have administrative privileges, right-click and choose **Run as Administrator** to run the installer.

The installer stops all the services on the App server automatically.

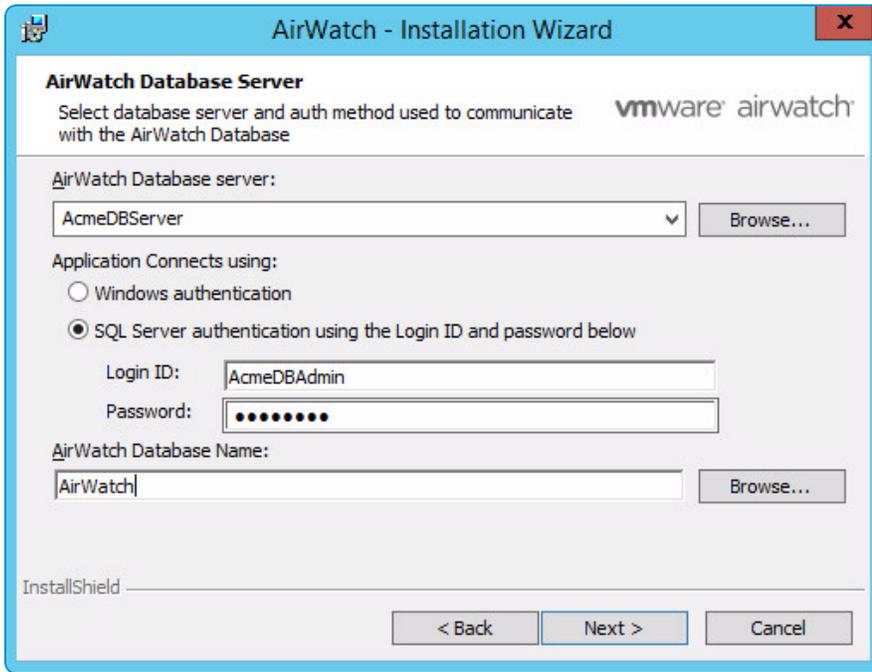
2. The installer installs pending server prerequisites, if any.

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. Click **Next** once the AirWatch installer begins. The **End User License Agreement (EULA)** appears.
4. Accept the EULA and select **Next**.
5. Next, specify if you are importing or exporting any AirWatch Setup Configurations from or to any other identically configured AirWatch servers.
 - Disregard this setting if you are deploying AirWatch without any load balanced High Availability (HA) or Disaster Recovery (DR) servers.
 - If you have multiple load-balanced Device Services servers, then you can export settings from the first Device Services server to use on any of the additional Device Services servers and increase install speed or import settings that you have previously exported. For more information, see [\(Optional\) Run the Installer on Additional Device Services Servers on page 61](#).
6. Select the AirWatch features that you want to install on the specific server.
 - In a standard, multi-server environment, enable only the AirWatch Console features or the AirWatch Device Services features for the respective server type.



- If you are installing the VMware Identity Manager Identity Service, you can do so on a standalone server. For more information on the installer screens that display when you enable this feature, see [Run the AirWatch Installer on the VMware Identity Manager Service on page 62](#).
 - If you want to enable Remote Management v3.0 capabilities to provide remote management capabilities to your supported devices, then refer to the **VMware AirWatch Remote Management v3.0 Guide**, [available on AirWatch Resources](#), which provides steps to enable this functionality through a standalone installer.
7. The AirWatch Prerequisites screen displays to ensure that you meet the requirements. At this point, the installer checks for modules that are required for a successful deployment of AirWatch. You are prompted to install any missing components. Select **Next**.
 8. Choose the directory to install AirWatch, and then select **Next**.
 - If you are installing AirWatch on multiple application servers, the directory path must be identical for each server on which the application files are installed.
 9. Enter information about the AirWatch Database.



- Select **Browse** next to the **Database server** text box and select your AirWatch database from the list of options. If you are using a custom port, do not select Browse. Instead, use the following syntax: **DBHostName,<customPortNumber>**, and then select **Browse** to select the Database server.
 - i.e. db.acme.com,8043
 - Select one of the following authentication methods:
 - Choose **Windows Authentication** mode to connect to the database, and then select **Next**. You are prompted to enter the service account that you want to use. This service account is used to run all the application pools and AirWatch related services. This account must be an account that has AirWatch Database access.
 - Choose **SQL Server Authentication** mode to connect to the database. You are prompted to enter the user name and password.
 - Enter the name of the AirWatch database or browse the SQL server to select it from a list.
10. Enter the Internal DNS URL or FQDN of the Console Server in the **Admin Console DNS/IP Address** text box for the **Web Console**. Enter the External DNS for the **Device Services External DNS name** text box for the **Device Services** server.

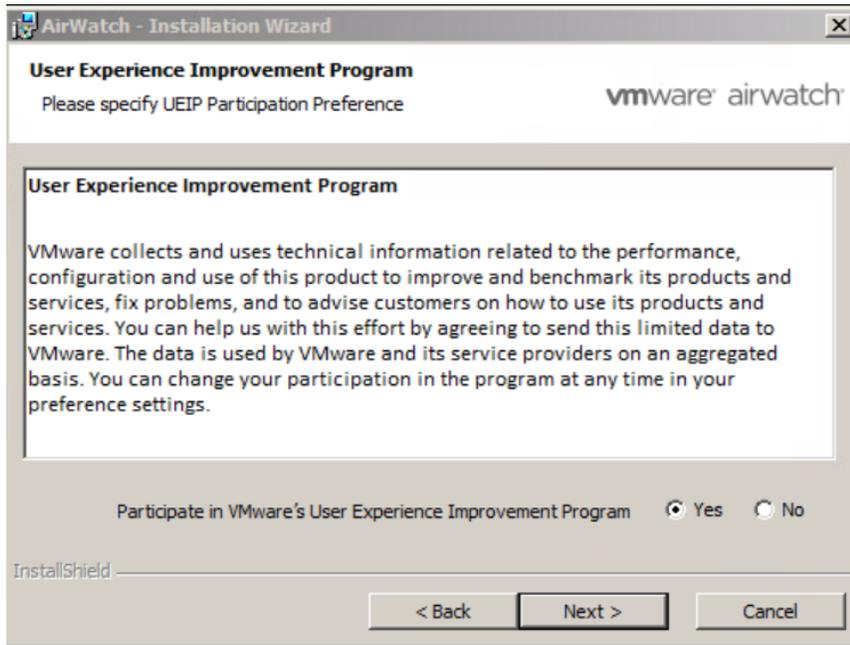
Ensure that you are entering the full internal DNS URL or FQDN of the Console Server in the Admin Console DNS/IP Address text box. Do **not** enter the shortname for the server. For example, if the Console server is awconsole.company.local, do **not** simply enter awconsole for your URL.

Ensure that the DNS names are correct and there are no spaces after the end of each. If an error is made, the whole installation must be removed and reinstalled.

Select whether to enable support for the SOAP API endpoints to be SSL Offloaded by selecting **API Server SSL Offloaded?**

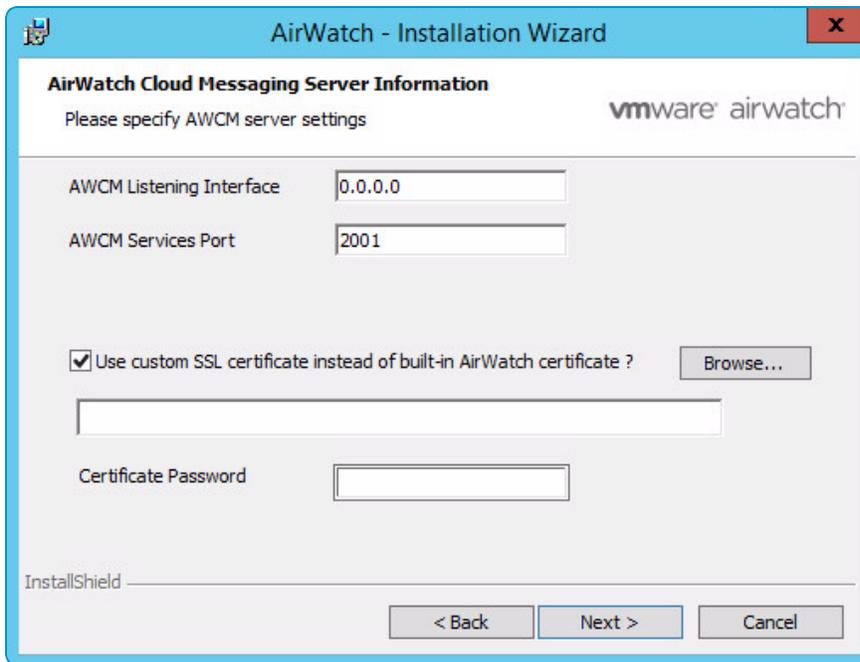
11. If the Global Enterprise Manager screen displays, then verify your Company name.
 - Enter your **Company Name**, which is your organization's Salesforce name provided by AirWatch.
 - Select your **Environment Type** from the drop-down menu.
 - Enter your **Installation Token** from myAirWatch.
 - See [Generate Installation Token from myAirWatch \(Automatic Method\)](#) on page 54 if your application server has outbound Internet access to the AirWatch signing service, as defined under the Network Requirements in the VMware AirWatch Recommended Architecture Guide.
 - See [Generate Installation Token from myAirWatch \(Manual Method\)](#) on page 56 if your application server does not have Internet access to reach the AirWatch signing service.
12. Choose whether you want to participate in the VMware User Experience Improvement Program.

This program collects and uses technical information related to the performance, configuration and use of AirWatch to improve and benchmark its products and services, fix problems, and to advise customers on how to use its products and services.



13. Choose the AirWatch used Web site. By default, the 'Default Web Site' is selected.
14. If you choose to install the **AirWatch Cloud Messaging** component (selected by default for the Device Services server), you receive a prompt to enter the AWCM settings:
 - Enter **0.0.0.0** for the value of the listening address, which is a wildcard value that tells AWCM to listen on all available interfaces on the server.
The value for listening address might be a specific IP address matching an interface on the server if this is needed per your network deployment.
Use 2001 as the **AWCM Services Port**. Consult your AirWatch account services representative before using another port.
 - To automatically use an AirWatch certificate without any additional configuration, ensure **Use custom SSL Certificate instead of built-in AirWatch certificate?** is disabled. Otherwise, select the **Use custom SSL Certificate instead of built-in AirWatch Certificate** check box and locate the PFX file of your SSL certificate.
If you are using your own certificate, ensure that you extract the full chain as part of the PFX file before uploading it.
 - If using SSL offloading through your load balancer, enable **AWCM Server SSL Offloaded?** and enter in the load balancer hostname. If you are not SSL Offloading AWCM, then you must upload your Device Services certificate

for AWCM.



15. When deploying AWCM node(s), select a clustering mode.
 - **Implicit Clustering** – The default, recommended method. Requires load balancer-based persistence.
 - **Explicit Clustering** – An alternative method for deploying multiple AWCM Nodes that does not use load balancer-based persistence – data is shared in memory across all nodes. For more information, see the **VMware AirWatch Cloud Messaging Guide**.
16. Click **Install** when prompted.

If you install using Windows Server 2016, a dialog box prompts you to disable HTTP2 support. Disable and continue.
17. Click **Finish** once all the files are copied to the server to complete the AirWatch installation.

The installation log file can be viewed by selecting a check box before Finish is selected.

Internet Explorer auto-launches and may fail, since IIS has not yet fully refreshed the Web sites.
18. Close Internet Explorer and run Chrome.

For the Console: Type **https://localhost/airwatch** to verify that the AirWatch Console renders successfully.

For Device Services: Type **https://localhost/devicemanagement/enrollment** to verify that the device Group ID prompt is shown.

Since the SSL certificate is not bound to the localhost session, an error displays. Select **Proceed** to view the site. The first time the Web site displays, it may take up to minute to resolve.
19. If necessary, reset IIS using the Command Prompt to bring the site online: **iisreset**

As part of the standard, multi-server installation, you must now go through the procedure again, this time for the other app servers. If you have extra device services servers, then you must run the installer on each additional Device Services server.

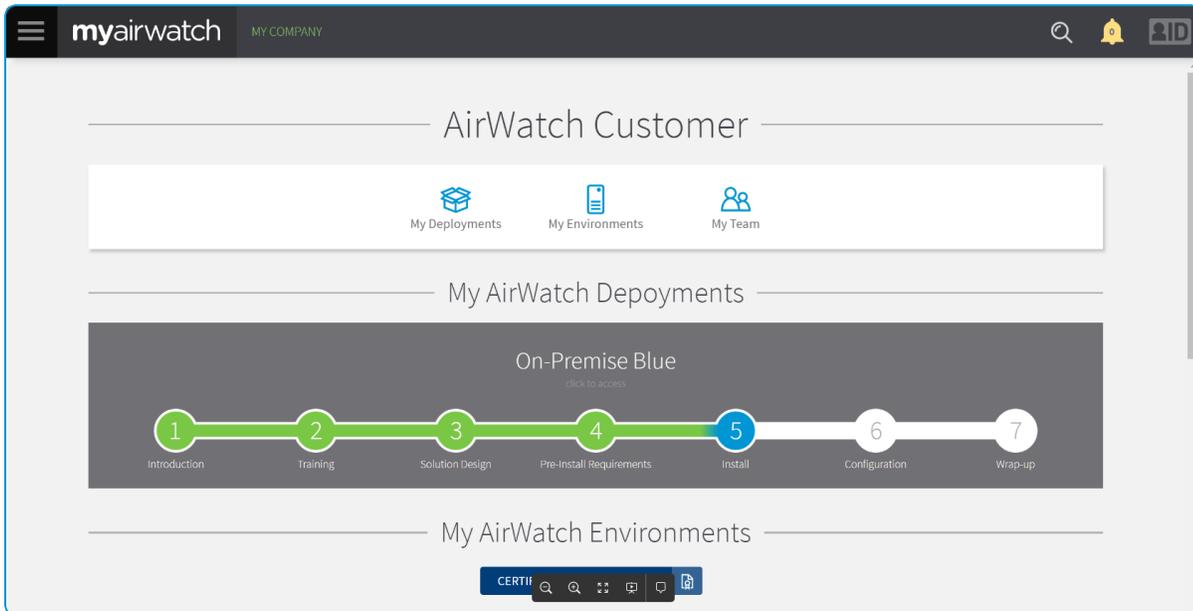
Generate Installation Token from myAirWatch (Automatic Method)

Toward the end of your AirWatch installation, you may see a screen asking for your Installation Token generated from myAirWatch. This token is used to provision the necessary secure channel certificate to your AirWatch database if it is not already present, such as in the case of a new installation.

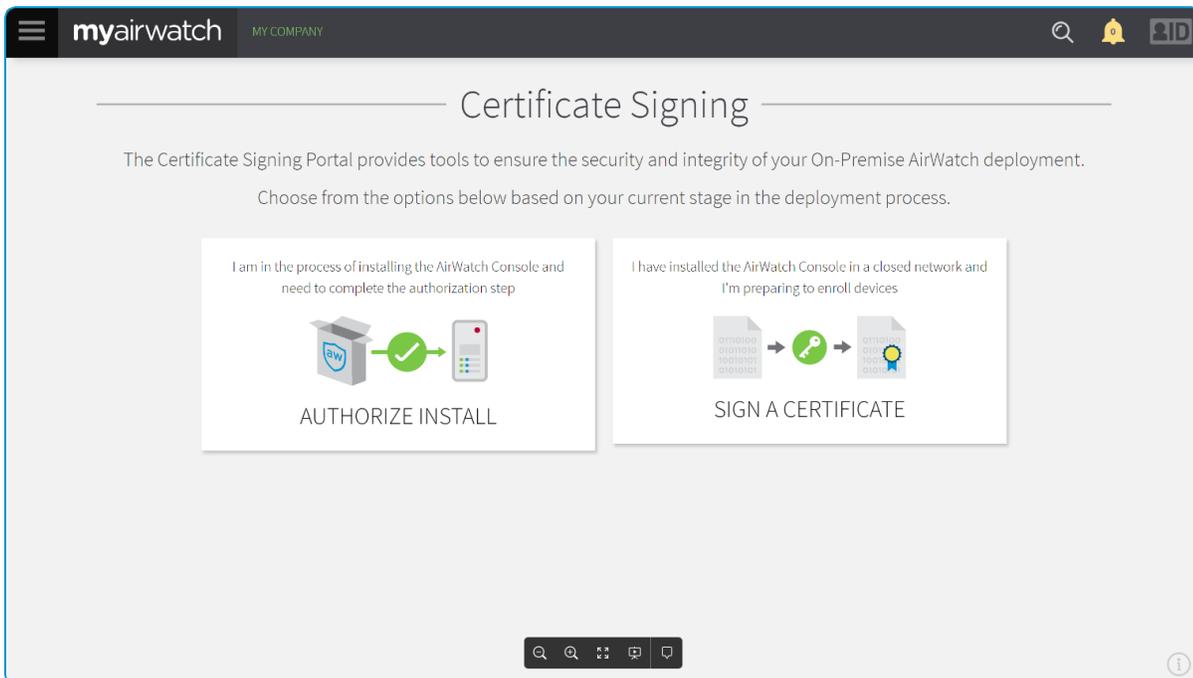
To retrieve the token automatically, your AirWatch application server must have outbound Internet access to the AirWatch signing service, as defined under Network Requirements in the VMware AirWatch Recommended Architecture Guide.

1. After AirWatch installation, on the Global Enterprise Manager screen, enter your **Company Name** and **Environment Type**.
2. Select the myAirWatch link, which should open the myAirWatch website. If the token field is not displayed, then no certificates are needed or the signing service could not be reached. If the service cannot be reached, see [Generate Installation Token from myAirWatch \(Manual Method\)](#) on page 56.

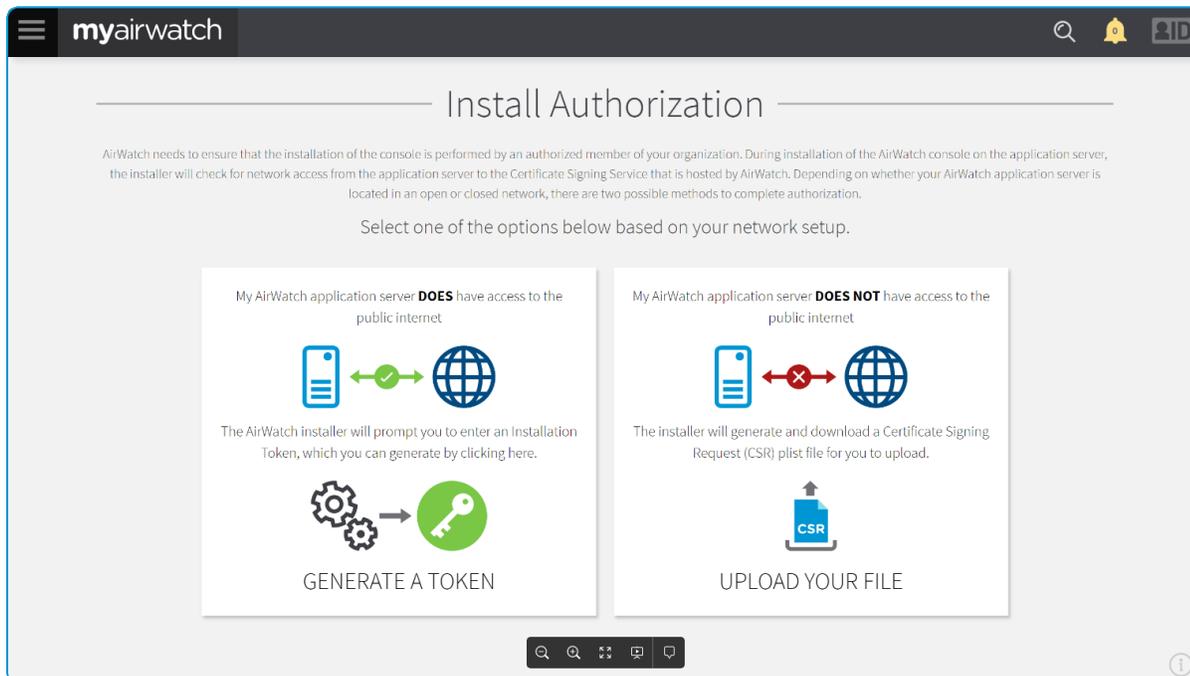
3. Log in to myAirWatch and navigate to myAirWatch > My Company.
4. Select **Certificate Signing Portal**.



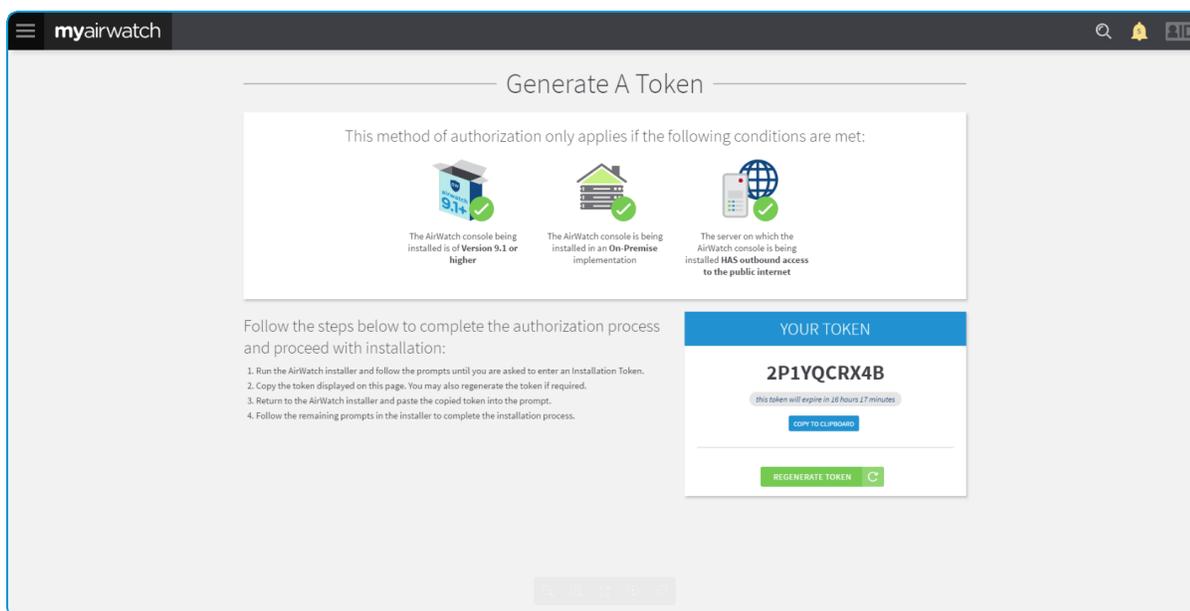
5. Select **Authorize Install**.



6. Select **Generate a Token**.



7. Enter your token in the **Installation Token** field on the [Global Enterprise Manager screen](#) to complete the installation.



Generate Installation Token from myAirWatch (Manual Method)

Toward the end of your AirWatch installation, you may see a Global Enterprise Manager screen asking for your Installation Token generated from myAirWatch. This token is used to provision the necessary secure channel certificate to your AirWatch database if it is not already present, such as in the case of a new installation.

If your AirWatch application server does not have outbound Internet access to the AirWatch signing service, as defined under Network Requirements, then the Authentication Token field does not display on the Global Enterprise Manager screen. In this case, the manual flow installer is automatically launched. In case the installer is not automatically

launched, you can manually run it by navigating to **AirWatch/Supplemental Software/CertInstaller/** and running **CertificateInstaller.exe**. This opens a screen to guide you through the manual installation method.

1. Hit **Next** to continue and start the wizard.
2. Select whether to use SQL Authentication or Windows Authentication. Select the same option that you chose during the main installation procedure. For SQL Authentication, the appropriate credentials are seeded in your config file. For Windows Authentication, you must enter the credentials of the Windows user to authenticate.

AirWatch Certificate Installer

Database Authentication Mode

Choose the mode of Authentication to the AirWatch Database. The settings here should be the same as defined in the AirWatch installer earlier in the installation. Choosing 'SQL Authentication' will use the values entered earlier in the install. Choosing 'Windows Authentication' will require entering the windows user with which to authenticate with again.

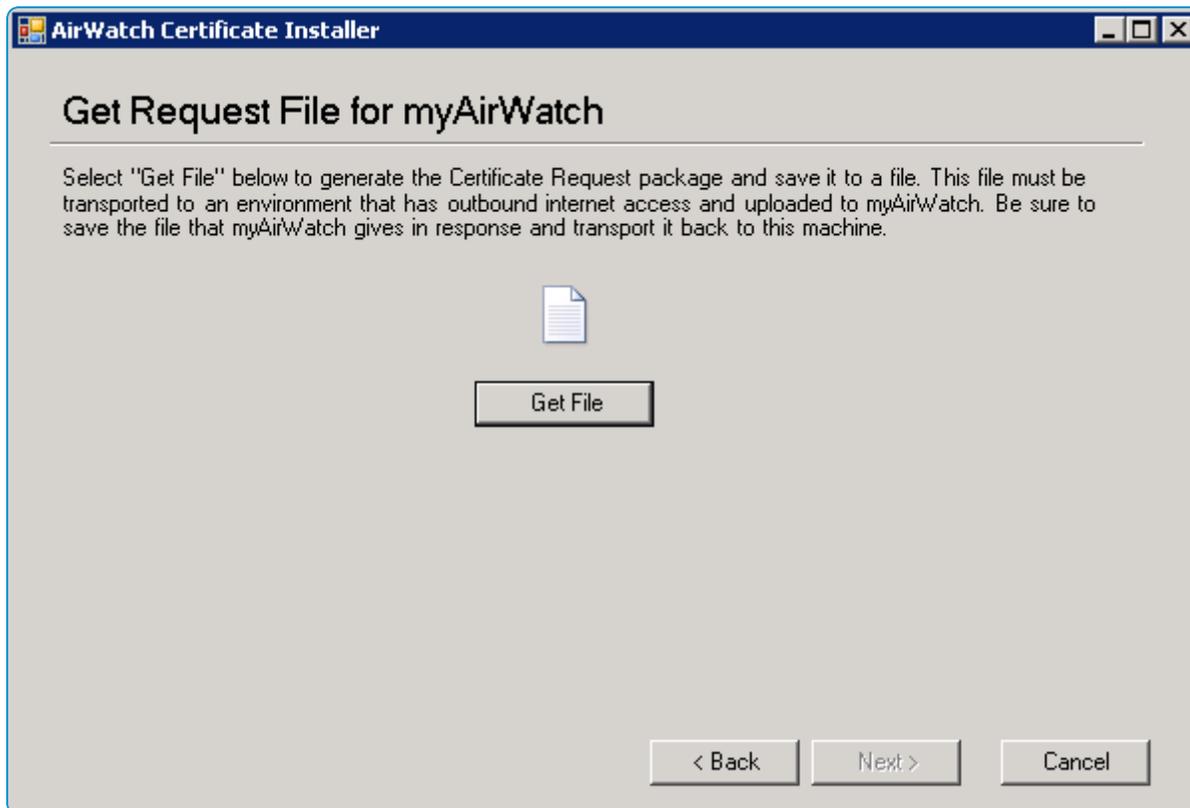
SQL Authentication
 Windows Authentication

Domain:

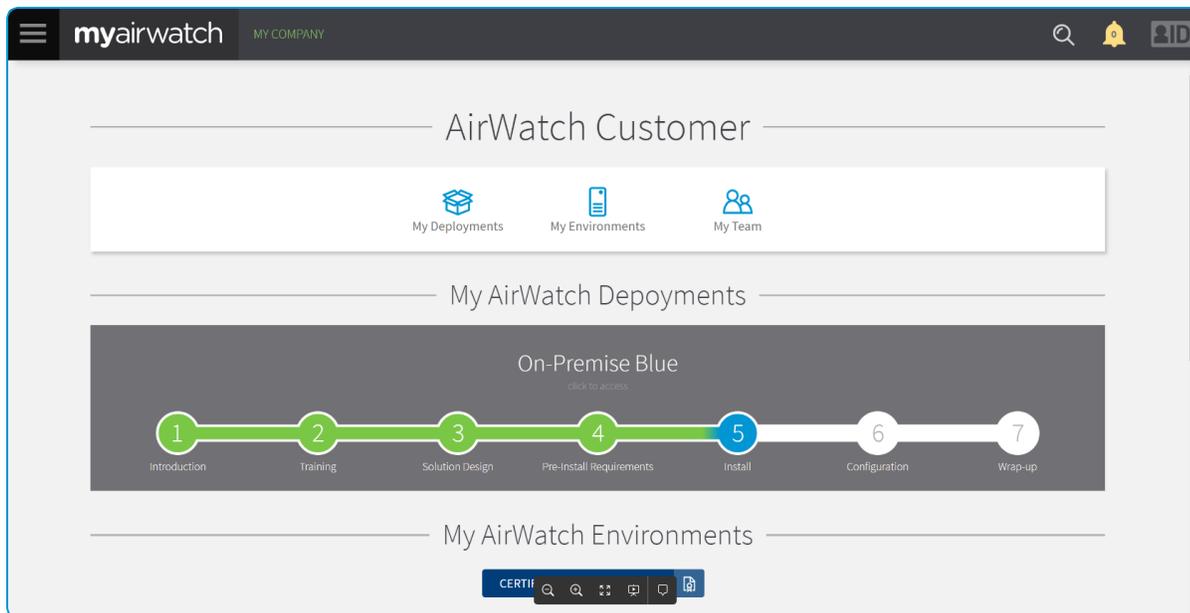
Username:

Password:

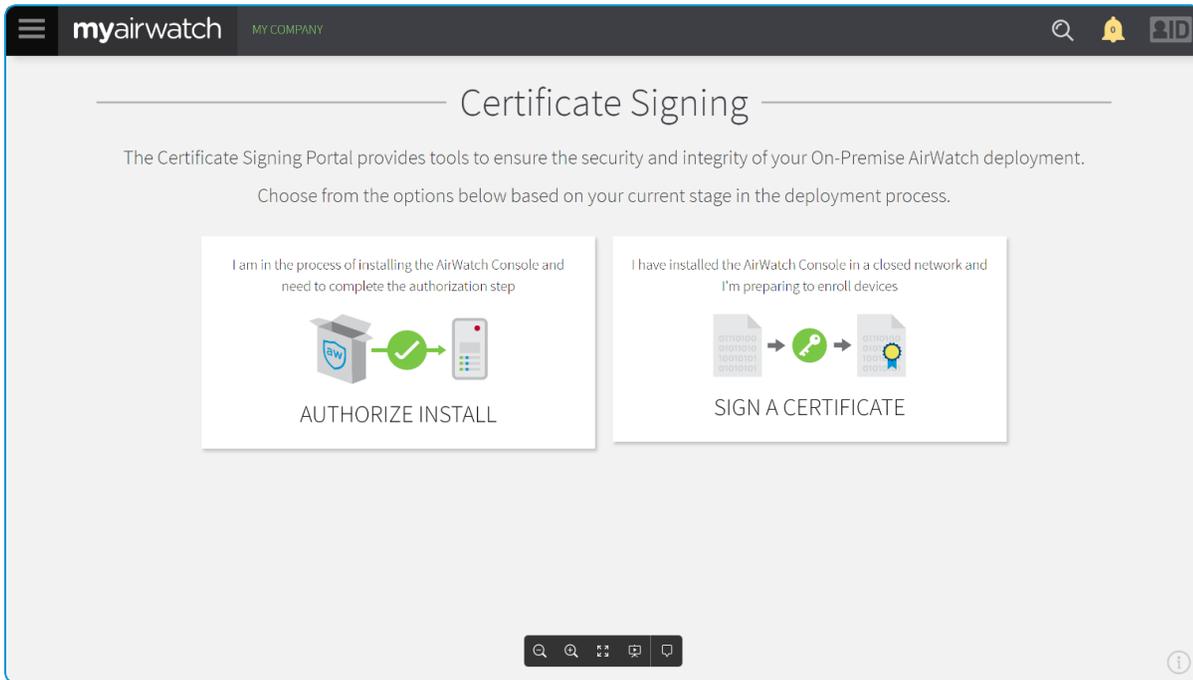
3. Select the **Get File** button to generate a .plist file that contains a batch of certificate signing requests. Save this file to a location that has outbound Internet access to the myAirWatch signing service.



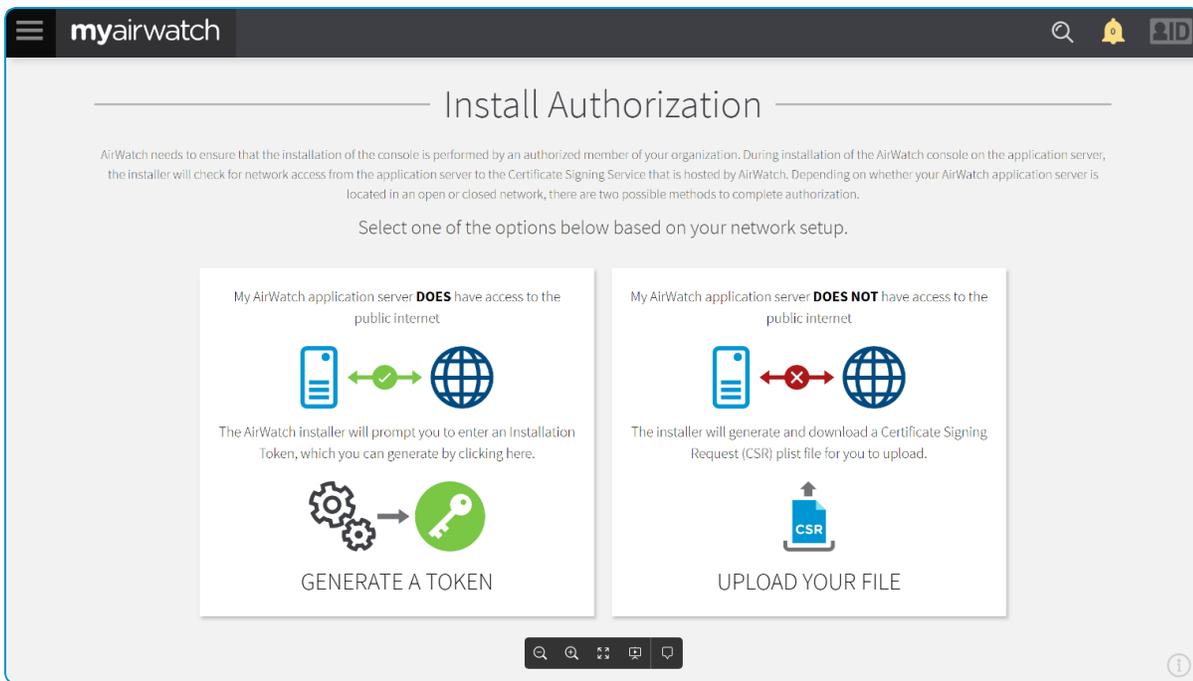
4. Log in to myAirWatch and navigate to myAirWatch > My Company.
5. Select **Certificate Signing Portal**.



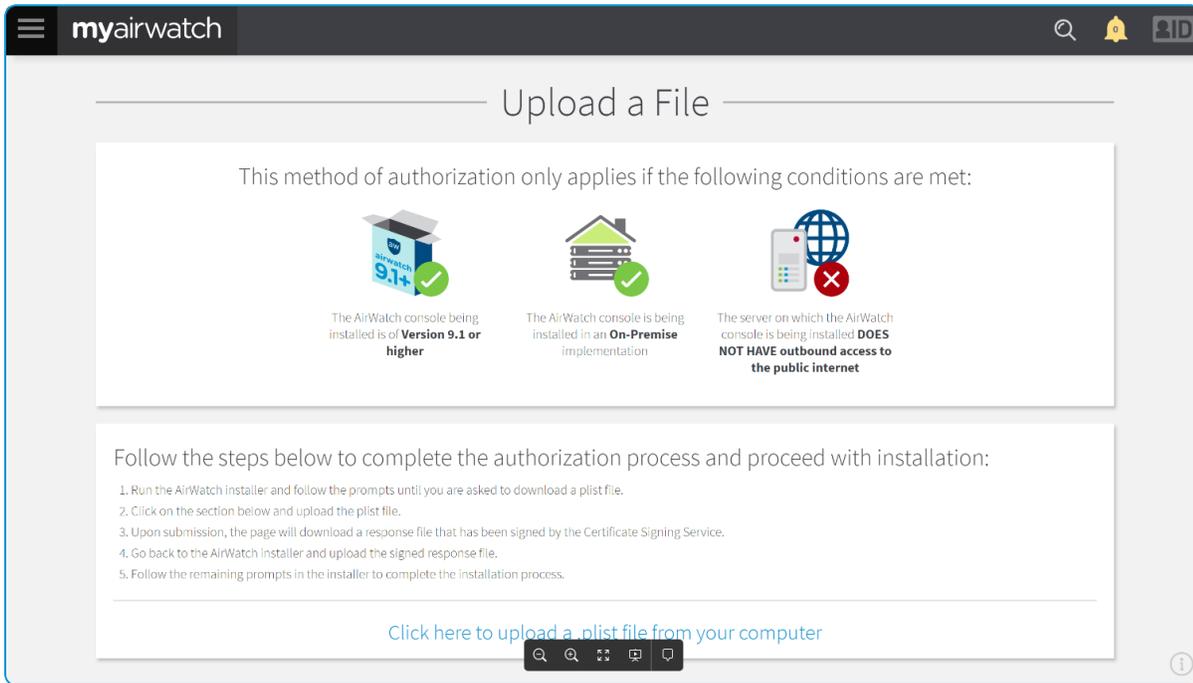
6. Select **Authorize Install**.



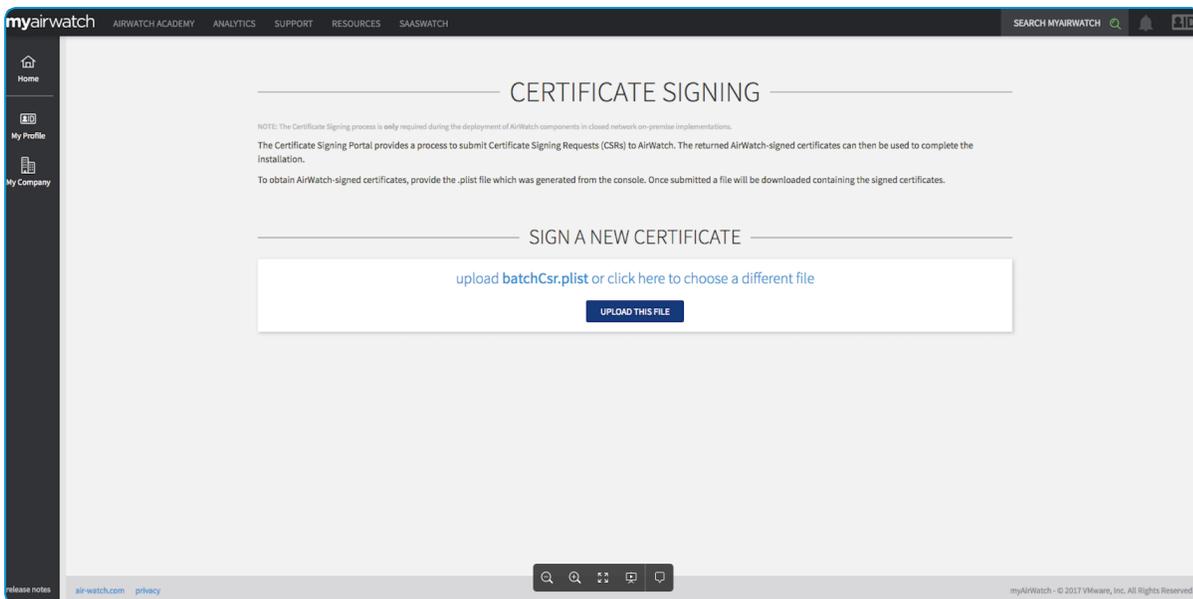
7. Select Upload Your File.



8. Select the link to upload a .plist file from your computer and select the .plist file you saved previously.



9. Select **Upload This File** and save the file provided.



10. In the installer, select **Set File** and select the file myAirWatch provided. If successful, the **Next** button is enabled and you may proceed with installation.

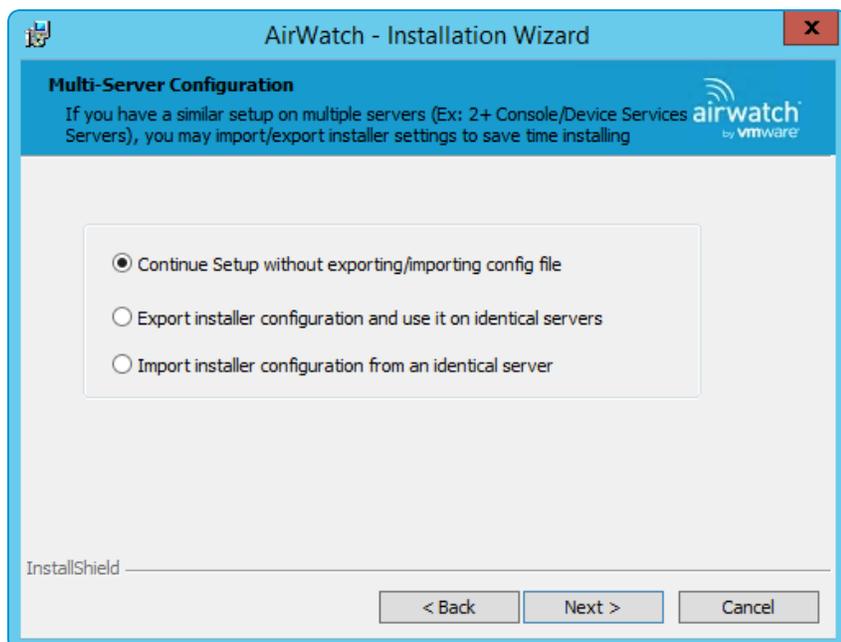
Installation Failed

If you see the installation failed screen at any point during installation, then something went wrong. You can select Back to try again or contact AirWatch Support for assistance.

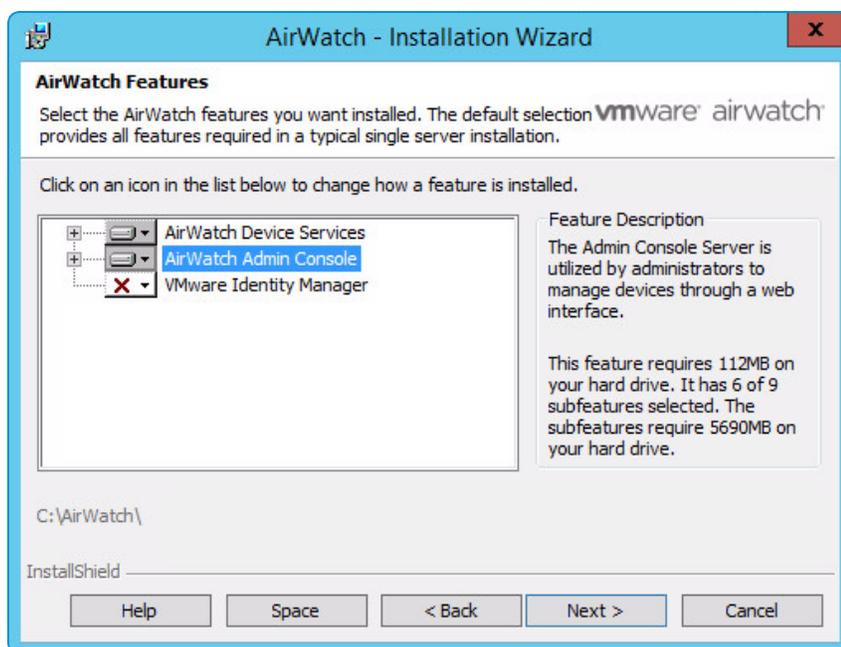
(Optional) Run the Installer on Additional Device Services Servers

Running the installer extra times is only required if you have more Device Services servers, because you must run the installer on each additional server.

1. Log on to one of your Device Services servers and start the **AirWatch Installer**.
2. Click through the screens until you reach the **Export/Import Setup Configuration** form. This time, select **Export configuration and use it on multiple servers** if you have multiple load-balanced Device Services servers. If you only have one Device Services server, then choose **Continue Setup without exporting/importing config file** once again.



3. Next, select the AirWatch features that you want to install on the specific server. This time, select only **AirWatch Device Services**.





If you are installing multiple AWCMs (which are typically on the Device Services servers), then you should refer to the following Knowledge Base article: <https://support.air-watch.com/articles/115001666028>.

4. Enter the file path to the AirWatch Directory once again, and choose **Next**.
5. Enter the information about the AirWatch Database. Do not select the check box as there is no need to generate a database script.
6. Enter the Console and Device Services Server URLs.
7. Specify the AirWatch Web Site.
8. Click **Install**, and then select **Finish**.
9. If you have additional Device Services servers to install, run the installer on each server but import the existing configuration file that you exported on your first Device Services server. You need to only select through the Installer without entering any configuration details.

Run the AirWatch Installer on the VMware Identity Manager Service

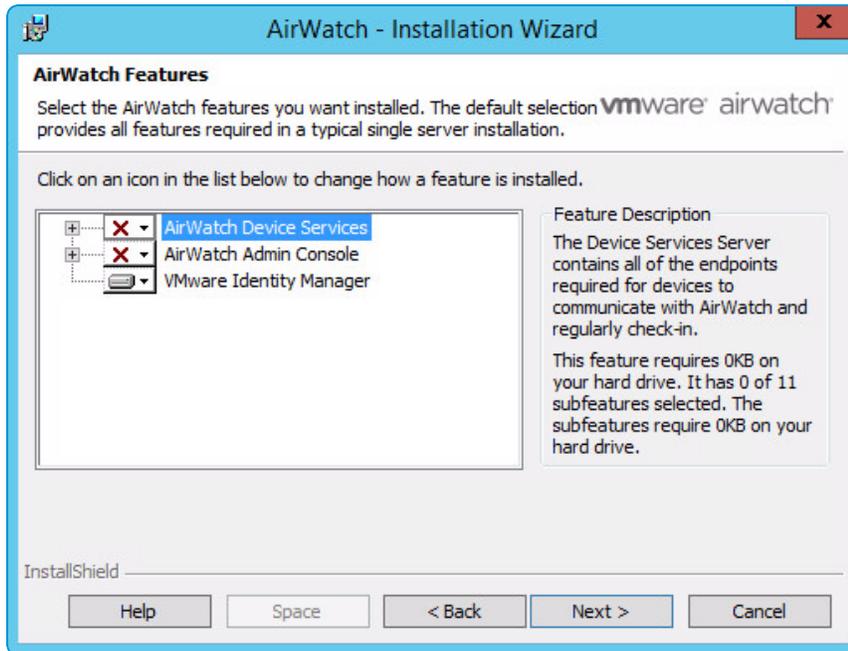
For Workspace ONE deployments, you must select and install the VMware Identity Manager Service as part of your AirWatch installation. You can deploy the service on a standalone identity manager server.

1. On the Identity Manager Service server, open the **9.2 Application** folder and run the **AirWatch Application 9.2.X Full Install.exe**.

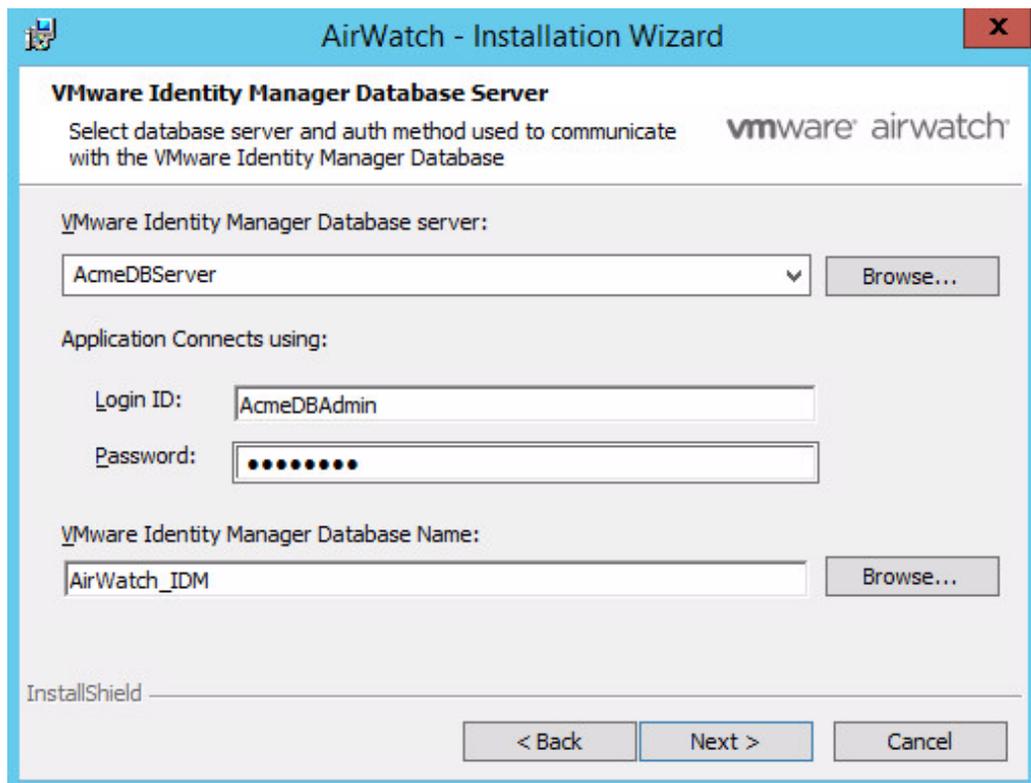
Run the AirWatch installer from an account with administrator privileges. If you do not have administrative privileges, right-click and choose **Run as Administrator** to run the installer.

The installer stops all the services on the App server automatically.

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. Click **Next** once the AirWatch installer begins. The **End User License Agreement (EULA)** appears.
4. Accept the EULA and select **Next**.
5. You can ignore the Multi-Server Configuration screen and select **Next**. This screen is used to configure additional Device Services servers. To set up high availability for Identity Manager, you must configure clustering settings, which are detailed in a future step.
6. Select only the VMware Identity Manager feature.



7. The AirWatch Prerequisites screen displays to ensure that you meet the requirements. At this point, the installer checks for modules that are required for a successful deployment of the Identity Manager service. You are prompted to install any missing components. Select **Next**.
8. Choose the directory in which to install the VMware Identity Manager service, and then select **Next**.
The directory path to which you install the VMware Identity Manager service cannot contain a space, or installation will fail. For example, an installation to **C:\Program Files** fails, while an installation to **C:\AirWatch** (the default installation location) succeeds.
9. Enter information about the AirWatch_IDM database.



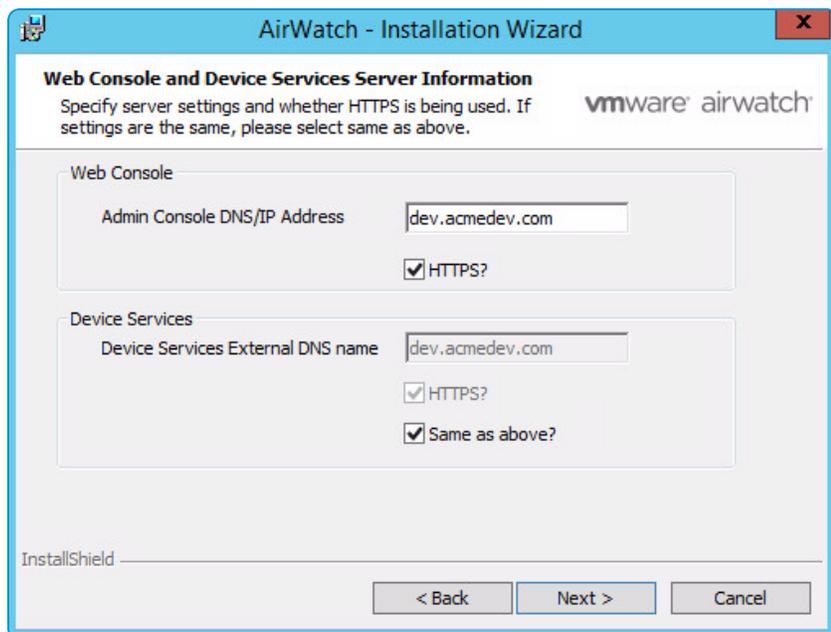
- Select **Browse** next to the **Database server** text box and select your database server from the list of options. If you are using a custom port, do not select Browse. Instead, use the following syntax: **DBHostName,<customPortNumber>**, and then select **Browse** to select the Database server.
 - For example: db.acme.com,8043

Do not select PostgreSQL as your database. This is an internal database created by the VMware Identity Manager service. This database does not scale and should only be used for Proof of Concept installs.
- Enter your SQL user credentials in the **Login ID** and **Password** text box. Windows authentication is not supported currently for the AirWatch_IDM database.
- Enter the name of the database – AirWatch_IDM – or browse the SQL server to select it from a list if you renamed it.

10. Enter the Internal DNS URL or FQDN of the Console Server in the **Admin Console DNS/IP Address** text box for the **Web Console**. Enter the External DNS for the **Device Services External DNS name** text box for the **Device Services** server.

Ensure that you are entering the full internal DNS URL or FQDN of the Console Server in the Admin Console DNS/IP Address text box. Do **not** enter the shortname for the server. For example, if the Console server is awconsole.company.local, do **not** simply enter **awconsole** for your URL.

Ensure that the DNS names are correct and there are no spaces after the end of each. If an error is made, the whole installation must be removed and reinstalled.



11. Enter information about your Identity Service.

- **External Hostname:** Enter your externally registered DNS record for your external hostname. You must enter the FQDN, and not the short hostname or IP address.
- **Internal Server Hostname:** Enter your internally registered DNS record for your internal hostname. You must enter the FQDN, and not the short hostname or IP address.
- **(Optional) Use your own SSL certificate:** Browse and upload your own SSL certificate and enter the certificate password.
- **(Optional) HTTPS proxy:** Enter information about your HTTPS proxy.

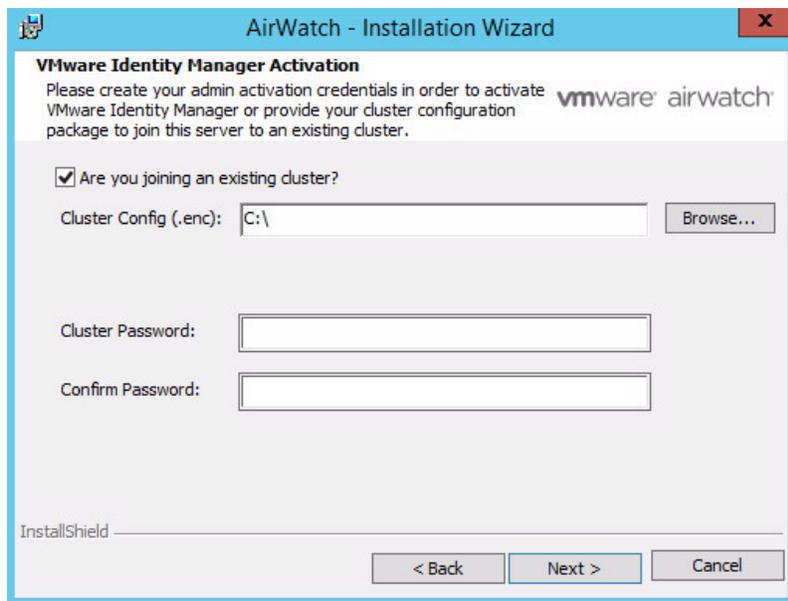
Select **Next**.

12. Create your default Identity Manager admin account password.

13. (Optional): Select the join a cluster check box if you want to join to an existing cluster for high availability. You must set up an initial Identity Manager instance before using this option. Use the following procedure:

- a. On your first Identity Manager instance, run the script located at <INSTALL_DIR>\VMwareIdentityManager\usr\local\horizon\scripts\generateClusterFiles.bat and provide a filename password to encrypt the cluster bundle.
- b. Upon installing your second Identity Manager instance, select the join a cluster check box.
- c. Browse to your cluster config (ENC) file. By default the file is located at <INSTALL_DIR>\VMwareIdentityManager\usr\local\horizon\<filename>.enc.

- d. Enter the cluster password you previously created and select **Next**.



14. Select **Install** when prompted.
15. To complete the installation, select **Finish** once all the files are copied to the server.
The installation log file can be viewed by selecting a check box before Finish is selected.

Configure the VMware Identity Manager Service Manually

If the installation of VMware Identity Manager does not successfully complete the configuration, you must manually do so.

To configure the VMware Identity Manager service manually:

1. Navigate to the configuration pages available at <https://<hostname>:8443/cfg>.

The hostname must be the FQDN.

2. Log in with the VMware Identity Manager service admin account password.

When you installed the VMware Identity Manager through the AirWatch installer, you created a default identity manager admin account password. Enter that password here.

3. Navigate to the **Select Database** page and configure the following settings:

- a. Select **External Database**.
- b. In the JDBC URL, enter:

```
jdbc:sqlserver://<hostname-or-DB_VM_IP_ADDR>;DatabaseName=AirWatch_
```

- c. Enter the database user name and password.
- d. Test the connection.

4. Update the FQDN. Configure the following settings:
 - a. Log in to the VMware Identity Manager administration console.
 - b. Select the Appliance Settings tab, then select **VA Configuration**.
 - c. Select **Manager Configuration** and log in with the admin user password.
 - d. Change the host name part of the URL from the VMware Identity Manager host name to the load balancer host name.
For example, if your VMware Identity Manager host name is "myservice" and your load balancer host name is "mylb", change the URL "https://myservice.mycompany.com" to the following: https://mylb.mycompany.com.
 - e. Select **Save**.

The VMware Identity Manager service is now configured.

Chapter 5:

Reports Installation

Reports Overview	69
Connect the Database to Reports Server	69
Configure the Service Account for SSRS	70
Configure the Web Service URL	72
Set up the Reporting Database	73
Verify the Report Manager URL and Web Service URL	74
Set up the AirWatch SSRS User	75
Add the SSRS User to IIS_IUSRS	77
Run the AirWatch Reporting Installer	78
Integrate Reports with the AirWatch Console	83
Reports Storage Overview	84

Reports Overview

This chapter walks you through the process of installing AirWatch Reports to enable report configuration, report subscription, and data driven email for your AirWatch deployment.

Reports Options

There are three options for configuring reporting.

- **Option 1:** Custom Reports

Custom reports allow you to create reports on your AirWatch deployment based on your business needs. Custom reports use a cloud-based report storage to gather data and create the reports. The custom reports feature provides faster, easier access to critical business intelligence data than normal AirWatch reports. Custom reports allow you to build customized reports using starter templates or create a report from scratch. You can choose from a wide range of data fields such as Apps and Devices.

For more information on Custom Reports, see the **Custom Reports Overview** in the **Report Analytics Guide**, available at my.air-watch.com/help.

- **Option 2:** New Reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your AirWatch solution. The exports of these reports are in CSV format.

For more information on Custom Reports, see the **Reports Overview** in the **Report Analytics Guide**, available at my.air-watch.com/help.

- **Option 3:** Legacy SSRS

The AirWatch Reporting module integrates with SQL Server Reporting Services (SSRS), which is a SQL Server module deployed with the main SQL Server instance. Sometimes the SSRS module is deployed on a separate Server. In this case, install AirWatch Reporting on the Server hosting SSRS.

Beginning with AirWatch v.9.2, the SSRS installer is no longer included with the AirWatch installation package. To add Legacy SSRS reporting to your AirWatch v9.3 deployment, run the Reports installer for AirWatch v.9.1 in addition to your normal AirWatch installation.

Important: While your reports server can be installed on the same server as the database, a dedicated SSRS instance is **required** for reports installations. Installing AirWatch Reports on an existing production reporting instance may cause reporting failures.

For more information on Legacy SSRS, see [Configure the Service Account for SSRS on page 70](#).

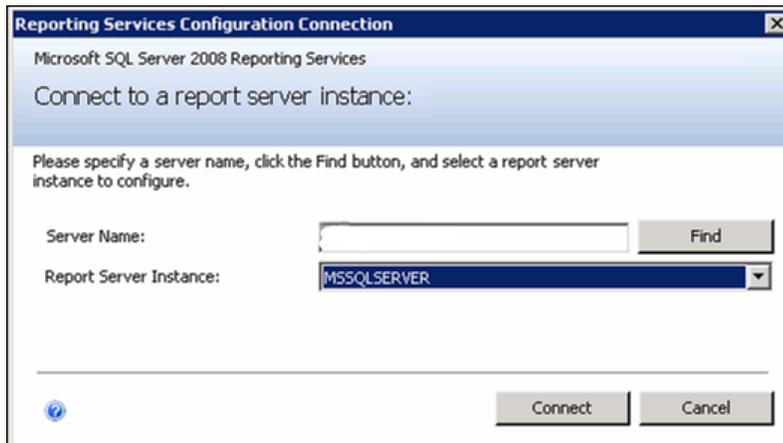
Connect the Database to Reports Server

If you are installing reports on the AirWatch database server, then you must connect the database to your reports service instance.

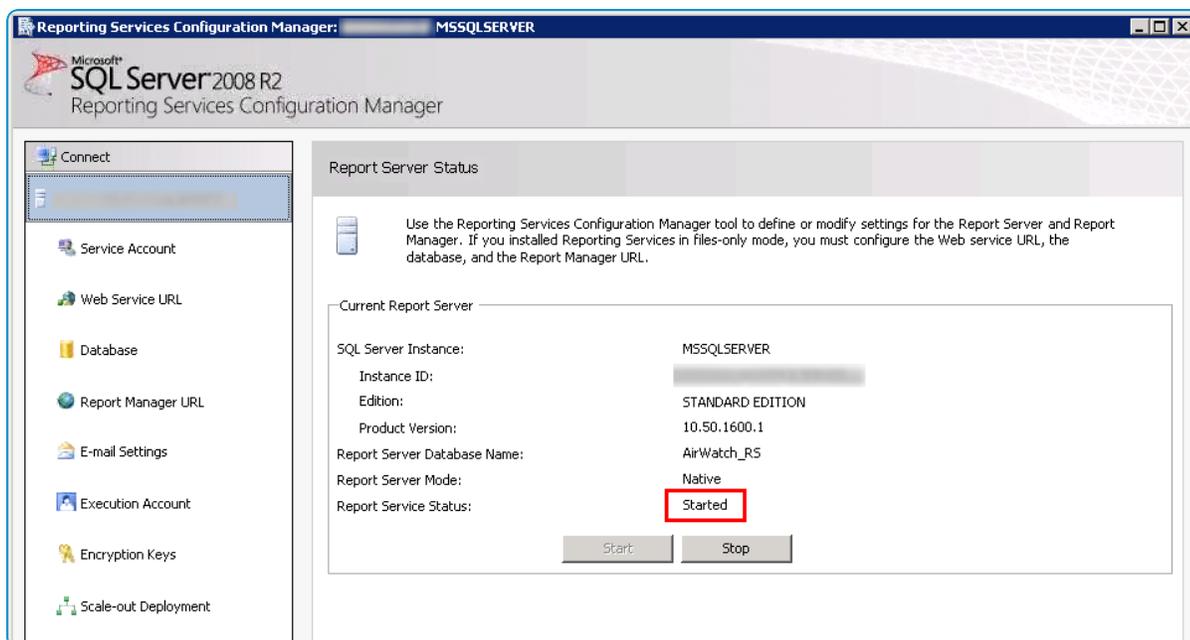
Complete the following steps to configure the SSRS instance on the SQL Server:

1. Navigate to **Reporting Services Configuration: Start > Microsoft SQL Server > Configuration Tools > Reporting Services Configuration**.

2. Provide the **Server Name** to select the name of the Server that SSRS runs on.
3. Select **Report Server Instance** from the drop-down menu to choose where to install AirWatch Reports.
4. Click **Connect**.



5. Ensure that the Report Server status is **Started**. If it is not, start the server from the **Configuration Manager Window**, or navigate to the **SQL Server Configuration Manager (Start > Microsoft SQL Server > Configuration Tools > SQL Server Configuration Manager)**, and start the service.



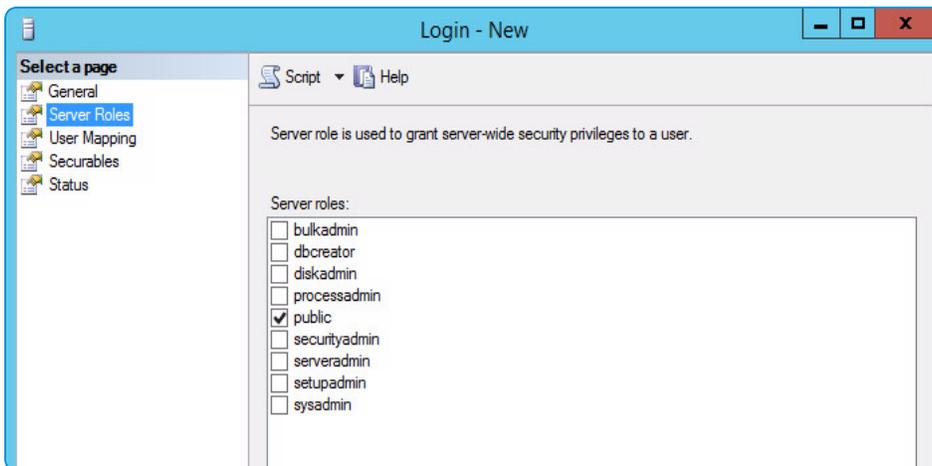
Configure the Service Account for SSRS

You must configure a Service Account where the SSRS instance runs. The default runs as a **Local System Service**. Alternatively, you can provide the account credentials to run under a service account.

Beginning with AirWatch v.9.2, the SSRS installer is no longer included with the AirWatch installation package, because improved reporting functions are included with the AirWatch v.9.2 Installation package. For more information about alternative options, see [Reports Overview on page 69](#)

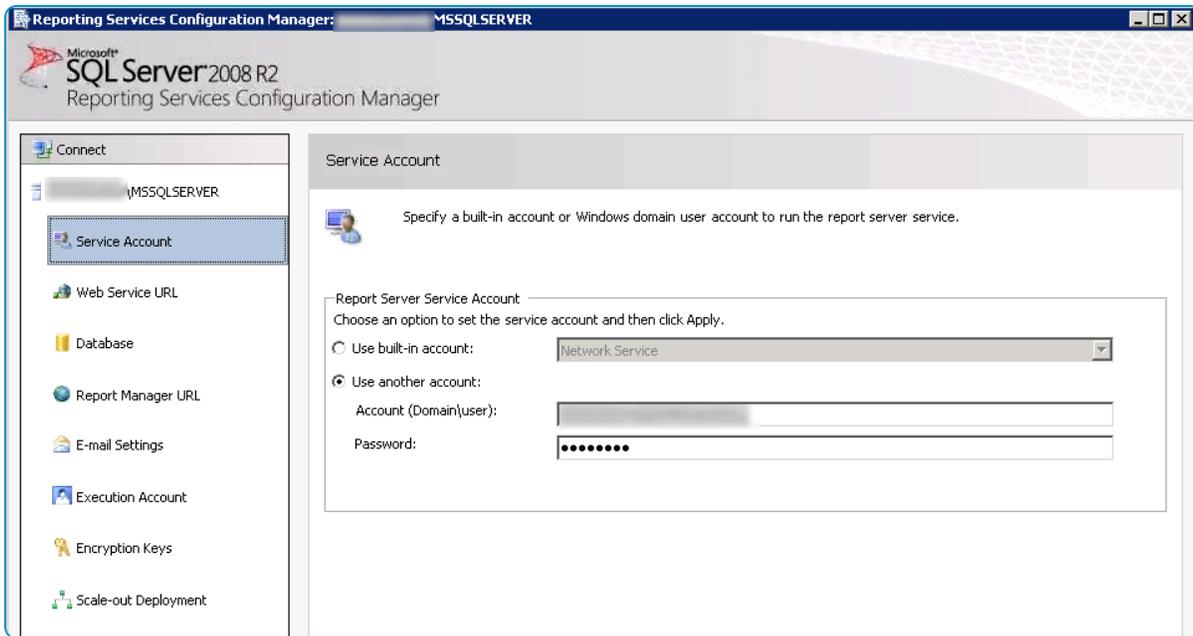
First, ensure that this account has the correct permissions to the AirWatch Database. You can add the following permissions to the service account for SSRS:

1. Log in to SQL Server Management Studio.
2. Navigate to **Security > Logins > <Your DB User>** to locate your DB User in the Object Explorer, and then right-click and choose **Properties**.
3. Navigate to the **Server Roles** tab. Select server role as **Public**.



4. Select **User Mapping**.
 - If you are running the reports installer using a **Service Account**, include the following permissions:
 - Select the AirWatch database, then select the **db_owner** and **public** roles.
 - Select the master database, then select the **public** role.
 - Select the msdb database, then select the **public** role.
 - Select the ReportsServer_Reports_DB database, then select the **db_owner**, **public**, and **RSExecRole** roles.
 - Select the RS_TempDB: Owner database, then select the **public** and **RSExecRole** roles.
 - If you are running the reports installer using **Windows Authentication**, include the following permissions:
 - Select the AirWatch database, then select the **public** role.
 - Select the master database, then select the **public** role.
 - Select the msdb database, then select the **public** role.

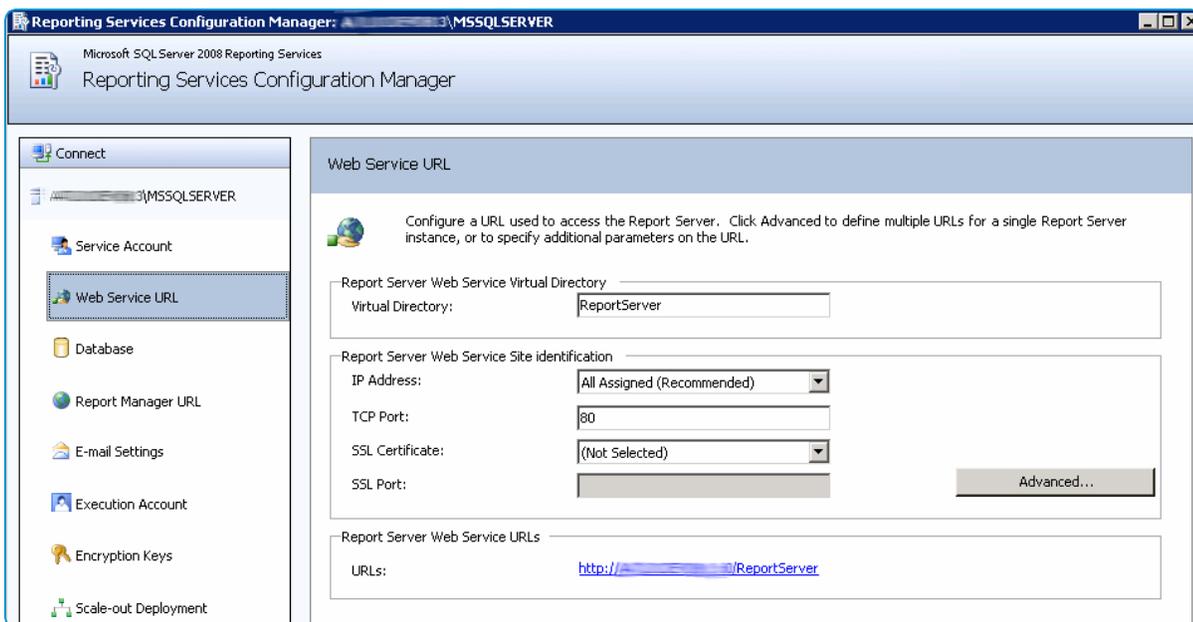
- After confirming these permissions, enter your service account details on the **Service Account** tab.



Configure the Web Service URL

After configuring service accounts (see [Configure the Service Account for SSRS](#)), you can configure the Web service URL used to access the AirWatch Reports server.

- Navigate to the **Web Service URL** tab.



- Complete the settings to configure the Web Service URL.

This URL is the endpoint that the Console Server accesses to view reports, and is specified in the Virtual Directory text box. The reporting URL is entered into the console as http://SSRS_SERVERNAME/ReportServer.

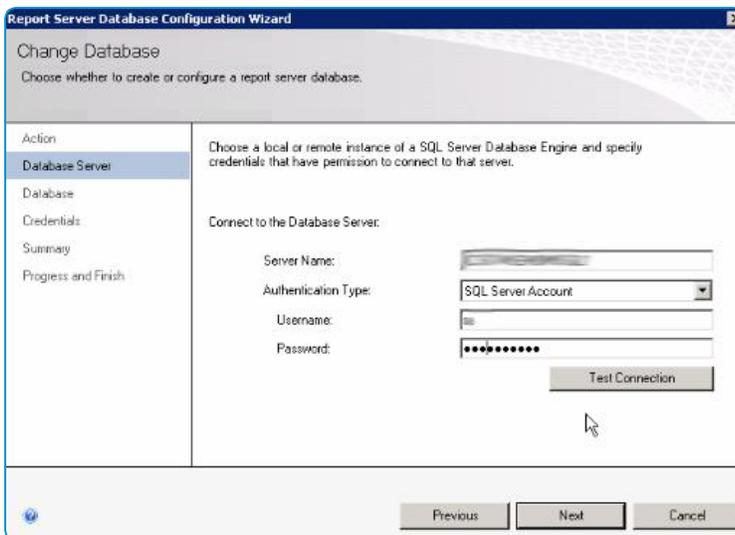
Note: If both IIS 7.0 and SQL Server are running on the same machine (that is, Appliance Type installs), set the SQL Server endpoint to listen on a port other than 80. This problem does not exist for IIS 6.0.

If there are multiple instances of reporting on the same SQL Server, give the new Web Service URL a unique name, for example, ReportServer_AirWatch.

Set up the Reporting Database

AirWatch Reports requires its own database. Use the following basic procedures to set up this database.

1. Configure the database used for the reporting services data. SysAdmin (SA) privileges are required to create an AirWatch Reporting database.



2. Specify the database used for reporting. The default name is **ReportServer**. If this name is already in use, change it to create a reporting database.

3. Create the Report Server Database in **Native Mode**.

The screenshot shows the 'Report Server Database Configuration Wizard' window, specifically the 'Change Database' step. The window title is 'Report Server Database Configuration Wizard' and the subtitle is 'Change Database'. Below the subtitle is the instruction: 'Choose whether to create or configure a report server database.' The left sidebar contains a list of steps: 'Action', 'Database Server', 'Database', 'Credentials', 'Summary', and 'Progress and Finish'. The 'Database' step is currently selected. The main area contains the following fields and options:

- Action:** Enter a database name, select the language to use for running SQL scripts, and specify whether to create the database in native or SharePoint mode.
- Database Name:** ReportServer
- Temp Database Name:** ReportServer Temp
- Language:** English (United States)
- Report Server Mode:**
 - Native Mode
 - SharePoint Integrated Mode

At the bottom of the window are three buttons: 'Previous', 'Next', and 'Cancel'.

4. Use the report server credentials to connect to the Report Server Database.

The screenshot shows the 'Report Server Database Configuration Wizard' window, specifically the 'Change Database' step. The window title is 'Report Server Database Configuration Wizard' and the subtitle is 'Change Database'. Below the subtitle is the instruction: 'Choose whether to create or configure a report server database.' The left sidebar contains a list of steps: 'Action', 'Database Server', 'Database', 'Credentials', 'Summary', and 'Progress and Finish'. The 'Credentials' step is currently selected. The main area contains the following fields and options:

- Action:** Specify the credentials of an existing account that the report server will use to connect to the report server database. Permission to access the report server database will be automatically granted to the account you specify.
- Credentials:**
 - Authentication Type:** Service Credentials
 - User name:** LocalSystem
 - Password:** (empty field)

At the bottom of the window are three buttons: 'Previous', 'Next', and 'Cancel'.

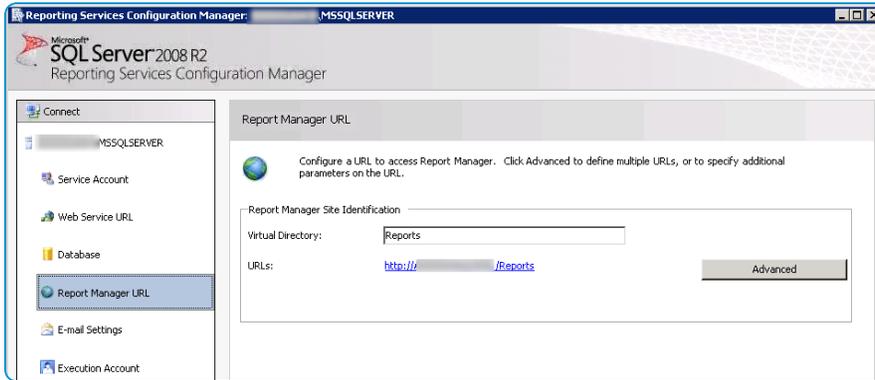
5. Complete the remaining options.

Verify the Report Manager URL and Web Service URL

The **Report Manager** is a service provided by SSRS to enable users to manage reports and to set the data source that the reporting Server uses. Use the Report Manager to add reports and upload RDL files to the AirWatch Reporting folder.

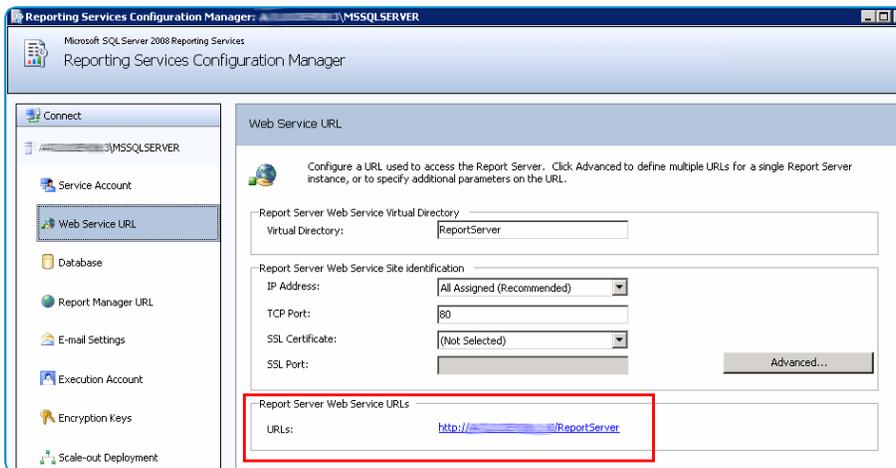
1. Access the Report Manager using the URL listed in the Report Manager URL page.

The default path is `http://SERVER_NAME/Reports`



2. Access the Web Service URL using the URL listed in the Web Service URL page.

The default path is `http://SERVER_NAME/ReportServer`



Set up the AirWatch SSRS User

The AirWatch Console requires credentials to access the reports server endpoint and run reports. These credentials allow the Console to communicate from the server it is hosted on and access the report server endpoint as an anonymous IIS user.

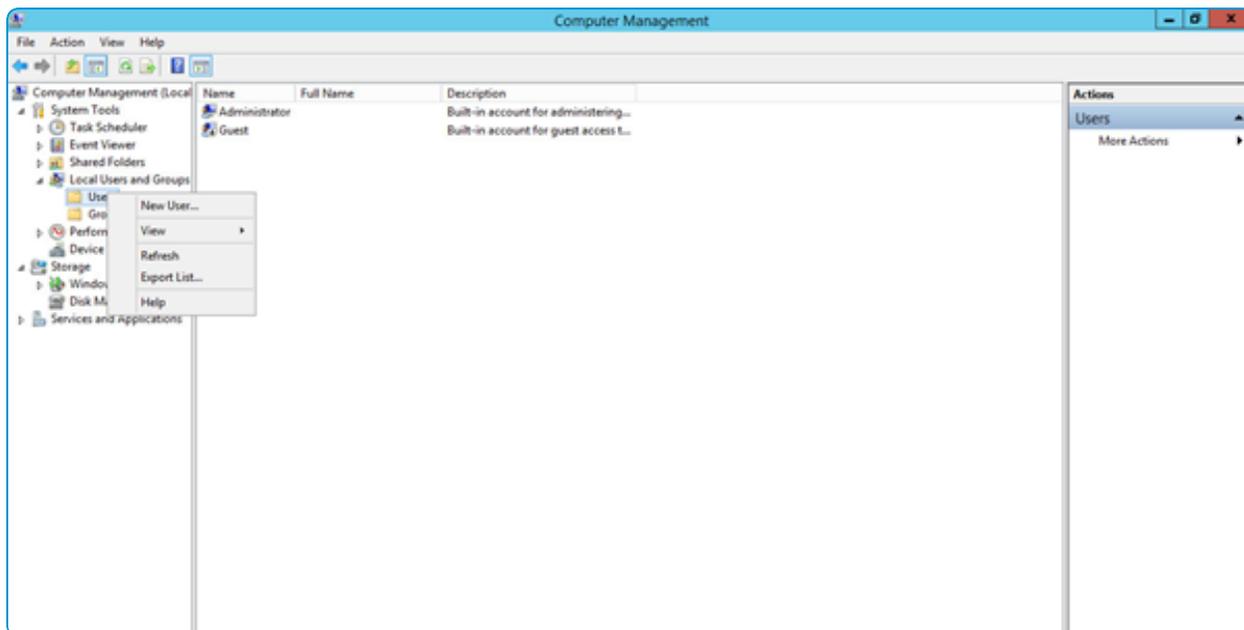
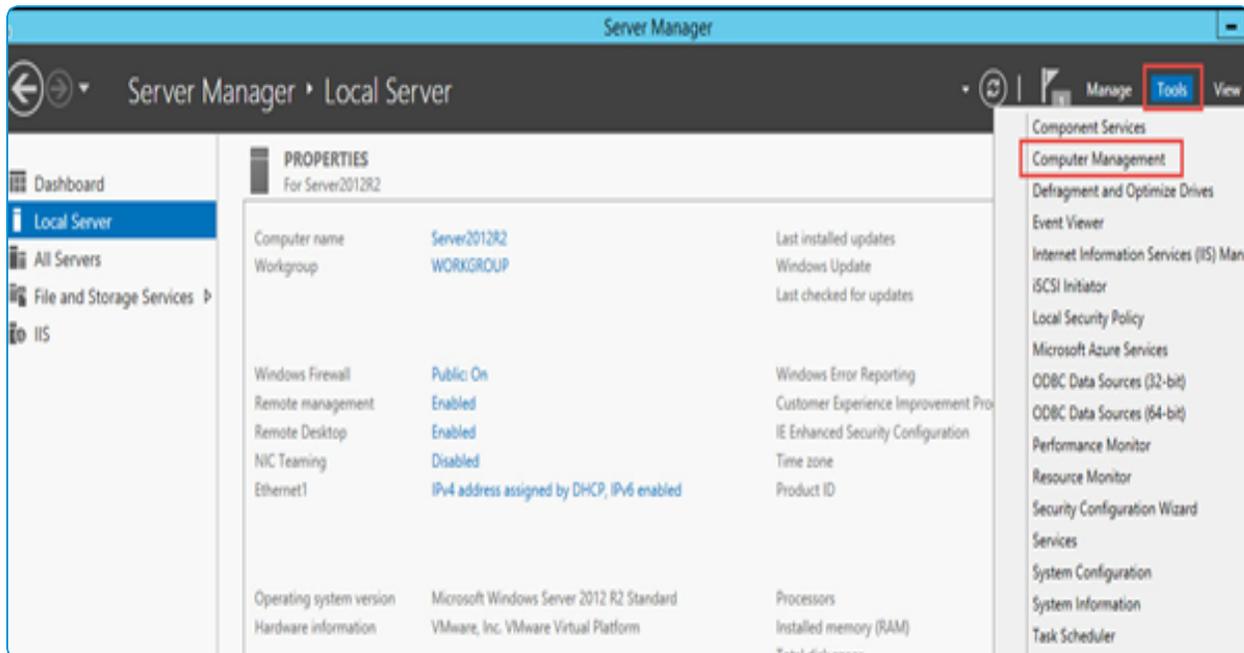
This can be done in two ways:

- Use a Domain Service Account that is a member of the Anonymous IIS user group on both the console and the SSRS Server.
- Set up a local user with the same Username and Password on both the Console Server and the Report Server and add this user to the IIS user groups on both Servers.

The steps below cover creating a local user. If you are using a domain service account, you can skip to Add the SSRS User to IIS_IUSRS.

Creating a Local User

1. From your local server, navigate to **Tools > Computer Management** and under **Local Users and Groups**, add a user. This must be done on both the **Console Server** and the **SQL Server** running SSRS.

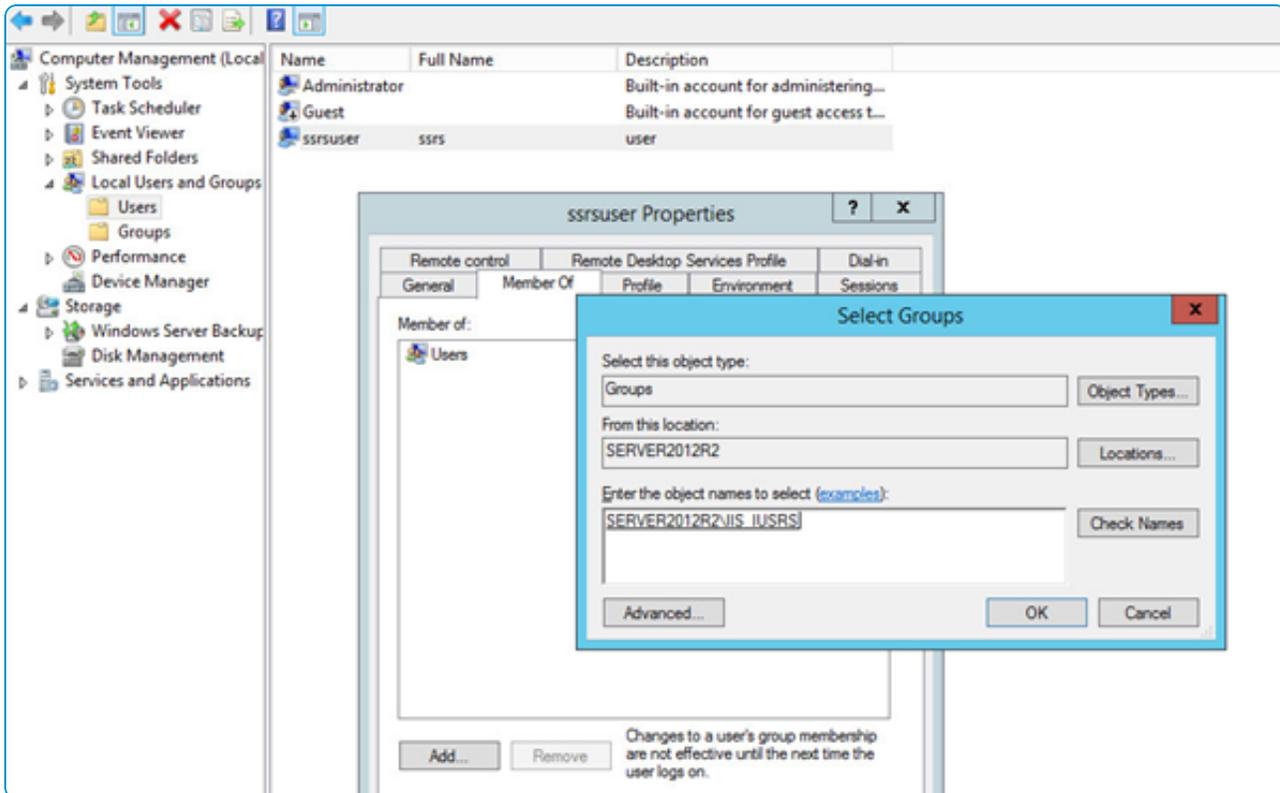


2. Choose any user name and password, if they are the **same on both the Console and SQL Reporting Server**. Remember these credentials for use in the AirWatch Console as the user name and password.
3. Clear the **User must change password at next logon** check box, and select the **User cannot change password** and the **Password never expires** check boxes.

Add the SSRS User to IIS_IUSRS

Whether you are using a Domain Service Account or a local user, that user must be added to the IIS_IUSRS group.

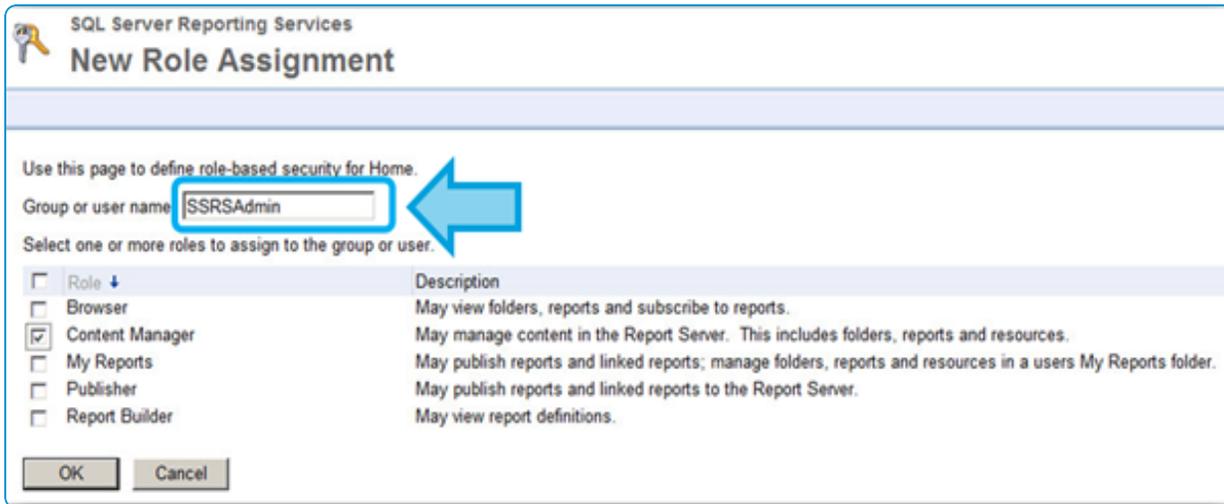
1. Click the **Member Of** tab for the user, and add the user to the **IIS_IUSRS** Group.



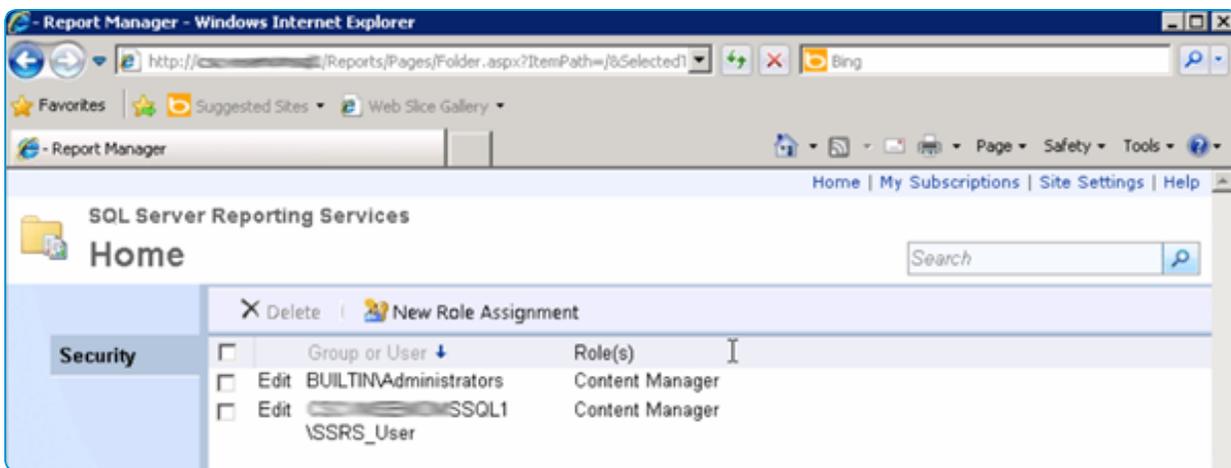
2. Ensure the SSRS_USER is also created on the AirWatch Console Server using the same steps. The password must be same.

Next you must add the SSRS_USER to the Content Manager Role.

3. On the SQL Server, navigate back to the **Reporting Services Configuration Manager**, select **Report Manager URL**.
4. Click **Folder Settings > Security > New Role Assignment**, from the home screen.
5. Enter the created SSRS User and select the **Content Manager** option.



6. Ensure that the SSRS_USER presents as a Content Manager in the **Home** folder.



Run the AirWatch Reporting Installer

The AirWatch Reporting Installer automatically configures reports, subscriptions to reports, and data driven emails on your server.

The Windows user running the Report installer must have access to both Report Manager and Report Database, as this access is required to deploy the report files on the Report Server. If you run the AirWatch Reporting Installer on a separate server from the AirWatch database, ensure that your user has write access to the AirWatch database.

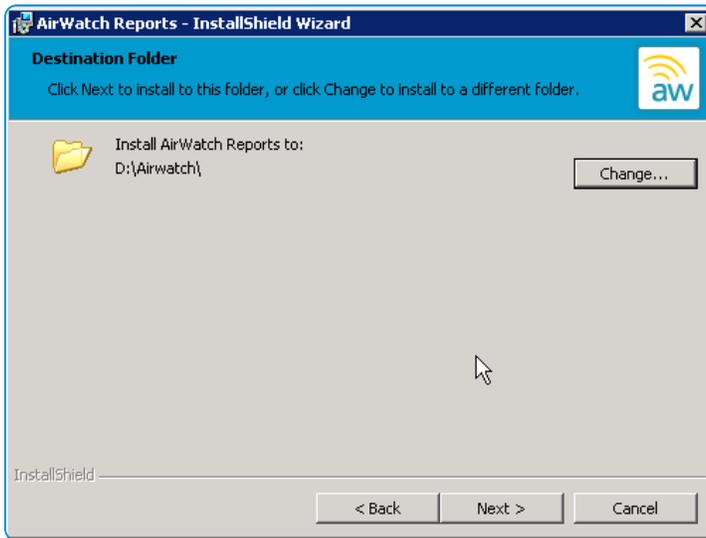
If you are using the Windows authentication credentials of the current user to connect to the database you are installing to, you must:

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

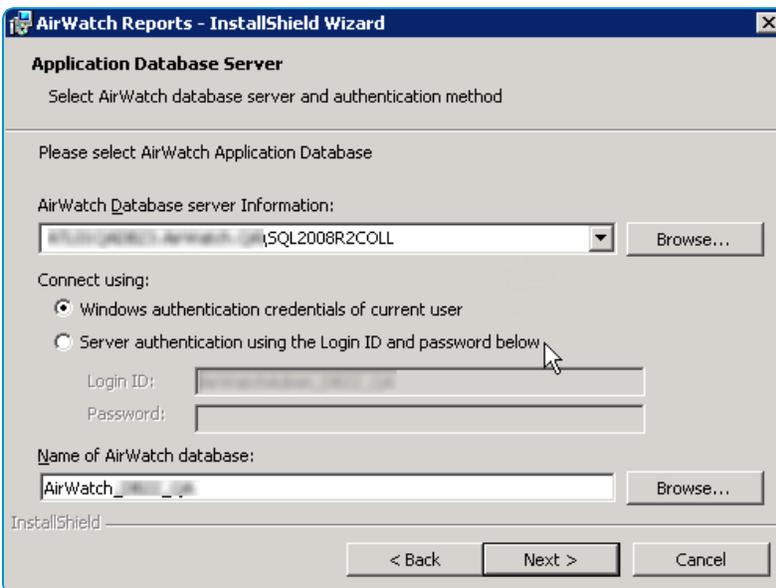
Perform the following steps to install AirWatch Reports:

1. On the SQL Reporting Services server (typically on the SQL server), open the **9.2 Reports** folder, right-click the **AirWatch_Reports executable**, and **Run as an administrator**.

2. Accept the End User License Agreement.
3. Choose a folder in which to download all installation files. After the download is complete, the installer uploads report files to the Report Server.



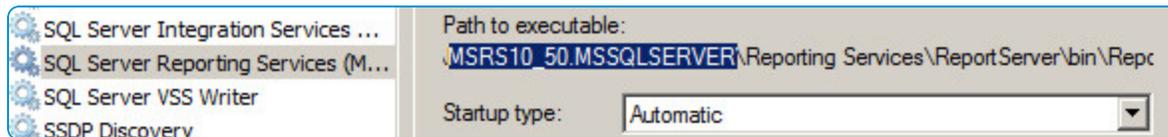
4. Complete the database connection information text boxes. A best practice is to connect using the local SQL account you used to install the AirWatch database, because it already has the correct permissions.
 - Connect using Windows authentication credentials.



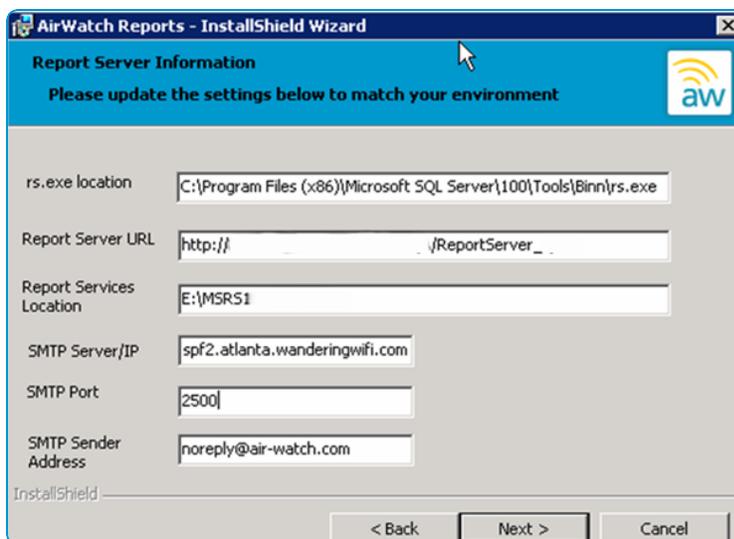
5. Provide Report Server and SMTP information, as shown. Confirm that the Report Server URL and Report Services Location are correct.
 - **rs.exe location** - The installer automatically populates this text box. If it is not populated, the typical path for this file is C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\rs.exe.
 - **Report Server URL** - This URL is the Web Service URL you configured in the step 1.

- **Report Service Location** - Navigate to Server Manager or go to Services.msc and open the **Services** tab to locate Report Services. Right-click "SQL Server Reporting Services" service and choose properties to view the path to executable. You only need the root directory. If you are running multiple instances of SSRS, then select the one that hosts AirWatch.

To avoid typographical errors, open **Server Manager** and navigate to **Services**. Locate **SQL Server Reporting Services**, select **Properties**, then copy the path **before** "\\Reporting Services" and paste it into the Report Services Location text box. See the image for an example. Ensure that there is no trailing "\\" in the Report Services Location text box once pasted.

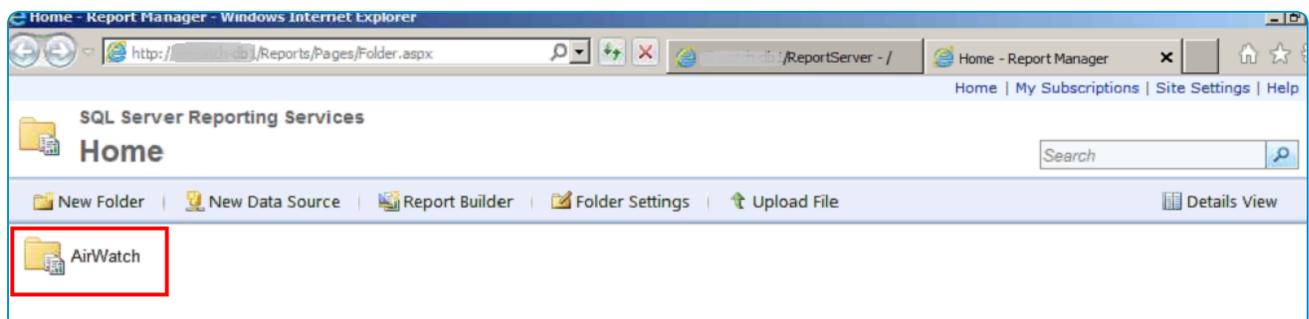


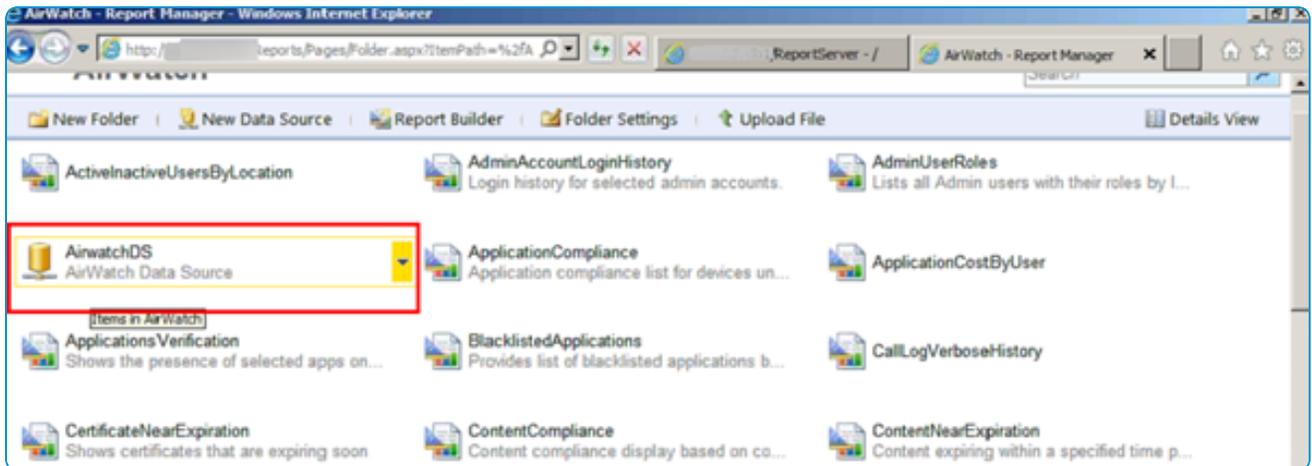
- **SMTP Port** - Pull the SMTP information from the rsReportServer.config file, located under E:\DirectoryAbove\Reporting Services\ReportServer\rsreportserver.config.



6. **For Only Windows authentication credentials:** From the SSRS, update the AirWatchDS information in the Connect using area.

- a. Locate and access the AirWatch Data Source in your SSRS instance:





- b. Select the **Credentials stored securely in the report server** option.

 A screenshot of the 'Generate Model' dialog box in the report manager. The dialog has a title bar with 'Delete', 'Move', and 'Generate Model' buttons. It contains the following fields and options:

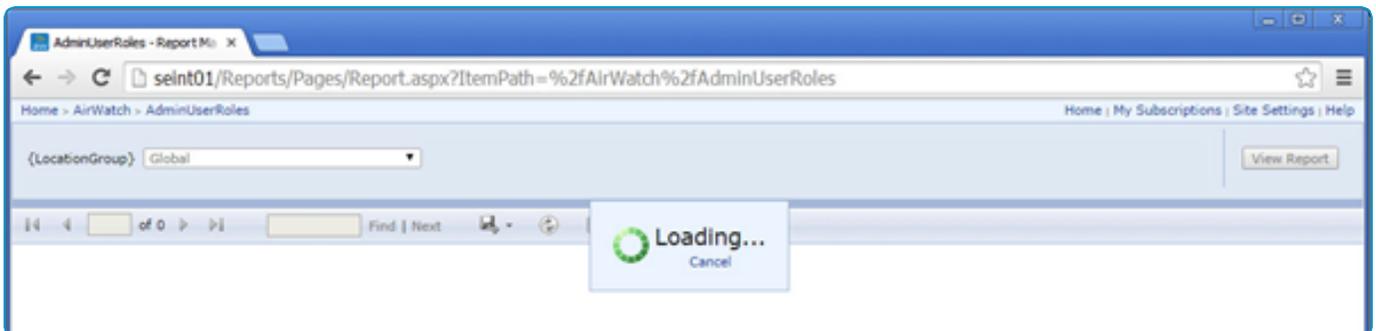
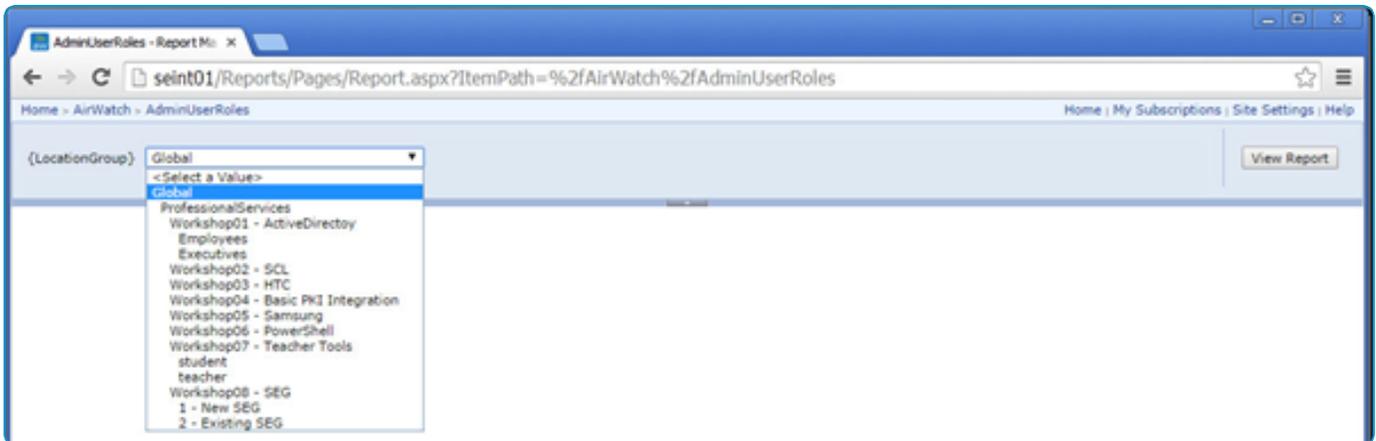
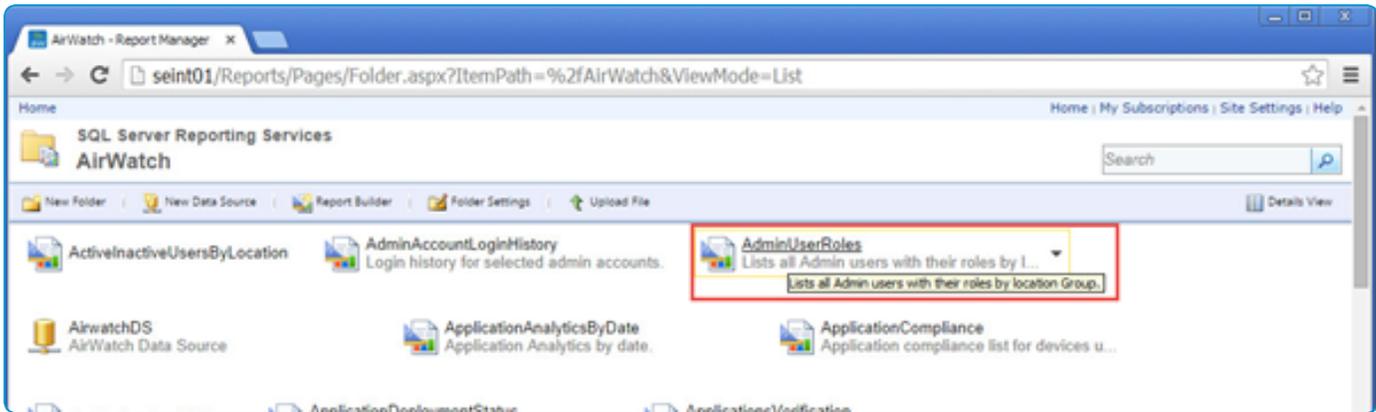
- Name: AirwatchDS
- Description: AirWatch Data Source
- Hide in tile view
- Enable this data source
- Data source type: Microsoft SQL Server
- Connection string: Data Source=.
- Connect using:
 - Credentials supplied by the user running the report
 - Display the following text to prompt user for a user name and password: Type or enter a user name and password to access the data source
 - Use as Windows credentials when connecting to the data source
 - Credentials stored securely in the report server
 - User name: [redacted]
 - Password: [redacted]
 - Use as Windows credentials when connecting to the data source
 - Impersonate the authenticated user after a connection has been made to the data source
 - Windows integrated security
 - Credentials are not required

 At the bottom, there are 'Test Connection' and 'Apply' buttons.

- c. Enter a user name. This user name is the same user name you use to run the SSRS.
- d. Enter the applicable password.
- e. Select the **Use as Windows credentials when connecting to the data source** check box and apply your settings.

Verifying Reports Functionality

To verify reports functionality, simply select a report and verify that it displays:





Integrate Reports with the AirWatch Console

The final step to enable AirWatch Reports in the Admin Console is configuring the application to use the Report Server endpoint.

If the SQL Server is on a separate domain from the Console Server, you must enter the Domain Name of the SQL Server.

1. In the Admin Console, navigate to **Groups & Settings > All Settings > Installation > Reports**. Ensure you are logged in as an administrator with the System Administrator role at the Global organization group level.
2. Enter the following parameters:
 - Server URL – The Report Server URL (http://YourReportServer/reportserver by default).
 - Username – The AirWatch SSRS user that you created.
 - Password – The AirWatch SSRS user password.
 - Domain Name – Enter the domain name of your active directory. This is only needed if you are using a Domain Service Account.

Installation / Reports

Current Setting Inherit Override

Server URL*

Username*

Password*

Domain Name

Reports Storage Overview

Optimize the storage of your AirWatch Reports through reports storage. This storage feature increases the performance of AirWatch Reports.

This storage is different than file storage used by reports, internal applications, and content. If you already use file storage, you do not need to enable reports storage. Consider enabling reports storage if you see a performance impact on your AirWatch database when using reports. Reports storage applies to reports only, helping increase overall reports performance, and reducing the burden on your AirWatch database.

If you enable both file storage and reports storage, reports storage overrides file storage when storing reports.

Report storage requires a dedicated server to host the service and storage of the reports.

Reports Storage Requirements

To deploy the reports storage solution, ensure that your server meets the requirements.

Note: If you are already using File Storage, then Report Storage is available, but not required to run your deployment. If you configure Reports Storage alongside File Storage, the report files will prioritize report storage over file storage.

Create the Shared Folder on a Server in your Internal Network

- Report storage can reside on a separate server or the same server as one of the other AirWatch application servers in your internal network. Ensure only the components that require access to the server can access the report storage server, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid an authentication failure. If the Device Services or Console servers are not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure Reports Storage at the Global Organization Group

Configure reports storage settings at the Global organization group level in the AirWatch Console.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for report storage.
- Give the local user read/write/modify permissions to the file share that is being used for the Report Storage Path.
If you give the user modify permission, AirWatch automatically deletes old reports from the storage. If you do not give the user modify permissions, consider monitoring report storage to prevent running out of space.
- Configure the Report Storage Impersonation User in AirWatch with the local user.

You can also use a domain service account instead of a local user account.

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use reports storage. Ensure that the reports storage location has enough space to accommodate the reports you intend to use.

For storing reports, your storage requirements depend on the number of devices, the daily number of reports, and the frequency with which you purge them. As a starting point, plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Also apply this sizing to your Console server if you enable caching.

Enable Reports Storage

Enable reports storage to store your reports on a dedicated server and increase performance.

To enable reports storage, take the following steps.

1. Navigate to **Groups & Settings > All Settings > Installation > Reports**.
2. Set **Report Storage Enabled** to **Enabled**.

3. Configure the report storage settings.

Serttings	Description
Report Storage File Path	Enter your path in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you created on the server.
Report Storage Caching Enabled	<p>When enabled, a local copy of the files requested for download is stored on the Console server as a cache copy. Subsequent downloads of the same file retrieve it from the Console server as opposed to file storage.</p> <p>If you enable caching, accommodate for the amount of space needed on the server where these files cache. For more information, see Reports Storage Requirements on page 84.</p>
Report Storage Impersonation Enabled	Enable to add a service account with the correct permissions.
Report Storage Impersonation Username	<p>Enter the username of a valid service account with both read, write and modify permissions to the shared storage directory.</p> <p>Displays when Report Storage Impersonation Enabled is enabled.</p>
Report Storage Impersonation Password	<p>Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory.</p> <p>Displays when Report Storage Impersonation Enabled is enabled.</p>

4. Select the **Test Connection** button to test the configuration.

Chapter 6:

Installation Verification

Verify Correct Site URL Population	88
Verify Connectivity	88
Verify Services Are Started	88
Validate GEM Functionality	89
(Optional) Disable Services on Multiple Console Servers	90
VMware Identity Manager Troubleshooting Overview	90

Verify Correct Site URL Population

The AirWatch system settings have a page that displays your site URLs. Verify these values have populated correctly as part of the installation.

1. Open a browser and access the console using the publicly signed URL.
2. Verify the AirWatch version by selecting **About AirWatch**.
3. Log in to the AirWatch Console by selecting a language, if applicable, and entering your credentials.
4. Accept the terms of use.
5. Define a Password Question and/or Security PIN.
6. Verify Correct Site URL Population.
 - Navigate to **Groups & Settings > All Settings > System > Advanced > Site URLs** and verify the URLs populated correctly.

The only Site URL that might include “localhost” is the Peripheral Service URL. Google Play has a hostname connected to a port number.

7. Change SOAP and REST API URLs from the AirWatch Console URL to the AirWatch Devices Services server URL:
For example, `https://acme-console.com/AirWatchServices` becomes `https://acme-ds.com/AirWatchServices` and `https://acme-console.com/API` becomes `https://acme-ds.com/API`.
For deployments of up to 100,000 devices and higher, AirWatch recommends a standalone API server, in which case you should change the Site URL to match your dedicated API server URL.

Verify Connectivity

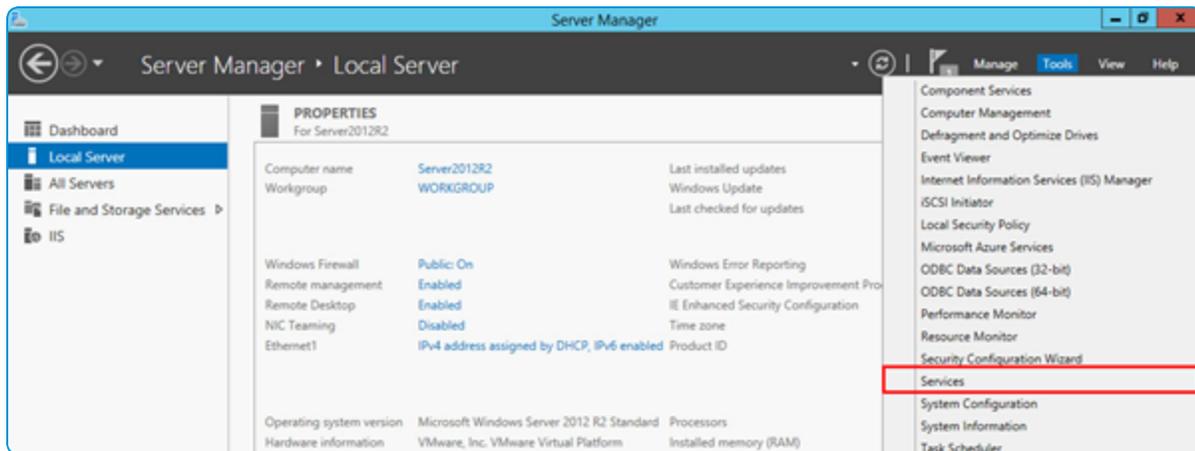
After installation, navigate to the various endpoints for each of the installed components to ensure that they are up and running.

1. Navigate to `https://localhost/AirWatch` from the Console server. An SSL error displays. Select to **Proceed anyway** and then the AirWatch Console login page displays.
2. Navigate to `https://localhost/DeviceManagement/Enrollment` on the Device Services server. On a device connected through data network connection or internal Wi-Fi, navigate to `https://<DS_URL>/DeviceManagement/Enrollment`.
3. From the AirWatch Devices Services Server, if that is where you installed the AWCM component, verify AWCM communication by opening the status page: `https://<DS_URL>:2001/awcm/status`.

Verify Services Are Started

After installation, verify that the various services for each of the installed components are started to ensure that they are up and running.

1. Open the **Server Manager**.
2. From the left pane, select Local Server then navigate to **Tools > Services**.



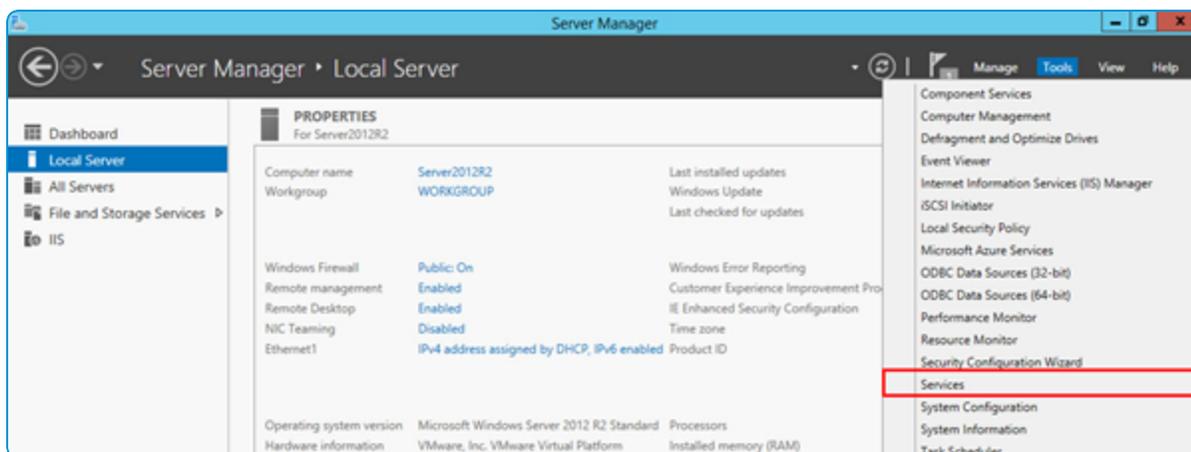
You will see all AirWatch Services at the top of the services list in alphabetical order. Each of these services start with AirWatch in the name.

3. Verify that each of these services show **Started** as the Status.

Validate GEM Functionality

After installation, ensure that the GEM Inventory Service is up and running.

1. On your Console server, navigate to **C:\AirWatch\Logs\Services**. Delete the AirWatchGemAgent.log file.
2. Open the **Server Manager**.
3. From the left pane, select Local Server and navigate to **Tools > Services**.



4. 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 **Restart**.
5. 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.

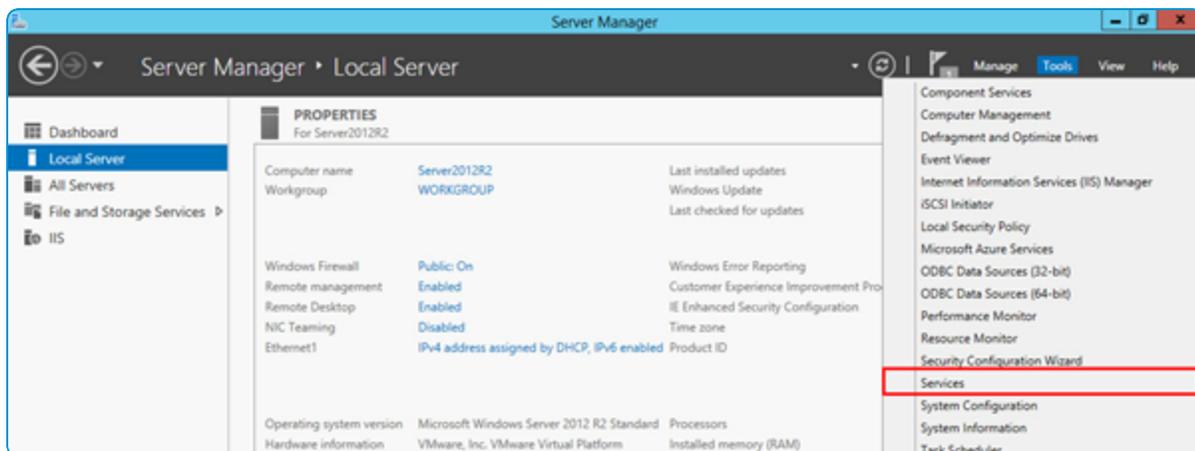
If you do not see a log file in this folder, then this is normal and you do not need to contact AirWatch Support.

(Optional) 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.

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



3. 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**, **Directory Sync**, and **AirWatch GEM Inventory Service**, right-click and select **Stop**.

VMware Identity Manager Troubleshooting Overview

If you are having issues with your VMware Identity Manager service, consider troubleshooting your issue before calling support. These troubleshooting steps involve logging in to the VMware Identity Manager service server to restart services.

These troubleshooting steps address the most common issues with the VMware Identity Manager service. The steps include:

- [Users Unable to Start Applications or Incorrect Authentication Method Applied in Load-Balanced Environments on page 90](#)
- [Group Does Not Display Any Members after Directory Sync on page 91](#)
- [Troubleshoot Elasticsearch and RabbitMQ on page 92](#)

Users Unable to Start Applications or Incorrect Authentication Method Applied in Load-Balanced Environments

Users are unable to start applications from the Workspace ONE portal or the wrong authentication method is applied in a load-balanced environment.

Problem

In a load-balanced environment, problems such as the following might occur:

- Users are unable to start applications from the Workspace ONE portal after they log in.
- The wrong authentication method is presented to users for step-up authentication.

Cause

These problems can occur if access policies are determined incorrectly. The client IP address determines which access policy is applied during login and during an application start. In a load-balanced environment, VMware Identity Manager uses the X-Forwarded-For header to determine the client IP address. Sometimes, an error might occur.

Solution

Set the `service.numberOfLoadBalancers` property in the `runtime-config.properties` file in each of the nodes in your VMware Identity Manager cluster. The property specifies the number of load balancers fronting the VMware Identity Manager instances.

Note: Setting this property is optional.

1. Log in to the VMware Identity Manager appliance.
2. Edit the `/usr/local/horizon/conf/runtime-config.properties` file and add the following property:

```
service.numberOfLoadBalancers numberOfLBs
```

where `numberOfLBs` is the number of load balancers fronting the VMware Identity Manager instances.

3. Restart the workspace appliance.

```
service horizon-workspace restart
```

Group Does Not Display Any Members after Directory Sync

Directory sync completes successfully but no users are displayed in synced groups.

Problem

After a directory is synced, either manually or automatically, the sync process completes successfully but no users are displayed in synced groups.

Cause

This problem occurs when there is a time difference of 5 seconds or more between the two or more nodes.

Solution

1. Ensure that there is no time difference between the nodes. Use the same NTP server across all nodes in the cluster to synchronize the time.
2. Restart the service on all the nodes.

```
service horizon-workspace restart
```

3. (Optional) In the administration console, delete the group, add it again in the sync settings, and sync the directory again.

Troubleshoot Elasticsearch and RabbitMQ

Use this information to troubleshoot problems with Elasticsearch and RabbitMQ in a cluster environment. Elasticsearch, a search and analytics engine used for auditing, reports, and directory sync logs, and RabbitMQ, a messaging broker, are embedded in the VMware Identity Manager full service.

Troubleshooting Elasticsearch

You can verify the health of Elasticsearch by using the following command in the VMware Identity Manager service.

```
curl 'http://localhost:9200/_cluster/health?pretty'
```

The command should return a result similar to the following:

```
{
  "cluster_name" : "horizon",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 3,
  "number_of_data_nodes" : 3,
  "active_primary_shards" : 20,
  "active_shards" : 40,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  Installing and Configuring VMware Identity Manager
  104
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0
}
```

If Elasticsearch does not start correctly or its status is red, follow these steps to troubleshoot:

1. Ensure port 9300 is open.
 - a. Update the node details by adding the IP addresses of all nodes in the cluster to the `/usr/local/horizon/scripts/updateiptables.hzn` file:

```
ALL_IPS="node1IPadd node2IPadd node3IPadd"
```

- b. Run the following script on all nodes in the cluster:

```
/usr/local/horizon/scripts/updateiptables.hzn
```

2. Restart Elasticsearch on all nodes in the cluster.

```
service elasticsearch restart
```

3. Check the logs for more details.

```
cd /opt/vmware/elasticsearch/logs

tail -f horizon.log
```

Troubleshooting RabbitMQ

You can verify the health of RabbitMQ by using the following command in the VMware Identity Manager service.

```
rabbitmqctl cluster_status
```

The command should return a result similar to the following:

```
Cluster status of node 'rabbitmq@node3' ...
[{nodes, [{disc, ['rabbitmq@node2', 'rabbitmq@node3']}]},
 {running_nodes, ['rabbitmq@node3']},
 {cluster_name, <<"rabbitmq@node2.example.com">>},
 {partitions, []},
 {alarms, [{'rabbitmq@node3', []}]}
```

If RabbitMQ does not start or the health URL <https://<hostname>/SAAS/API/1.0/REST/system/health> shows "MessagingConnectionOk": "false", follow these steps to troubleshoot:

1. Ensure ports 4369, 5700, 25672 are open. To open the ports:
 - a. Create the file by using this command:

```
touch /usr/local/horizon/scripts/updateiptables.hzn
```

- b. Run the following script:

```
/usr/local/horizon/scripts/updateiptables.hzn
```

2. Restart RabbitMQ.
 - a. Kill any existing `rabbitmq` processes.
 - b. `rabbitmqctl stop`
 - c. `rabbitmq-server -detached`
3. You may need to restart the VMware Identity Manager service if RabbitMQ does not start gracefully.

```
service horizon-workspace restart
```

Fix Memory Allocation Issues when using VMware Identity Manager for App Catalog Only

The VMware Identity Manager service does not dynamically allocate memory. If you have additional memory over the minimal requirements, you must update the `wrapper.conf` file to reflect the additional memory.

Problem

The VMware Identity Manager service does not use all available memory on the server when deployed for App Catalog only.

Cause

The VMware Identity Manager service has hard-coded memory allocation in the `wrapper.conf` file. If you use additional memory over the minimal requirements, the service does not dynamically update the memory allocation to reflect the additional memory.

Solution

You must edit the `wrapper.conf` file to use the additional memory.

To edit the file:

1. Login to the server as an administrator
2. Navigate to the file:

```
C:\INSTALL_DIR\VMwareIdentityManager\opt\vmware\horizon\workspace\conf\wrapper.conf
```

3. Edit the following lines of the file:

```
wrapper.java.additional.13="-Xss1m"
```

This line sets the java thread stack size.

```
wrapper.java.additional.14="-Xmx2g"
```

This line specifies the maximum memory allocation pool for a Java Virtual Machine (JVM).

```
wrapper.java.additional.15="-Xms768m"
```

This line specifies the initial memory allocation pool.

4. After updating wrapper.conf, reinstall the service:

```
<VMWARE_INSTALL_DIR>\usr\local\horizon\scripts\horizonService.bat reinstall
```

If you are running as a domain user, you must enter the following values:

```
wrapper.ntservice.account=  
wrapper.ntservice.password=
```

After service installation, the password is erased from the file.

5. After installation, restart the service:

```
c:\INSTALL_DIR\usr\local\horizon\scripts\horizonService.bat start
```

Chapter 7:

Next Steps

Overview	97
Create a Corporate Apple ID	97
Run the Workspace ONE Wizard	97

Overview

Now that you have installed AirWatch, you will want to perform some testing, such as test enrolling devices. To do this you will need the devices themselves, such as an iPhone/iPad or Android smartphone or tablet. You will also need to create a corporate Apple ID and corporate Google ID.

Create a Corporate Apple ID

If your deployment includes Apple iOS devices, you must generate an APNs certificate on behalf of your company. You can easily generate this certificate post-installation but it requires an Apple ID. Because this certificate must be renewed, AirWatch recommends that an Apple ID is created with an email address multiple users have access to. This way, your company does not have to rely on one person in order to renew the certificate. If you need to create a new Apple ID, please follow the link below and select Create an Apple ID:

<https://appleid.apple.com>

Run the Workspace ONE Wizard

VMware Identity Manager is required for Workspace ONE deployments and must be configured to communicate with your AirWatch Console. This process is largely automated through the AirWatch Getting Started experience in the AirWatch Console. Consider using the Getting Started wizard before attempting to use the Workspace ONE application.

Only run the Getting Started wizard after the health API has passed and the load balancer (if you are using one) shows "green."

For a walkthrough of enabling VMware Identity Manager integration, the Workspace ONE application, and core Workspace ONE features, please see the Workspace ONE Quick Start Guide, available at https://docs.vmware.com/en/VMware-Identity-Manager/3.2/ws1_quickconfiguration.pdf.

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.