Installing Workspace ONE UEM

for on-premises and SaaS deployments

VMware Workspace ONE UEM 2203

vmware®

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

https://docs.vmware.com/

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

Contents

Workspace ONE UEM Installation 1

You can install Workspace ONE UEM powered by AirWatch onto application servers to meet your deployment needs. The installer handles the Workspace ONE UEM console server components, the Devices Services server components, and API server components. Learn more about installation prep, documentation, and verification of the Workspace ONE UEM installation process.

Workspace ONE UEM Installation Preparation

Installing Workspace ONE UEM requires specific prerequisites and procedures in an on-premises solution. Make sure to meet the prerequisites before proceeding with the installation instructions.

For detailed instructions on preparing for installation, see Chapter 2 Preparing to Install Workspace ONE UEM.

Database and Application Server Installations

Installing Workspace ONE UEM on premises involves configuring servers for your database, application, and any auxiliary components, and reports. Workspace ONE UEM comprises several different components, which can be combined with application servers or installed on their own dedicated servers.

To begin the database server installation, see Chapter 3 Installing Workspace ONE UEM Database Servers.

To begin the application server installation, see Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services).

Reports Installation and Storage

Installing Workspace ONE UEM on premises involves installing and configuring reporting functionality for your deployment. After the reporting functionality is set up, you must configure storage for the reports that Workspace ONE UEM generates.

To install and configure reports, see Chapter 5 Installing Workspace ONE UEM Reports .

Installation Verification

After Workspace ONE UEM is installed and configured, verify that all the components you have installed function properly.

To verify your installation, see Chapter 6 Verifying the Workspace ONE UEM Installation.

Next Steps

When your installation is finished, see Chapter 7 Workspace ONE UEM Post-Installation Steps for information on running the Workspace ONE Getting Started Wizard.

Recommended Architecture

To review recommended architectures based on your deployment size, refer to the **VMware Workspace ONE UEM Recommended Architecture Guide**, available at docs.vmware.com.

This chapter includes the following topics:

- Before You Begin Checklist
- Procedure Checklist for Installing Workspace ONE UEM

Before You Begin Checklist

Installing Workspace ONE UEM has several caveats and notes that need to be addressed prior to beginning the installation. Learn more about the requirements, install package files, and the Workspace ONE UEM components.

Be aware of several notes and caveats before attempting to install Workspace ONE UEM 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 docs.vmware.com. Workspace ONE UEM frequently makes updates to documentation; 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 Workspace ONE UEM consultant as part of the deployment process. If you do not have the link to the installation package files, then you can search for the files in My Workspace ONE Resources.

Meet the Requirements

Meet all the requirements needed for a Workspace ONE UEM installation. Specific hardware and software requirements are outlined in the **Workspace ONE UEM Recommended Architecture Guide**, available on docs.vmware.com. A list of other requirements can be found in the Chapter 2 Preparing to Install Workspace ONE UEM.

Note As of AirWatch v9.1 we have changed our supported SQL versions. Review the latest list of prerequisites in the **Recommended Architecture Guide** to ensure that your current version is supported.

To ensure an uninterrupted installation of Workspace ONE UEM, temporarily deactivate scanning for any anti-virus software running on the servers you are updating.

Verify On-Call Resources

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

Workspace ONE UEM Components

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

- The **Workspace ONE UEM console Server** refers to the component of Workspace ONE UEM that renders and displays the UEM console. It presents and sends data to the database directly from the Workspace ONE UEM console.
- The **Workspace ONE UEM Device Services Server** refers to the component of Workspace ONE UEM 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 **Workspace ONE UEM Application Server** is any server that runs a Workspace ONE UEM instance. The standard Workspace ONE UEM deployment method involves installing multiple application servers for these components alongside a database. For each procedure in this guide that references an Application server, complete the procedure on all Workspace ONE UEM servers (Console, Device Services, AWCM, API).
- This documentation assumes that you are using one of the recommended architectures as detailed in the **Workspace ONE UEM Recommended Architecture Guide**, available on docs.vmware.com. If you are not using one of these architectures, contact VMware AirWatch for additional assistance.

A Note About Screenshots in this Document

Where applicable, this documentation uses screenshots from Windows Server 2012 R2. If you are using Windows Server 2016 or Windows Server 2019 Desktop Experience, then perform the same actions documented in this guide, with the knowledge that the exact steps can slightly differ.

Procedure Checklist for Installing Workspace ONE UEM

You can follow along the list of Workspace ONE UEM installation items to ensure you perform the steps in order. Learn more about the installation steps, their requirements, and documentation notes to assist with the Workspace ONE UEM installation process.

Use the links provided to jump to a particular section, but ensure that you complete all the required steps.

StatusChecklist	Requirement	Notes
Step 1: Prepare for Your Installation		
	Verify Database Server Prerequisites Are Met	See Database Server Prerequisites.
	Verify Application Server Prerequisites Are Met	See Application Server Prerequisites.
	Perform Optional Installs	See Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services).
	Create the Workspace ONE UEM Database	See Create the Workspace ONE UEM Database.
	Assign Database Roles	See Create the Workspace ONE UEM SQL Account and Assign DB Owner Roles.
	Configure Application Servers	See Configure Your Application Servers.
	Server Internal DNS and Certificate Requirements	See Configure Your Internal DNS Record and Certificates.
	Server External DNS and Certificate Requirements	See Configure Your External DNS Record and Certificates.
	Stage Install Files	See Stage Install Files.
	(OPTIONAL) Run the Workspace ONE Validation Tool	
Step 2: Perform the Database Installation		
	Run the Workspace ONE UEM Database Setup Utility	See Run the Workspace ONE UEM Database Setup Utility.
	Verify Proper Database Installation	See Verify Proper Database Installation.
Step 3: Perform Application Server Installation		
	Start the Workspace ONE UEM Installer on Each Application Server	See Chapter 4 Installing a Workspace ONE UEM Application Server.

StatusChecklist	Requirement	Notes
	(IF APPLICABLE) Run the Workspace ONE UEM Installer on Any Additional Device Services Servers	See Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services).
Step 4: Perform Reports Installation		
	Integrate Reports with the Console and Enable Reports Storage	See Chapter 5 Installing Workspace ONE UEM Reports and Reports Storage

This guide does not cover post-install configuration, but does include a Chapter 7 Workspace ONE UEM Post-Installation Steps, which covers some of the essential procedures to get you started.

Preparing to Install Workspace ONE UEM

2

There are several database, application, and certificate prerequisites that must be met to achieve a successful on-premises, Workspace ONE UEM installation. Learn more about component prerequisites and how to ensure that they are met prior to installation.

Installing Workspace ONE UEM requires specific prerequisites and procedures for an on-premises solution. Make sure to meet the prerequisites before proceeding with the installation instructions.

At any point in the installation process, you may see a prompt to reboot your system. Reboot as soon as possible. On reboot, the installer will automatically restart and proceed to the step where you left off so you can continue the installation process.

This chapter includes the following topics:

Database Server Prerequisites

Meeting database prerequisites is essential to a successful Workspace ONE UEM installation. Learn more about all requirements for SQL Server hardware and software, TCP/IP, SQL Server Always On, and how to ensure that they are met.

SQL Server Hardware Requirements

The exact specifications needed for your SQL server depend on the size and needs of your deployment. Gather this information before proceeding so you size your servers correctly. Read the **Workspace ONE UEM Recommended Architecture Guide**, available at docs.vmware.com, for hardware sizing information and other technical details that ensure the smooth operation of your Workspace ONE UEM database.

Note To ensure the best installation experience, do not run the database installer from the database server.

SQL Server Software Requirements

- SQL Server 2012, SQL Server 2014, SQL Server 2016, SQL Server 2017, or SQL Server 2019 with Client Tools (SQL Management Studio, SQL Server Agent, latest service packs). Ensure that the SQL Servers are 64-bit (OS and SQL Server).

  Workspace ONE UEM does not support Express, Workgroup, or Web editions of SQL Server. These editions do not support all the features used in the Workspace ONE UEM application. Workspace ONE UEM supports only the Standard and Enterprise Editions.
- 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 4.8 is required to run the database installer and is installed through the .NET Framework web downloader. If you do not want to install .NET on to your database server, then run the database installer from another Workspace ONE UEM server or a jump server where .NET can be installed.
- Ensure that the SQL Server Agent Windows service is set to Automatic or Automatic (Delayed) as the Start type for the service. If set to Manual, then the service has to be manually started before database installation.
- To create, back up, and restore a database, you must have the access and knowledge required.

When the database installer runs, it automatically updates your SQL server with the latest versions of:

- ODBC Driver 13 for SQL Server 64-bit
- Command Line Utilities 13 for SQL Server 64-bit

TCP/IP Enabled

Workspace ONE UEM can use TCP/IP to connect to the database. Deactivating Named Pipes forces TCP/IP communication, which can improve performance. Workspace ONE UEM works with active and deactivated named pipes. In the SQL Server Configuration Manager, navigate to **SQL Server Network Configuration** and select **Protocols** for MSSQLSERVER.

SQL Server Always On

The SQL server's Always On capability combines failover clustering with database mirroring and log shipping. Always On allows for multiple read copies of your database and a single copy for read-write operations.

For more information about Always On functionality, see https://msdn.microsoft.com/en-us/library/ff877884.aspx.

If you have the bandwidth to support the traffic generated by Workspace ONE UEM, then the Workspace ONE UEM database supports Always On. The following Always On functionality has been tested for support:

- Database in an Availability Group
- Availability Group failover
- Secondary Replica promotion to Primary
- Synchronous Replication

To integrate the SQL server's Always On, set up the following prerequisites:

- Create a database listener to integrate with the Workspace ONE UEM Application and Database installations.

  For more information on creating a database listener, see https://docs.microsoft.com/en-us/sql/database-engine/availability-groups/windows/create-or-configure-an-availability-group-listener-sql-server.

- If the SQL accounts used for Workspace ONE UEM have minimal permissions, you might need to script the SQL account creation on the secondary nodes.

  You will need to query the system table on the primary node to get the hexadecimalSID for the login. Use the following query:

  ```
  USE [master]SELECT * FROM SYS.SYSLOGINS WHERE NAME LIKE '%LOGINNAME%'
  ```

  Once you get the SID, the script below can be used to create the login on secondary nodes.

  ```
  USE [master]GOCREATE LOGIN [SqlLogin] WITH PASSWORD=N'[Password]', SID=[HexadecimalSID],
  DEFAULT_DATABASE=[myDatabase], DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRATION=[setting],
  CHECK_POLICY=[setting]GO
  ```

- If the Always On Availability Group uses different network subnets, you must configure your Availability Group Listener settings before you can deploy Workspace ONE UEM. Run the following commands using PowerShell on each database server in your cluster before you run the database installer:

```
>Get-ClusterResource <AG Listener Resource Name> | Set-ClusterParameter -Name
HostRecordTTL -Value 60
```

```
>Get-ClusterResource <AG Listener Resource Name> | Set-ClusterParameter -Name
RegisterAllProvidersIP -Value 0
```

  For more information about HostRecordTTL values, including how to retrieve the AG Listener Resource Name, see https://blogs.msdn.microsoft.com/alwaysonpro/2014/06/03/connection-timeouts-in-multi-subnet-availability-group/.

  Your database administrators decide the value for the HostRecordTTL. Low values result in a faster reconnection after a fail-over. For example, with a value of 60, the listener's DNS record updates take up to 60 seconds to match the IP address of the Primary (Active) SQL Node after an SQL fail-over.

Workspace ONE UEM Database Performance Recommendations

Workspace ONE UEM provides a database of performance recommendations based on scalability tests performed by the Workspace ONE UEM team.

Recommendation	Description
TempDB Configuration	The number of TempDB files must match the number of CPU cores when the core is less than or equal to 8 cores. Beyond 8 cores, the number of files must be the closest multiple of 4 that is less than or equal to the number of cores (example, 10 cores need 8 tempDBs, 12 cores need 12 TempDBs, 13 cores need 12 TempDBs, 16 cores need 16 TempDBs.) File size, growth rate, and the location must be the same for all TempDB files.
Memory Allocation	80% of the server memory should be allocated to SQL. The remaining 20% must be freed up to run the OS.
Cost Threshold for Parallelism and Maximum Degree of Parallelism	Cost Threshold for Parallelism is the cost needed for a query to be qualified to use more than a single CPU thread. Maximum Degree of Parallelism is the maximum number of threads that can be used per query. The following are recommended values for these parameters: ■ Cost Threshold of Parallelism: 50 ■ Max Degree of Parallelism: 2 and reduce to 1 if there is high server utilization.
Trace Flag	The following trace flags must be set to 1 at Global. 1117 (https://msdn.microsoft.com/en-us/library/ms188396.aspx) 1118 (https://msdn.microsoft.com/en-us/library/ms188396.aspx) 1236 (https://support.microsoft.com/en-us/kb/2926217) 8048 (https://blogs.msdn.microsoft.com/psssql/2015/03/02/running-sql-server-on-machines-with-more-than-8-cpus-per-numa-node-may-need-trace-flag-8048/)
Trace Flag - SQL Server 2016	See https://docs.microsoft.com/en-us/sql/t-sql/database-console-commands/dbcc-traceontrace- flags-transact-sql/view=sql-server-2017

Recommendation	Description
Hyperthreading	To ensure best performance, hyperthreading must be deactivated on the database if the database is running on a physical server. If it is on a VM, then having hyperthreading enabled on the ESX host doesn't have any performance impact, but hyperthreading must be deactivated on the Windows host level.
Optimize for Ad hoc Workloads	Enable Optimize for Ad hoc Workloads under SQL server properties. This is recommended to free memory from the server. Refer to the following article for more information: https://msdn.microsoft.com/en-us/library/cc645587(v=sql.120).aspx.
Lock Escalation	Deactivate Lock Escalation for the “interrogator.scheduler” table by running the “alter table interrogator.scheduler set (lock_escalation = {Disable})” command. This is recommended as the scheduler table has very high rate of updates/inserts. There is a high contention on this table with the use of FCM, and deactivating lock escalation helps improve performance. However, the drawback is that more memory is consumed. Refer to the following article for more information: https://technet.microsoft.com/en-us/library/ms184286(v=sql.105).aspx.
Autogrowth	For Production and Temp DBs, set Autogrowth to 128 MB and max size to Unlimited.

For device deployments of more than 150,000 devices, ensure that the Database is partitioned. You can run the installer from an elevated command prompt with the following flag:

`Name_Of_Database_installer.exe /V"AWINSTALLPARTITIONEDDATABASE=1".`

For example: `AirWatch_DB_9.1_GA_Setup.exe /V"AWINSTALLPARTITIONEDDATABASE=1".`

Important This command requires SQL Enterprise. If you are running this command on a Workspace ONE UEM Database, you must run the installer with the flag for each upgrade from then on. If you do not, an error displays.

Application Server Prerequisites

Meeting application server prerequisites is essential to a successful Workspace ONE UEM installation. Learn more about all requirements for your hardware, network, software, Server Manager roles, RDP, and VM Access to Application Servers, and Service account permissions.

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

A Workspace ONE UEM installation can involve many servers, and the exact specifications depend on the size and needs of your deployment. Gather this information before proceeding so you size your servers correctly. Read through the **Workspace ONE UEM Recommended Architecture Guide**, available at docs.vmware.com, for hardware sizing information and other technical details that ensure the smooth operation of your Workspace ONE UEM solution.

Network Requirements

Review all the network requirements as outlined in the **Workspace ONE UEM Recommended Architecture Guide**. These requirements include the firewall ports that must be opened for Workspace ONE UEM 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
- Branch Cache enabled on all application servers
- Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 Desktop Experience
  - For Windows Server 2012 R2, ensure that your Windows installation includes KB2999226 to avoid errors when you start a .NET Core application.
- .NET Framework 4.8. The .NET Framework 4.8 web installer is packaged with the Workspace ONE UEM installer and installs automatically if it is not already present.
- NET Core 3.1.1. The minimum supported .NET Core version is 3.1.1.
- PowerShell version 5.0+ if you are deploying the PowerShell MEM-direct model for email. To verify your version, open PowerShell and run the command $PSVersionTable. More details on PowerShell and other email models are available in the **Workspace ONE UEM Mobile Email Management Guide**, available at docs.vmware.com.
- Microsoft SQL Server 2012 Native Client 11.3.6538.0 to run the database installer. If you do not want to install SQL Server 2012 Native Client, run the database installer from another Workspace ONE UEM server (or a jump server) where Microsoft SQL Server 2012 Native Client 11.3.6538.0 can install.

  Note You must have administrator privileges to run the database installer.
- If you plan to use an Active Directory service account for SQL authentication to the Workspace ONE UEM database, then the Workspace ONE UEM application server must be joined to the domain. This AD service account must have administrator-level permissions for each application server.
- URL Rewrite 2.0. The correct URL Rewrite version will download and install as part of the installation process if it is not present.
- Enable the following cipher suites based on the server version of the application servers to communicate with Apple for the new HTTP/2 change that went into effect in 2021:
  - “TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384” (Windows Server 2016 and later) - This is handled by a crypto library in the product for operating systems that do not support it.
  - "TLS_RSA_WITH_AES_256_CBC_SHA" (Windows 2012 R2 and earlier)

Proxy Requirements

The Workspace ONE UEM servers can be configured with a proxy/PAC file for outbound Internet access.

Apple APNs traffic is not HTTP traffic, and is not 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, then your proxy application must support SOCKS V5, SOCKS V4, and SOCKS V4a are not supported.

To verify the integrity of Android devices and ensure that they are not compromised, the Workspace ONE UEM Device Services application uses Google's SafetyNet Attestation API. To do so, it makes outbound API calls to Google servers. In on-premises environments, organizations might choose to only allow the Device Services application to make outbound connections through a proxy. In these cases, customers must configure the proxy settings at the application level in the Workspace ONE UEM Console and the outbound proxy at the system level for the Windows server that hosts the Device Services application. If the Windows server is unable to make outbound connections to the required Google endpoints, then the SafetyNet Health Attestation fails.

Install Role from Server Manager

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

- IIS 8.5 (Server 2012 R2)
- IIS 10.0 (Server 2016)
- IIS 10.0 (Windows Server 2019 Desktop Experience)

Configure the BranchCache only on Device Services servers.

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 Workspace ONE UEM is installed on. Verify this access before attempting to install Workspace ONE UEM servers.

Permissions of Workspace ONE UEM Service Accounts

The service account you create for Workspace ONE UEM needs the appropriate permissions to integrate with your back end systems. The account can be one service account that has all required access. Verify the connectivity between your Workspace ONE UEM service account and your backend systems.

Workspace ONE UEM Antivirus Prerequisites

You can implement an antivirus solution on servers running Workspace ONE UEM powered by AirWatch. Learn more about the prerequisites required to successfully implement an antivirus software within the Workspace ONE UEM platform.

Workspace ONE UEM can easily be configured to accommodate antivirus software on the servers. When you install or upgrade your antivirus solution, meet the following prerequisites:

- Exclude or remove the /AirWatch folder from the antivirus scan functionality.
- Confirm that the ports listed in the Recommended Architecture Guide, available on docs.vmware.com. are not blocked by the antivirus traffic controller.

Create the Workspace ONE UEM Database

Part of your installation prep is creating the Workspace ONE UEM database. Learn more about using an administrator account with the correct read/write permissions to successfully create the Workspace ONE UEM 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.

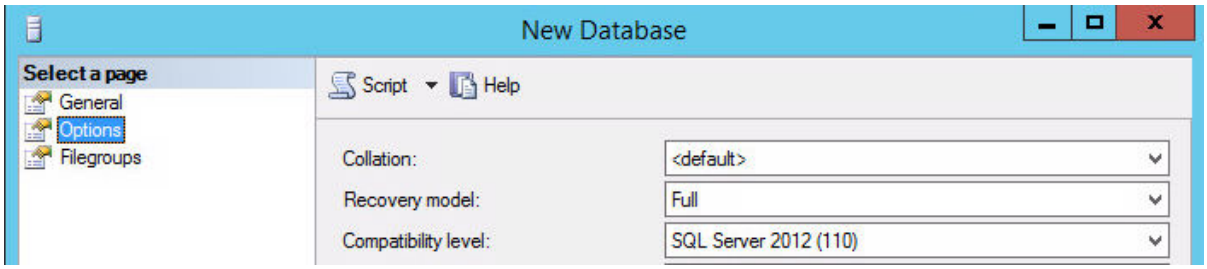
3 Click **Connect**.

4 Right-click **Databases** and select **New Database**.

5 Enter **`WorkspaceONEUEM`** as the Database name.

6 Scroll to the right side of Database files, select the **...** next to **Autogrowth for Workspace ONE UEM**, 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 Workspace ONE UEM database.

9 Expand **Databases** and verify the Workspace ONE UEM database is created.

Create the Workspace ONE UEM SQL Account and Assign DB Owner Roles

Once the Workspace ONE UEM database has been created, you must configure the SQL user credentials. Learn how to create the SQL account and a assign the proper database owner roles.

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

Procedure

1 Open SQL Server Management Studio.

2 Log in to the DB server containing the Workspace ONE UEM database.

3 Navigate to **Security > Login**, right-click, and select **New Login**.

4 Select whether to use a **Windows** account or local **SQL Server** account for authentication. For SQL Server authentication, enter your user credentials.

5 Select the Workspace ONE UEM database as the **Default database**.

6 Navigate to the **Server Roles** tab. Select Server Role as **Public**.

7 Select **User Mapping.**

8 Select the Workspace ONE UEM Database. Then, select the **db_owner** role.

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

   b Select the msdb Database. Then, select the **SQLAgentUserRole** and **db_datareader** roles. SQLAgentUserRole is not pictured below.

   Note The SQL user account used to install the DB will own SQL Server Agent Jobs and as such future upgrades require the same account to be used or an account with system admin level privileges.

9 Select **OK**.

Configure Your Application Servers

Part of the Workspace ONE UEM installation configures your application server permissions and roles automatically. Learn more about configuring the roles and permissions manually, outside of the Workspace ONE UEM installer.

The Workspace ONE UEM 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 **Workspace ONE UEM console Server** and **Workspace ONE UEM 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 might already be enabled):

- **Common HTTP Features**: Static Content, Default Document, HTTP Errors, HTTP Redirection
- **Application Development**: ASP.NET, .NET Extensibility, ASP, ISAPI Extensions, ISAPI Filters

  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
- Ensure that WebDAV is not installed.

4 Click **Next**.

5 On the **Features** tab, verify the following required features are added:

- **.NET Framework 4.x Features**:
  - .NET Framework 4.x
  - ASP.NET 4.x
  - WCF Services
  - HTTP Activation
  - TCP Port Sharing
- **Message Queuing**: Message Queuing Server (expand Message Queuing > Message Queuing Services to select)

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**.

Configure Your Internal DNS Record and Certificates

You can configure your internal DNS to connect to Workspace ONE UEM through the proper records and certificates. Learn more about how to setup your internal DNS to communicate with Workspace ONE UEM.

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 Workspace ONE UEM (specifically, the Device Services server). An internal DNS record must be registered on the internal domain server.

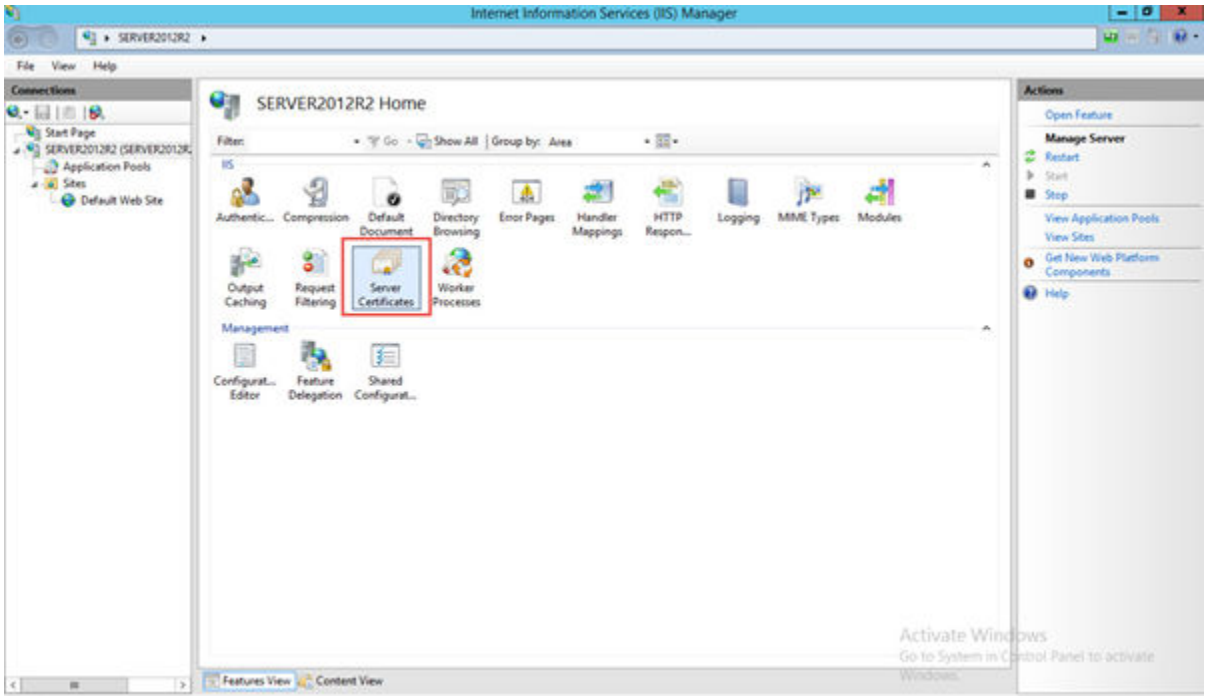
In the standard, multi-server deployment, you must generate a self-signed certificate for your Console server (or you can use an internally issued certificate).

The externally available URL of the Workspace ONE UEM server must be set up with a trusted SSL certificate. A wildcard or individual website certificate is required.

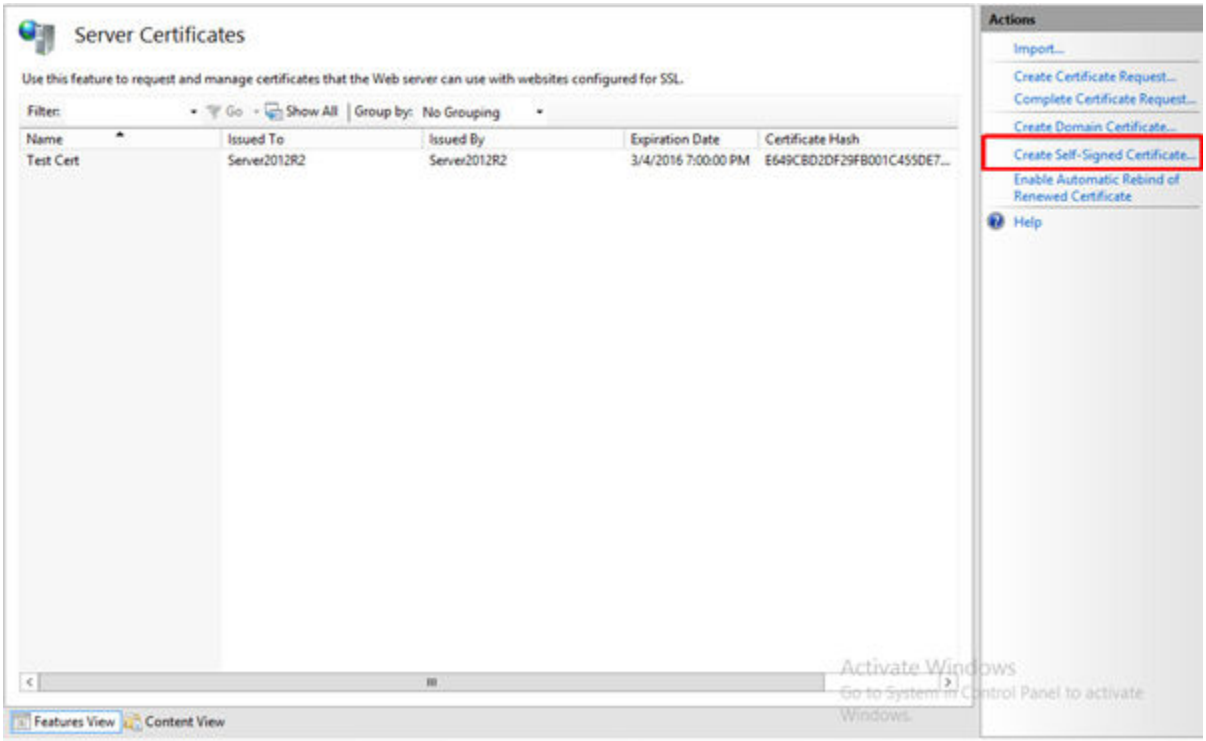
1 Open **Server Manager** and navigate to **Roles > Web Server (IIS)**.

2 Click the **Server Name**.

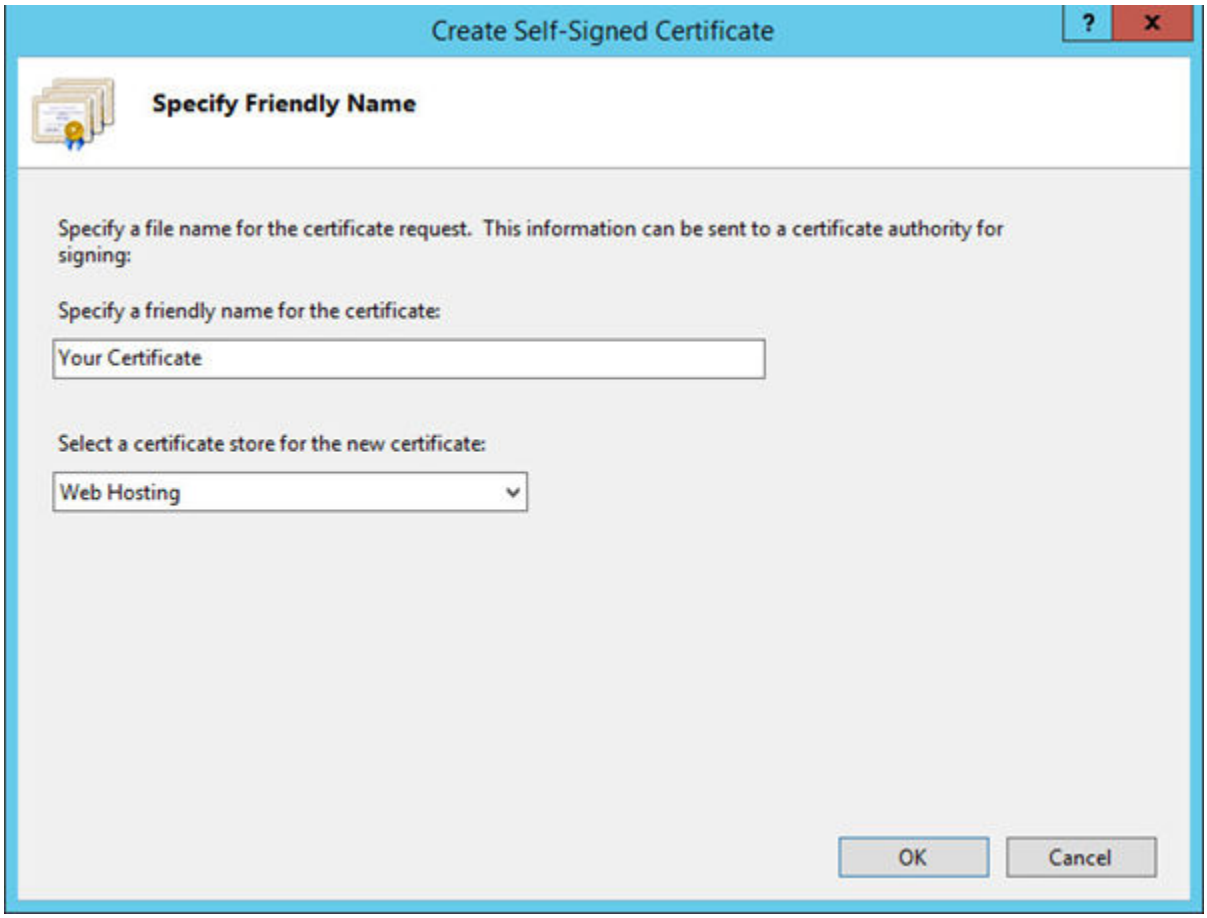
3 Select **Server Certificates**.



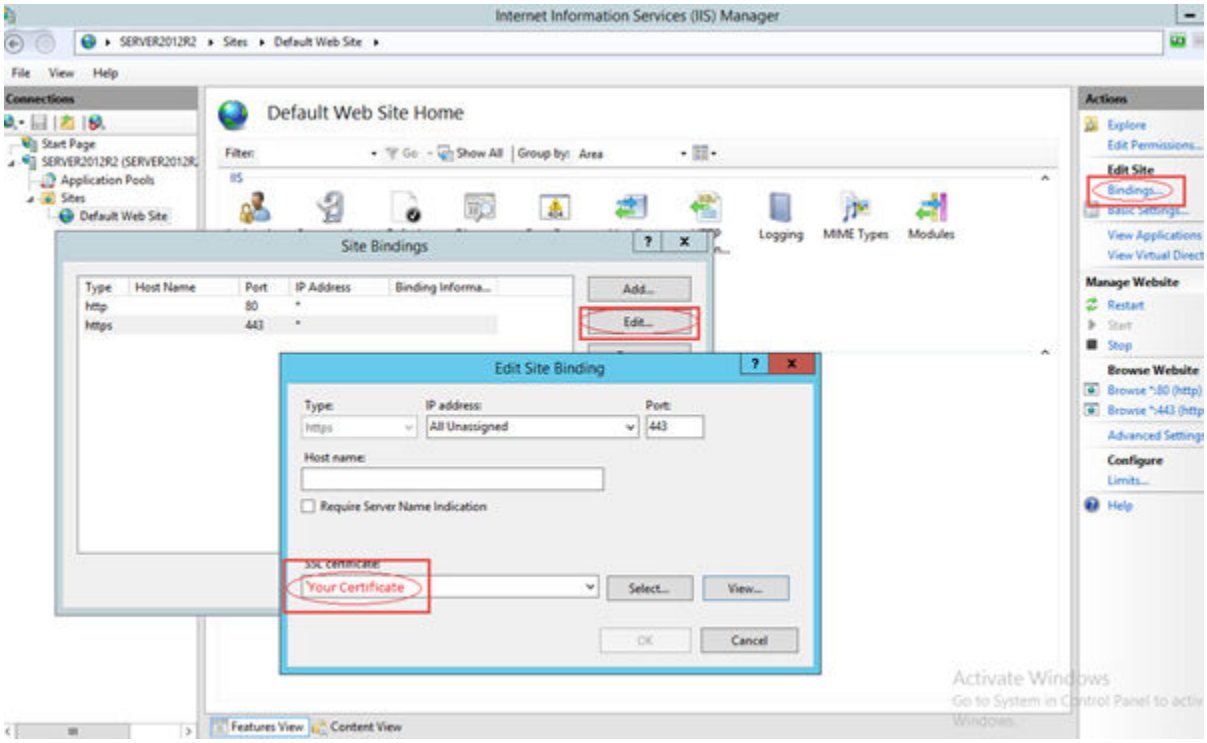
4 Under Actions, select **Create Self-Signed Certificate**.



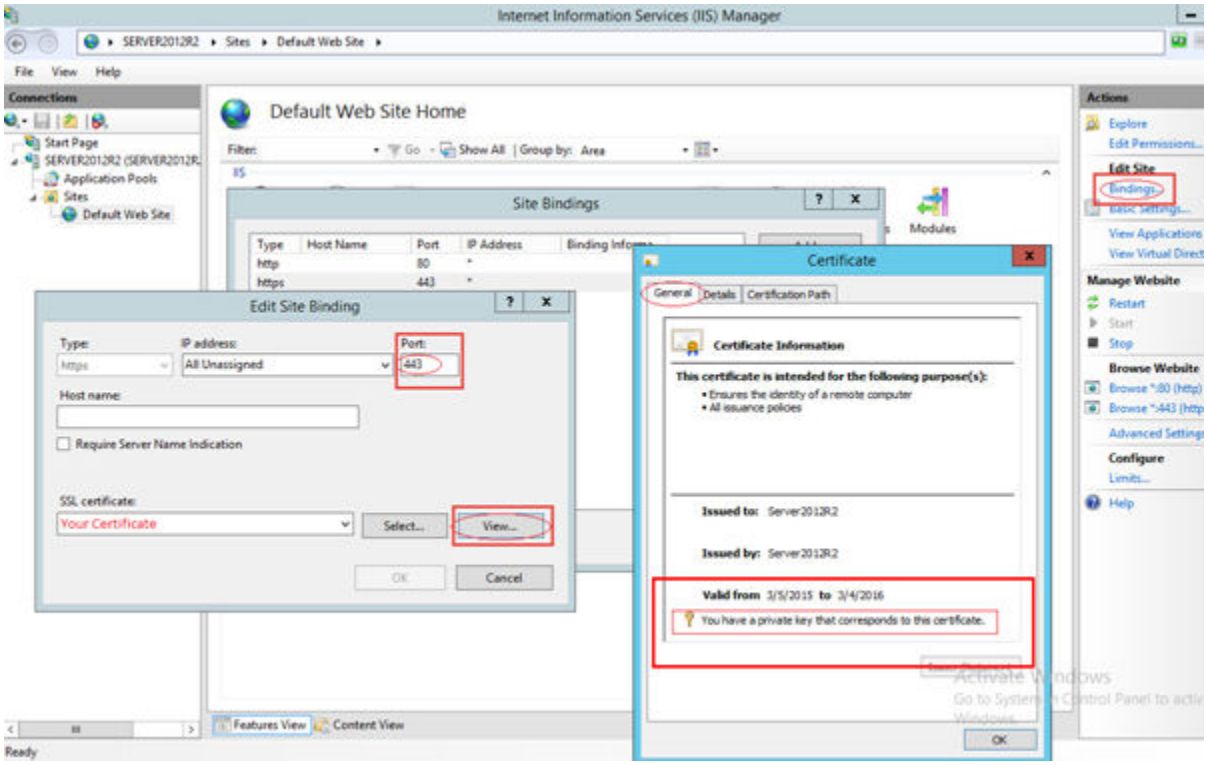
5 Enter the friendly name (FQDN) and select OK.



6 Next you can add a 443 binding to the Default website 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 Verify that you have a private key that corresponds to your certificate.



Configure Your External DNS Record and Certificates

Your external DNS must be setup with a trusted SSL certificatie by all device types to ensure poper communication with Workspace ONE UEM. Learn more about setting up the external DNS records and certificates.

The two main components of Workspace ONE UEM 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 Workspace ONE UEM (the Device Services server). This externally available URL must be set up with a trusted SSL certificate trusted by all device types. For Apple, you can see a list of root certificates 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 website certificate is required.

Important Ensure that these steps are performed on both the Workspace ONE UEM 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 **Workspace ONE UEM console** and **Device Services** Servers, open **MMC**:

   a Start > Run

   b Type `mmc`

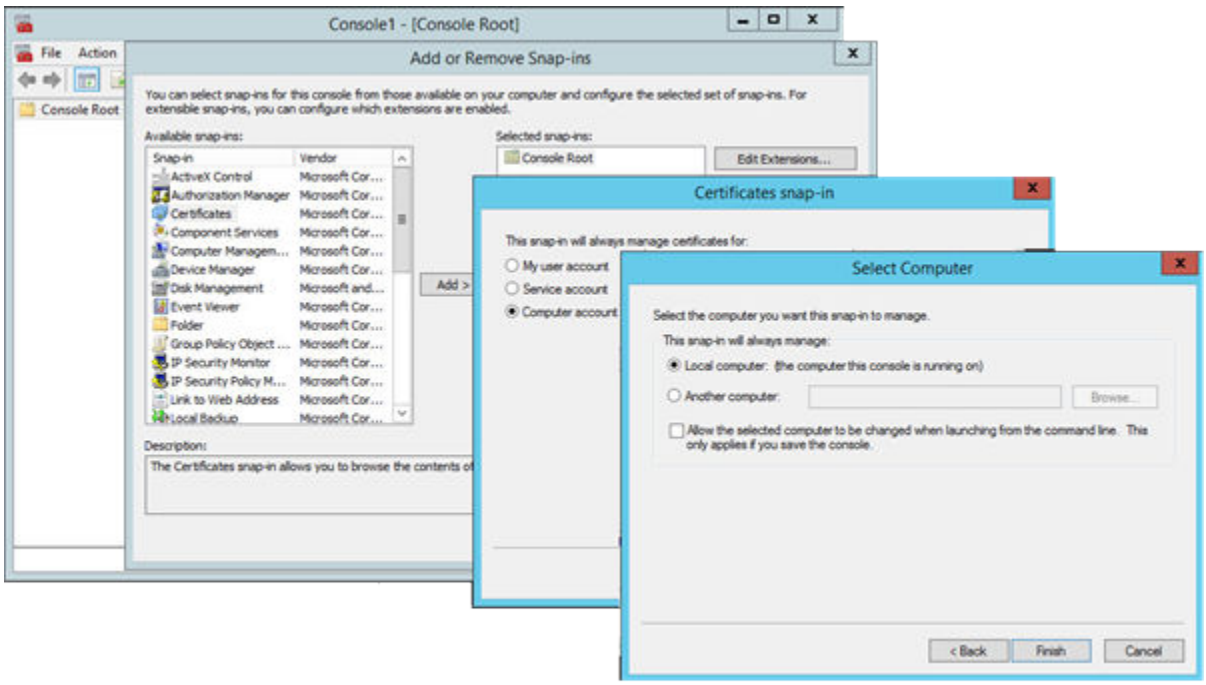
   c Select **OK**

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
   - Enable **Mark this key as Exportable**

     (This setting is optional and allows you to export the certificate from this server to use it on another server.)

   - Enable **Include all extended properties**

   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** and verify that the move was successful.

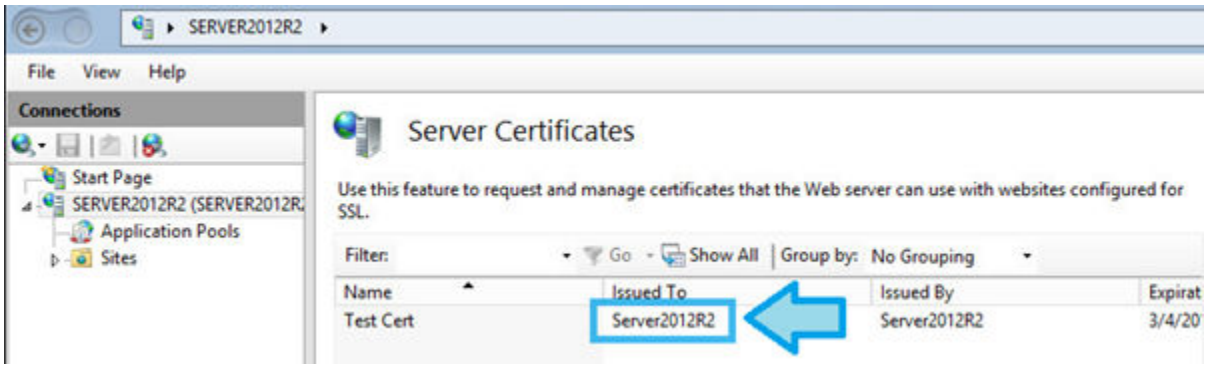
12 Navigate back to **Personal > Certificates**, and drag the **Intermediate CA Certificate** into the **Intermediate Certification Authorities** folder. Navigate to **Intermediate Certification Authorities > Certificates** and verify that the move was successful.

13 To close MMC, select **File > Exit** . Select **No** to save changes.

14 Open Server Manager, select **Roles** and expand: **Web Server (IIS) > Information Services (IIS) Manager**.

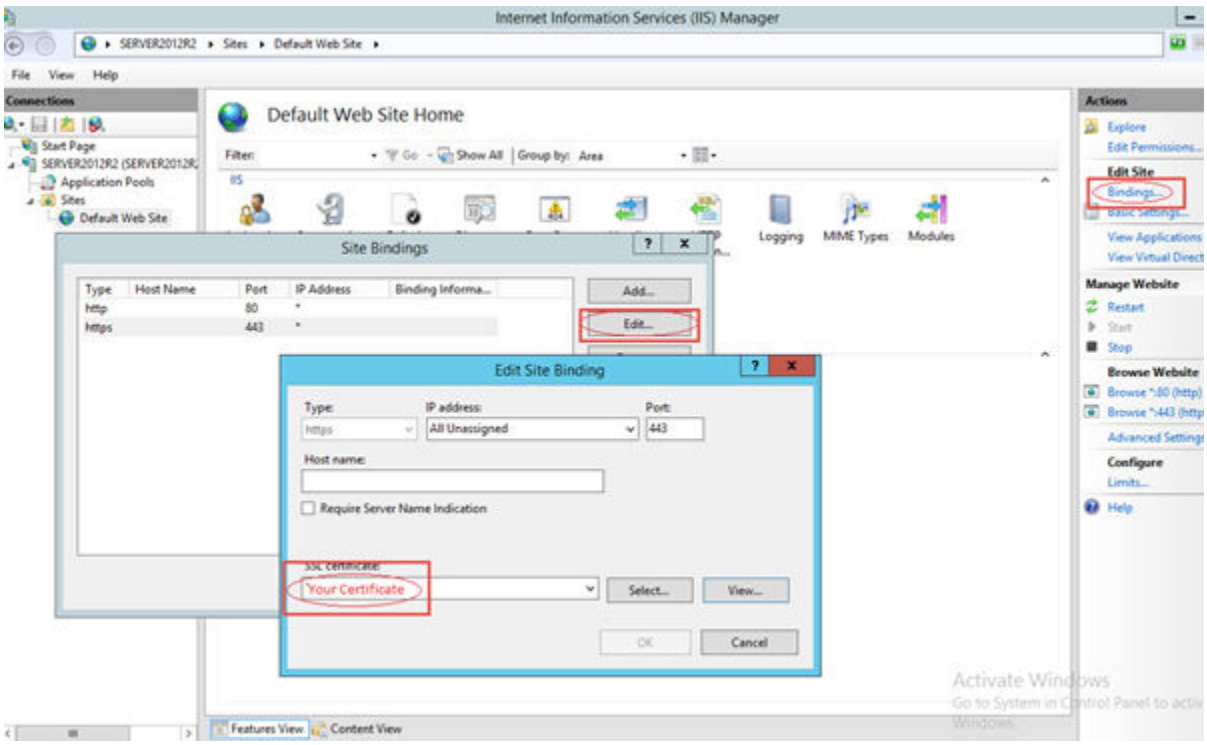
15 In the right pane, under **Connections**, select the server.

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 website in IIS. Your SSL certificate appears in the drop-down menu of available certificates.

17 Under **Connections**, expand **Sites** and select **Default Website**.



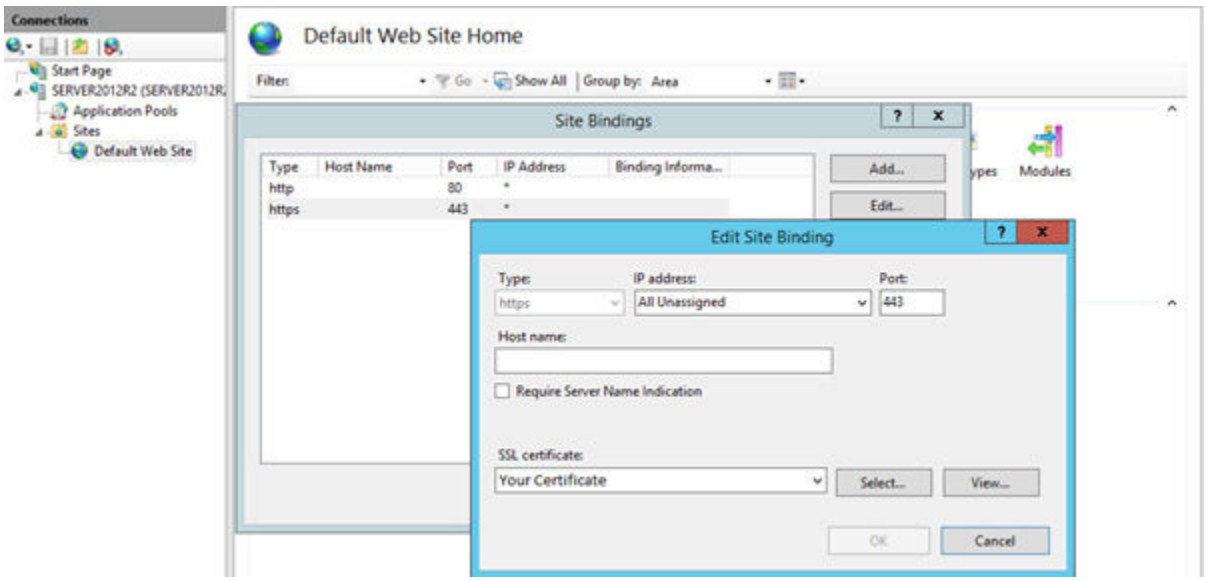
18 Under **Actions**, to the far right side, under **Edit Site**, select **Bindings** and select **Add**...

19 Configure the following settings:

- Type: https
- SSL certificate: Your certificate

20 Click **OK** and select to **Close**.

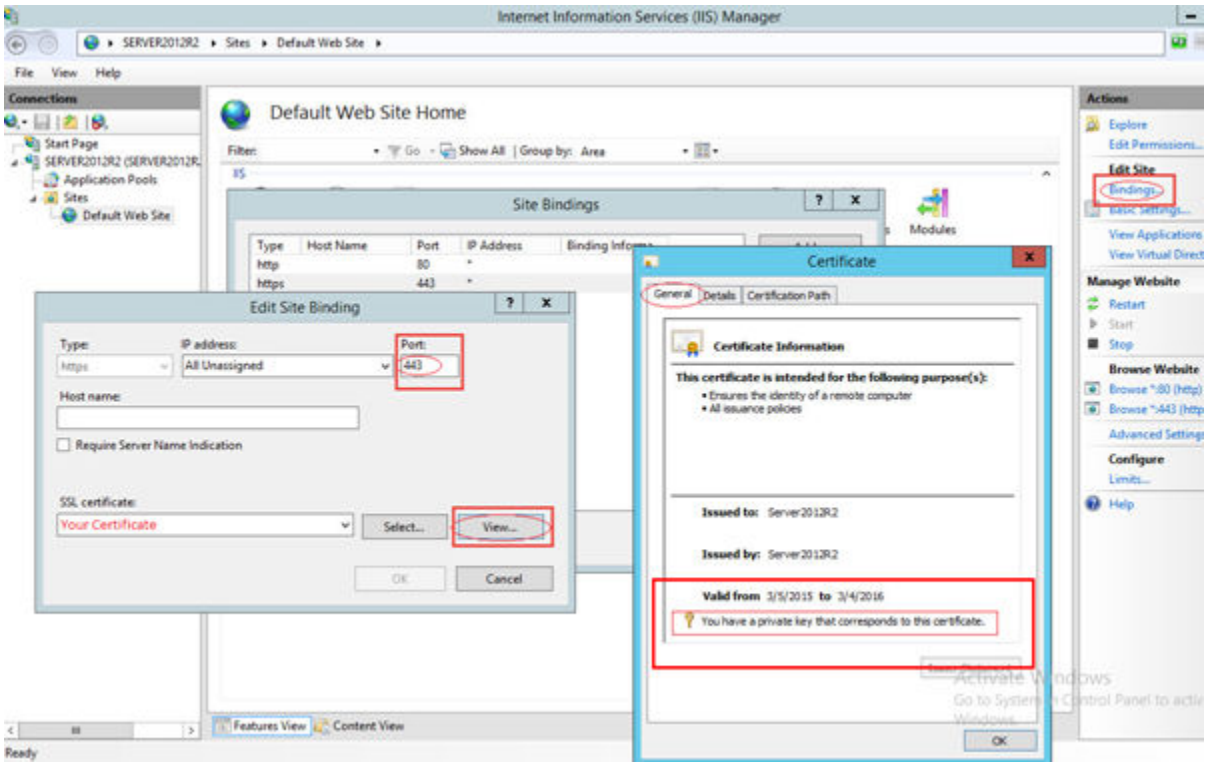
The IP address and Port are not altered. Do not populate the Hostname with an IP or a DNS entry, since it affects the functionality of the SSL binding. A slight delay occurs when the certificate is bound to the website.



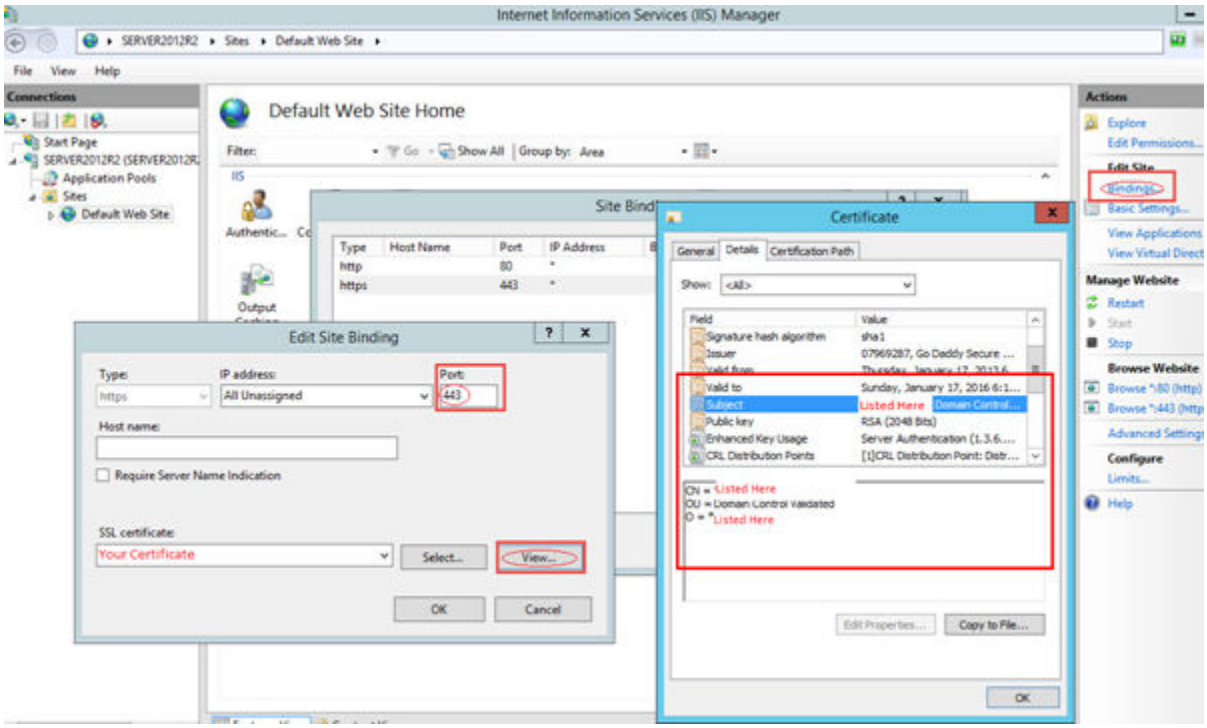
21 Click **OK** and select to **Close**.

22 Under **Actions/Browse Website**, verify **Browse *.443 (https)** is an available option.

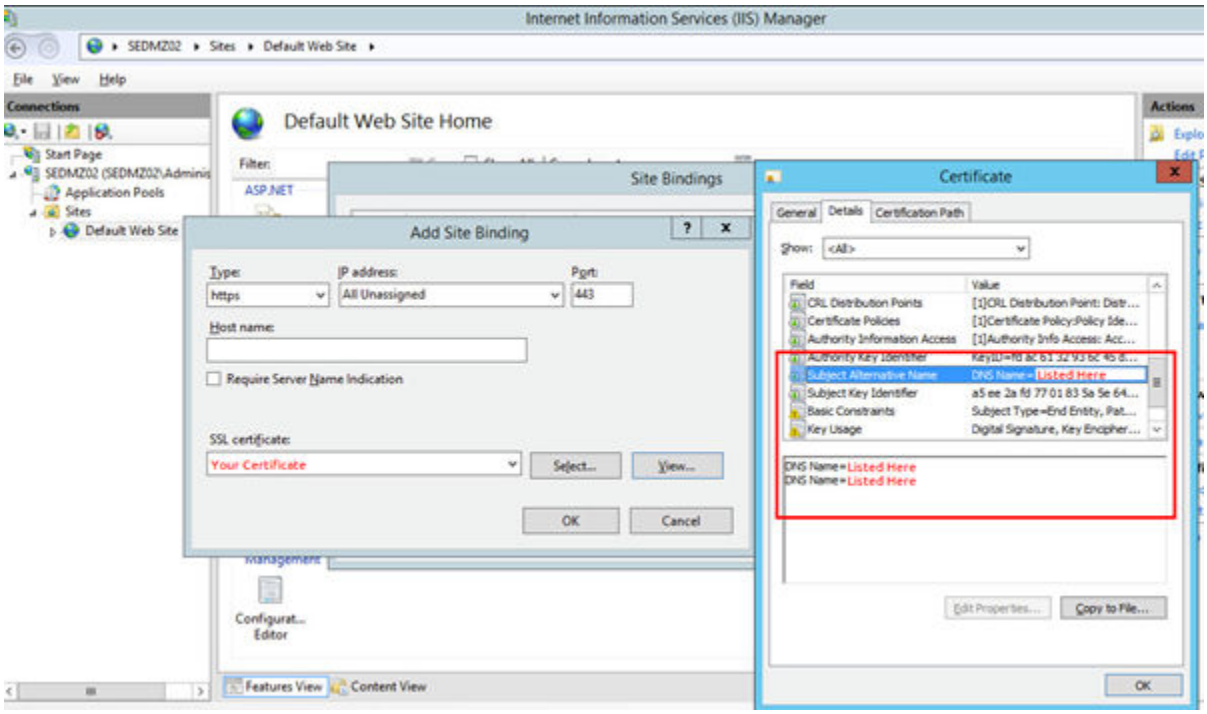
23 Also verify that you have a private key that corresponds to your certificate.



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://[yourUEMDomain].com). At this point, the IIS splash page displays.

Important If SSL is used for UEM console access, ensure that FQDN is enabled.

Stage Install Files

Once you have met the prerequisites for the database and the application server, configured your internal and external DNS, it is time to stage the Workspace ONE UEM install files. Learn more about how to stage files on your appropriate Console, Device Services, and SQL servers.

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 Workspace ONE UEM consultant as part of the deployment process.

2 Unzip the files on to the appropriate server.

3 Extract the contents.

Installing Workspace ONE UEM Database Servers

3

Configuring servers for your database is essential for a successful Workspace ONE UEM installation. Learn more about how to install the required database servers.

Installing Workspace ONE UEM on premises involves configuring servers for your database before you proceed with the installation.

Install the required database servers by completing the following:

1 Run the Workspace ONE UEM Database Setup Utility

2 Replicate SQL Agent Jobs on Additional Database Servers

3 Verify Proper Database Installation

This chapter includes the following topics:

Run the Workspace ONE UEM Database Setup Utility

After meeting prerequisites, run the Workspace ONE UEM database executable. Learn more about how to set up your Workspace ONE UEM database.

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

If you are planning to use Windows authentication, then log in as the account you want to use, or you must shift+right-click when you run the Workspace ONE UEM 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 Workspace ONE UEM database, the population of the tables during the database setup fails.

1. On the Workspace ONE UEM console or Database Server, open the **DB** folder, right-click the Workspace ONE UEM Database executable, and **Run as an administrator**. If you plan to use Windows authentication for SQL, then run the installer on the application server using this account.
2. The DB Installer automatically prompts you to install any essential missing components. When complete, select **Next**.
3. Accept the Workspace ONE UEM **EULA**, and then select **Next**.
4. Select a location to install the Workspace ONE UEM database files, and then select **Next**. The best practice is to install wherever the Workspace ONE UEM folder exists on your system. For example, C:\Workspace_ONE_UEM.

   The Database Server screen displays.
5. Click the **Browse** button next to the **Database** server text box and select your Workspace ONE UEM database from the list of options.

   Note If you do not have browsing functionality, enable SQL Browser Service. Otherwise, enter the SQL server hostname.

   - 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 **Workspace ONE UEM database catalog**.

     The Workspace ONE UEM database installation user (the account used to install the database only) has DB owner privileges on:

     - Workspace ONE UEM Database
     - SQLAgentUserRole
     - db_datareader on the msdb database
   - If you are integrating SQL AlwaysOn Availability Groups, select the **Using SQL AlwaysOn Availability Groups?** check box. This creates a SQL Agent job for an AlwaysOn Availability Group. This job checks the status of the server to see if it is currently the primary node or not. If the server is the primary node, it keeps the other jobs enabled, and if not, the job disables them. The new job is named 'AAG_EnableJobs.'

For more information about SQL AlwaysOn functionality, see Database Server Prerequisites.

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 has completed.

Replicate SQL Agent Jobs on Additional Database Servers

If you have SQL Server AlwaysOn with Workspace ONE UEM, the jobs must be available in all database servers that belong to the SQL Availability Group. Learn how to replicate your SQL jobs to ensure availability.

If you are deploying SQL Server AlwaysOn, SQL jobs are created under the SQL Server Agent during the Workspace ONE UEM Database deployment. These jobs must be available in all database servers which belong to the SQL Availability Group.

T-SQL scripts are generated from the jobs, which are then transferred to target databases and run against them to create the same exact jobs.

After deploying the Workspace ONE UEM Database against one of the servers, perform the following:

1 Using SSMS (SQL Server Management Studio), navigate to **SQL Server Agent > Jobs**. Locate the jobs for the target Workspace ONE UEM database which follow the naming convention `AirWatch_<DatabaseName> - <JobName>`, including the **AAG_EnableJobs** job.

2 For each Workspace ONE UEM job:

   a Right-click the job, then select **CREATE TO > New Query Editor Window**.

   b Save the T-SQL script to your local computer.

3 When you have saved all jobs as a script, perform the following steps:

   a Transfer all generated T-SQL scripts (for example, using a file share) to the database servers which belong to the SQL Availability group.

   b Open each T-SQL script in SSMS and run it.

   c Verify that all jobs are present by navigating to **SQL Server Agent > Jobs** (a refresh of the SSMS instance might be necessary).

4 If the SQL user account used for Workspace ONE UEM has minimal permissions, assign permission to run the **AAG_EnableJobs** job by running the following command in each database server that contains the **AAG_EnableJobs** job:

```
GRANT VIEW SERVER STATE TO [AccountName]
```

   [AccountName] is the SQL user account used to access the Workspace ONE UEM database.

5 If you use Workspace One Intelligence, the following jobs pertaining to Change Data Capture (CDC) must be copied to the secondary database as well:

   a 'cdc.{DBName}_capture'

   b 'cdc.{DBName}_cleanup' job

6 As an alternative you can create the 'cdc.{DBName}_capture' and 'cdc.{DBName}_cleanup' job with the following command on the secondary server:

   a EXEC sys.sp_cdc_add_job @job_type = N'capture';

   b EXEC sys.sp_cdc_add_job @job_type = N'cleanup';

7 Verify in the primary DB when CDC is activated (i.e. 'cdc.{DBName}_capture' job is running) , ADP_Export job is deactivated.

If a target database fails to join the SQL Availability Group, see https://technet.microsoft.com/en-us/library/ms178029(v=sql.120).aspx for troubleshooting steps.

Verify Proper Database Installation

After you set up and install the Workspace ONE UEM database, you can verify that the database installed successfully. By verifying the installation, you can ensure that accurate version was installed.

Procedure:

1 In SQL Server Management Studio, select your Workspace ONE UEM instance.

2 Enter the following: `SELECT * FROM dbo.DatabaseVersion`.

3 Select **Execute**.

4 In Results, verify that the correct version shows. For a 9.4 or later GA release, you see **MajorVersion** 9, **MinorVersion** 4, and **Description** Workspace ONE UEM 9.4 GA.

Installing a Workspace ONE UEM Application Server

4

After verifying the database installation, begin installing the Workspace ONE UEM Application Servers. Learn more about the requirements and how to install your application servers.

Installing Workspace ONE UEM on premises involves configuring your application servers before you proceed with the installation.

See the following to install the required application servers:

- Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services)
- (Optional) Run the Installer on Additional Application Servers
- Installation Tokens for Application Servers

This chapter includes the following topics:

Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services)

Run the Workspace ONE UEM executable file on your application servers to install the Workspace ONE UEM console and the Device Services features. Learn about how to run and install the Workspace ONE UEM installer on each application server.

When preparing to install VMware Workspace ONE UEM, take note of the following regarding the installer path,

- The Workspace ONE UEM installer concretes the File Path in the Workspace ONE UEM Console during on a fresh install.
- If you run the installer again during the upgrade and change the install path, or uninstall and reinstall to a new install path, then manually update the File Path in the console.
- The File Path updates based on the install path on the first box installed. Install all boxes (CS/DS) on the same drive.

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 **XXXX Application** folder and run the **Workspace ONE UEM Application XXXX Full Install.exe.**

   Execute the Workspace ONE UEM installer from an account with administrator privileges. To run the installer if you do not have administrative privileges, right-click and select **Run as Administrator**.

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. Reboot when prompted. The Workspace ONE UEM Installer automatically resumes after the prerequisites install.

3 Click **Next** once the Workspace ONE UEM 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 Workspace ONE UEM Setup Configurations from or to any other identically configured Workspace ONE UEM servers.

   - Disregard this setting if you are deploying Workspace ONE UEM 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 servers and increase install speed or import settings that you have previously exported. For more information, see (Optional) Run the Installer on Additional Application Servers.

6 Select the Workspace ONE UEM features that you want to install on the specific server.

   - In a standard, multi-server environment, enable only the Workspace ONE UEM console features or the Workspace ONE UEM Device Services features for the respective server type.

7 The Workspace ONE UEM Prerequisites screen displays to ensure that you meet the requirements. The installer checks for modules that are needed for a successful deployment of Workspace ONE UEM. You are prompted to install any missing components. Select **Next**.

8 To install Workspace ONE UEM, select the directory. Then, select **Next**.

9 Enter information about the Workspace ONE UEM database.

   - Select **Browse** next to the **Database server** text box and select your Workspace ONE UEM database from the list of options. If you are using a custom port, do not select Browse. Use the following syntax: **DBHostName,<customPortNumber > ,**. To select the Database server, select **Browse**
     - Example: db.acme.com,8043

- Select one of the following authentication methods:
  - To connect to the database, select **Windows Authentication** mode. 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 Workspace ONE UEM related services. This account must be an account that has Workspace ONE UEM Database access.
  - To connect to the database, choose **SQL Server Authentication** mode. You are prompted to enter the user name and password.
- Enter the name of the Workspace ONE UEM 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 **UEM 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 Workspace ONE UEM 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.

Use HTTPS for the Console and Device Services servers.

If your deployment uses legacy .NET SEG, 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 Workspace ONE UEM.
- Select your **Environment Type** from the drop-down menu.
  - Production - Default
  - Development
  - QE
- Enter your **Installation Token** from myAirWatch. See Installation Tokens for Application Servers.

12 When prompted, selections for participating in the **VMware Customer Experience Improvement Program**.

Note The **VMware Customer Experience Improvement Program** (CEIP) provides information that VMware uses to improve its products and services, fix problems, and advise how best to deploy and use VMware products. This program is only available to on-premises Workspace ONE UEM deployments. The CEIP prompt appears when you install or upgrade Workspace ONE UEM. You must make a selection. You can change your selection any time afterwards from the Workspace ONE UEM console.

13 Select the Workspace ONE UEM website. By default, the 'Default Website' is selected.

14 If you choose to install the **VMware 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 Workspace ONE UEM account services representative before using another port.

- Best practice is to use a publicly trusted SSL certificate. Select the **Use custom SSL Certificate instead of built-in Workspace ONE UEM 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.

  To use a Workspace ONE UEM certificate without configuration automatically, ensure that **Use custom SSL Certificate instead of built-in Workspace ONE UEM certificate?** is deactivated.

- 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 nodes, 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 or Windows Server 2019 Desktop Experience, a dialog box prompts you to deactivate HTTP2 support. Deactivate support and continue.

17 When prompted, choose participation in the **VMware Customer Experience Improvement Program**.

Note The **VMware Customer Experience Improvement Program** (CEIP) provides information that VMware uses to improve its products and services, fix problems, and advise how best to deploy and use VMware products. This program is only available to on-premises Workspace ONE UEM deployments. The CEIP prompt appears when you install or upgrade Workspace ONE UEM. You must make a selection. You can change your selection any time afterwards from theWorkspace ONE UEM console.

18 Click **Finish** once all the files are copied to the server to complete the Workspace ONE UEM installation. View the installation log file by selecting a check box before Finish is selected.

19 Close Internet Explorer and run your default browser.

For the Console: To verify that the Workspace ONE UEM console renders successfully, type **https://localhost/airwatch**.

For Device Services: To verify that the device Group ID prompt shows, type **https://localhost/devicemanagement/enrollment**.

Since the SSL certificate is not bound to the local host session, an error displays. To view the site, select **Proceed**. The first time the website displays, it might take up to minute to resolve.

20 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.

If you are enabling SQL AlwaysOn, you must replicate the SQL Agent Jobs on the any additional database servers. For more information, see Replicate SQL Agent Jobs on Additional Database Servers.

Installation Tokens for Application Servers

You can determine the Workspace ONE UEM installation token you need based on your server configuration. Learn how to determine your Workspace ONE UEM token.

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

To retrieve the token automatically, your Workspace ONE UEM application server must have outbound Internet access to the Workspace ONE UEM signing service.

If your Workspace ONE UEM application server does not have outbound Internet access to the signing service, as defined under Network Requirements, then the Authentication Token field does not display on the Global Enterprise Manager, and you must generate the token manually.

Generate Installation Token from myWorkspaceONE (Automatic)

Generate and upload a token to install Workspace ONE UEM automatically on your server.

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

1 After Workspace ONE UEM installs, go to the Global Enterprise Manager screen and enter your **Company Name** and **Environment Type**.

2 Select the myWorkspaceONE link. 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 the information below for generating an installation token manually.

3 Log in to myWorkspaceONE and navigate to **myWorkspaceONE > 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 Run the Workspace ONE UEM Installer on Each Application Server (Console and Device Services) to complete the installation.

Generate Installation Token from myWorkspaceONE (Manual)

If your Workspace ONE UEM application server does not have outbound Internet access to the signing service, as defined under Network Requirements, then the Authentication Token field does not display on the Global Enterprise Manager. 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 EXE file opens a screen to guide you through the manual installation method.

1 Select **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.

3 Select the **Get File** button and 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 **Hamburger menu > myAirWatch > My Company**.

5 Select **Certificate Signing Portal**.

6 Select **Authorize Install**.

7 Select **Upload Your File**.

8 Using the link, 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.

Note The Next button is enabled and you may proceed with installation. If you see theInstallation Failed screen at any point during installation, select Back to try again, or contact Workspace ONE Support for assistance.

(Optional) Run the Installer on Additional Application Servers

If you have more than one application server, you must run the installer on all additional application servers. Learn more about how to run the installer on all your additional Workspace ONE UEM Application Servers.

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

1 Log on to one of your Device Services servers and start the **Workspace ONE UEM Installer**.

2 Progress 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 Application servers. If you only have one Application server, then choose **Continue Setup without exporting/importing config file** .

3 Next, select the Workspace ONE UEM features that you want to install on the specific server.

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.workspaceone.com/articles/115001666028.

4 Enter the file path to the Workspace ONE UEM Directory once again, and choose **Next**.

5 Enter the information about the Workspace ONE UEM 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 Workspace ONE UEM website.

8 Select **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. Progress through the Installer without entering any configuration details.

Installing Workspace ONE UEM Reports

5

You can enable report configuration, subscription, and data driven email for your Workspace ONE UEM by installing Workspace ONE UEM Reports. Learn more about how to isntall Reports and where to find information on custom reports.

This section walks you through the process of installing Workspace ONE UEM Reports to enable report configuration, report subscription, and data driven email for your Workspace ONE UEM deployment.

For more information on Custom Reports, see the **Report Analytics Guide**, available on docs.vmware.com.

Reports Options

There are two options for configuring reporting.

- Option 1: Custom Reports

  Custom reports allow you to create reports on your Workspace ONE UEM 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 Workspace ONE UEM 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.

- Option 2: New Reports

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

This chapter includes the following topics:

Reports Storage

You can optimize the storage of your Workspace ONE UEM reports through reports storage. while the reports storage feature is separate from file storage, if you curently utilize file storage, you do not need to enable reports storage.

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 Workspace ONE UEM database when using reports. Reports storage applies to reports only, helping increase overall reports performance, and reducing the burden on your Workspace ONE UEM 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 and see an improvement in reports performance in Workspace ONE UEM, 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 Workspace ONE UEM 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 UEM 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, Workspace ONE UEM 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 Workspace ONE UEM 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 can 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 improve the performance of reports run in Workspace ONE UEM.

You must be in an on-premises environment.

1 Navigate to **Groups & Settings > All Settings > Installation > Reports**.

2 Set **Report Storage Enabled** to **Enabled**.

3 Configure the report storage settings.

Settings	Description
Report Storage File Path	Enter the path reports are to be stored 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	When enabled, files are cached locally on the DS server when accessed for the first time. Subsequent requests are served using the file cached on the DS server instead of streaming from the file storage location. If you enable caching, consider accommodating for the amount of space needed on the server.
Report Storage Impersonation Enabled	Enabling this option adds a service account with the correct permissions.
Report Storage Impersonation user name	Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.
Report Storage Impersonation Password	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.

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

Reports Storage Requirements

To deploy the reports storage solution and see an improvement in reports performance in Workspace ONE UEM, 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 Workspace ONE UEM 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 UEM 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, Workspace ONE UEM 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 Workspace ONE UEM 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 can 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 improve the performance of reports run in Workspace ONE UEM powered by AirWatch.

Prerequisites

You must be in an on-premises environment. For more information, see Reports Storage Requirements.

Procedure

1 Navigate to **Groups & Settings > All Settings > Installation > Reports**.

2 Set **Report Storage Enabled** to **Enabled**.

3 Configure the report storage settings.

Settings	Description
Report Storage File Path	Enter the path reports are to be stored 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	When enabled, files are cached locally on the DS server when accessed for the first time. Subsequent requests are served using the file cached on the DS server instead of streaming from the file storage location. If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see Reports Storage Requirements.
Report Storage Impersonation Enabled	Enabling this option adds a service account with the correct permissions.
Report Storage Impersonation user name	Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.
Report Storage Impersonation Password	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.

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

Verifying the Workspace ONE UEM Installation

6

After you install and configure Workspace ONE UEM, you can verify that the installation was successful. By verifying the installation, you can ensure that all components are functioning correctly.

Verify the Correct Site URL Population

During the Workspace ONE UEM installation, your URLs populate on a system settings page. Learn more about how to verify your URLs have populated correctly.

The Workspace ONE UEM 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 Workspace ONE UEM version by selecting AboutWorkspace ONE UEM.

3 Log in to the Workspace ONE UEM 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.

   a 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 Workspace ONE UEM console URL to the Workspace ONE UEM 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`.

   Workspace ONE UEM recommends a standalone API server, for deployments of up to 100,000 devices and higher, in which case, change the Site URL to match your dedicated API server URL.

Verify Connectivity

After the installation has completed, verify connectivity between your various endpoints to ensure they are operational. Learn more about how to verify connectivity with Workspace ONE UEM endpoints.

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 Workspace ONE UEM 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 Workspace ONE UEM 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 Workspace ONE UEM Services Are Started

After installing Workspace ONE UEM, start each service for the installed components to ensure they are running. Learn more about how to verify your Workspace ONE UEM service have all restarted upon complettion of the installation.

The Workspace ONE UEM installer properly configures the associated Windows services, and the start type and recovery options for each service should not be modified. If services are not automatically restarted, use Windows Services Manager to reset Window Services to Automatically Delayed Start.After a typical installation, open the Windows Services Manager to verify that the installed component services are running.

1 Open the **Services 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

In addition to verifying other services are up and running, GEM Inventory Service has its own validation steps to make sure the service is operational. Learn how to validate GEM functionality with Workspace ONE UEM.

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 Workspace ONE UEM Services at the top of the services list in alphabetical order. Each of these services start with AirWatch in the name. For the **AirWatch GEM Inventory Service**, right-click and select **Restart**.

5 To see if a log regenerates, select the C:\AirWatch\Logs\Services\ folder. If a log regenerates with errors, contact Workspace ONE UEM Support for further assistance.

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

Deactivate Services on Multiple Console Servers

Some of the Workspace ONE UEM services can only be active on one primary console. Learn how to deactivate applicable services on servers.

To ensure maximum performance, certain Workspace ONE UEM services must only be active on one primary console server. If you deploy these services, deactivate them on non-primary servers after you have fully installed Workspace ONE UEM.

Workspace ONE UEM Services that must only be active on one server are:

- AirWatch Device Scheduler
- Directory Sync
- Content Delivery Service
- AirWatch GEM Inventory Service

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

Deactivate these services on any console servers other than the primary server:

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 The active Workspace ONE UEM Services at the top of the services appear in alphabetical order. For the **AirWatch Device Scheduler**, **Directory Sync**, **Content Delivery Service**, and **AirWatch GEM Inventory Service**, right-click and select **Stop**.

4 After the services have stopped, change the Startup Type for each service to **Manual** or **Disabled**. Changing the Startup Type prevents the service from restarting after any reboot.

5 When you upgrade your Workspace ONE UEM console, the Content Delivery Service automatically restarts. To maintain expected performance, manually deactivate the applicable services again on all extra servers.

Workspace ONE UEM Post-Installation Steps

7

After the installation is completed and verified, you can test device connections, and run the Workspace ONE UEM Wizard before beginning the post-installation configuration.

This guide does not cover post-install configuration, but does include two post-installation steps, which cover some of the essential procedures to get you started.

Apple Device Connection Testing

Now that you have installed Workspace ONE UEM, you can start enrolling devices. Having the physical device, such as an iPad or iPhone, is required for testing. You may also need to create a corporate Apple ID. Learn more about how to test device connection and Apple ID creation.

Create a Company-Dedicated 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, Workspace ONE UEM suggests that an Apple ID is created with an email address multiple user have access to. This way, your company does not have to rely on one person to renew the certificate.

If you need to create an Apple ID, click the following link and select Create an Apple ID: https://appleid.apple.com

Run the Workspace ONE Getting Started Wizard

Once the Workspace ONE UEM installation is complete, you can run the Workspace ONE UEM wizard to begin the configuration settings of Workspace ONE.

Workspace ONE Access is required for Workspace ONE deployments and must be configured to communicate with your Workspace ONE UEM console. This process is largely automated through the Workspace ONE UEM Getting Started experience in the Workspace ONE UEM console. Consider using the Getting Started wizard before attempting 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 enabling Workspace ONE Access integration, the Workspace ONE application, and core Workspace ONE features, see the Workspace ONE Quick Configuration Guide, available at docs.vmware.com.