Microsoft Certificate Authorities

Integrating Certificate Authorities for Microsoft Resources

VMware Workspace ONE UEM 1903

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

1 Microsoft Certificate Authorities 4

2 Workspace ONE UEM Integration with Microsoft NDES via SCEP 5

System Requirements 5

High Level Design 6

Install, Set Up, Configure Certificate 8

Tips and Troubleshooting 15

3 Workspace ONE UEM Integration with Microsoft ADCS via DCOM 16

System Requirements 16

High Level Design 17

Install, Set Up, Configure Certificate 19

Microsoft Certificate Authorities 1

Set up Microsoft certificate authorities for your enrolled devices within your deployment of Workspace ONE UEM.

This documentation explains how to install and set up Microsoft certificate authorities (CA) for direct integration with Workspace ONE UEM. This setup allows Workspace ONE UEM to take advantage of digital certificates by automating the issuing, renewal, and revocation process to mobile devices.

Workspace ONE UEM is set up to integrate with two Microsoft certificate authorities.

- Chapter 3 Workspace ONE UEM Integration with Microsoft ADCS via DCOM
- Chapter 2 Workspace ONE UEM Integration with Microsoft NDES via SCEP

Workspace ONE UEM Integration with Microsoft NDES via SCEP

2

This documentation explains the installation and setup of the Microsoft certificate authority (CA) for direct integration with Workspace ONE UEM over the NDES/SCEP/MSCEP protocol.

Since there is not much difference between NDES, SCEP, and MSCEP (mostly dependent on which version of MS Server you deploy), this documentation may be used for all three protocols.

This chapter includes the following topics:

- System Requirements
- High Level Design
- Install, Set Up, Configure Certificate
- Tips and Troubleshooting

System Requirements

The following requirements must be met prior to proceeding with the protocol configuration.

- Compatibility with the MS server running the protocol:
  - NDES is only available in the Enterprise version of Microsoft Server 2008, 2008 R2, and 2012 or 2016 Standard or Enterprise.
  - SCEP or MSCEP is available in versions older than Microsoft Server 2008.
- A Certificate Authority (CA) installed, configured, and made available to the NDES/SCEP/MSCEP server.
  - The CA and NDES/SCEP/MSCEP can be installed on the same server or on different servers. If NDES/SCEP/MSCEP is to be installed on the same server as the CA, the installation of the CA must be completed first and the server rebooted prior to installing NDES/SCEP/MSCEP.
- The following certificate templates are needed during NDES/SCEP/MSCEP setup and service certificate renewal:
  - Exchange Enrollment Agent (Offline request)
  - CEP Encryption

  Note **Note:** It is possible for all of the following accounts to be the same account. However, there are security concerns if a single account is used.

Connection Requirements

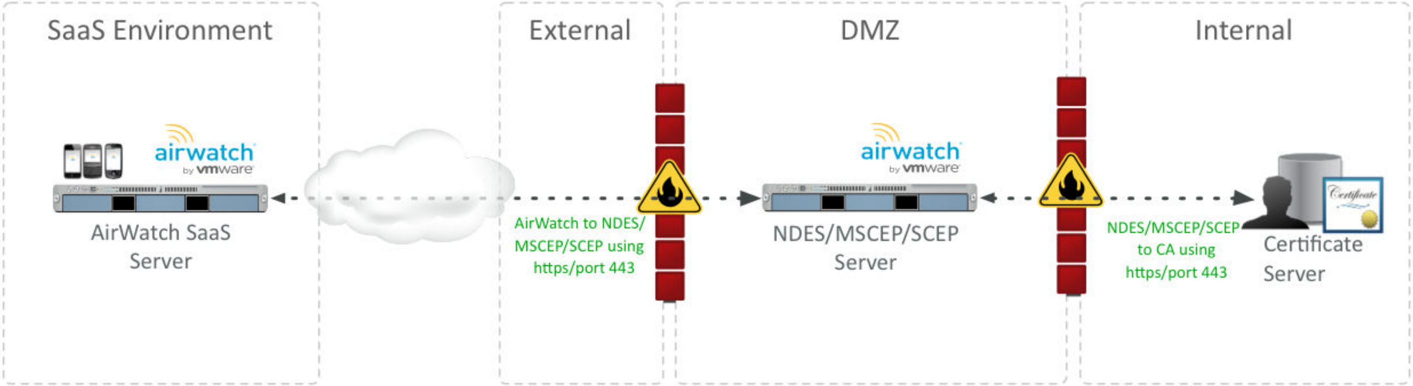
- SCEP endpoint must be accessible from the device in order for certificate enrollment to complete.
    - The exception to this requirement is when you utilize the **Enable Proxy** option in the **Certificate Authority - Add/Edit** page for non-generic SCEP protocol usage.
- An **Admin Account** must exist in the domain. This account is used to install the NDES/SCEP/MSCEP role service and must meet the following requirements.
    - Member of the Local Administrators group (Standalone Installation)
    - Member of the Domain Admins group (Enterprise)
    - ‘Enroll’ permissions on NDES/SCEP/MSCEP service certificate templates (Enterprise). See Step 1: Install the Microsoft CA Role below for information on setting permissions.
- A **Service Account** must exist. It is used by the NDES/SCEP/MSCEP application pool and must meet the following requirements.
    - Member of the local IIS_USRS group. Role installation will fail if this is not present.
    - ‘Request’ permission on the configured CA. See Step 2: Set Permissions for the NDES/SCEP/MSCEP Admin Account below for information on setting permissions.
    - ‘Read’ and ‘Enroll’ permissions on configured device certificate templates. See Step 2: Set Permissions for the NDES/SCEP/MSCEP Admin Account below for information on setting permissions.
    - A Service Principal Name (SPN) must be added by using: **SetSpn –a HTTP/<ComputerName > <AccountName >**
- **<ComputerName >** is the name of the computer where NDES/SCEP/MSCEP is installed.
- **<AccountName >** is the computer account name when NetworkService is used, or the domain user account when a custom application pool identity is configured.
- The **Device Administrator** account used to request password challenges from NDES/SCEP/MSCEP must meet the following requirements.
    - ‘Enroll’ permissions on all configured device certificate templates (Enterprise). See Step 2: Set Permissions for the NDES/SCEP/MSCEP Admin Account below for information on setting permissions.
    - Member of the Local Administrator group (standalone).

High Level Design

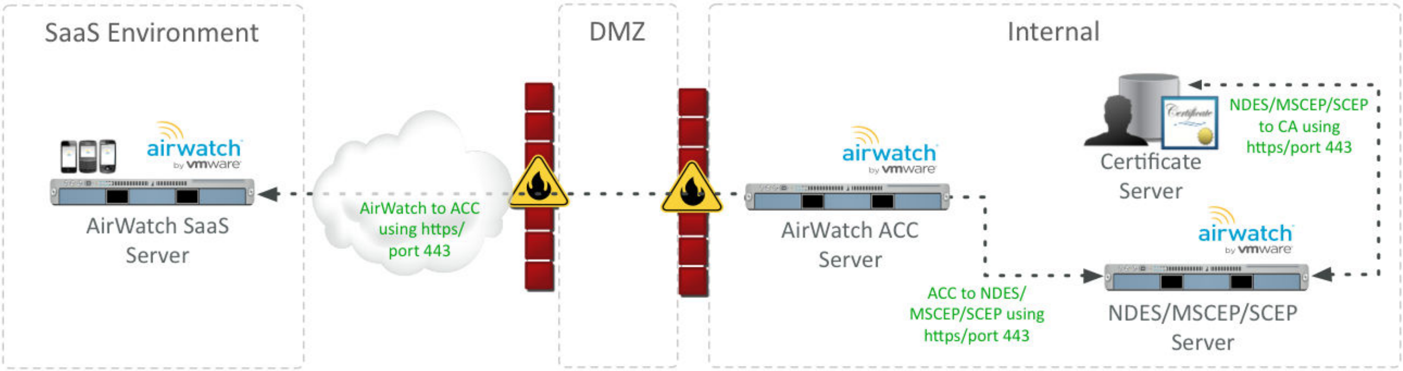
In order for Workspace ONE UEM to use a certificate in a profile, which is used to authenticate a user, an enterprise certificate authority does not need to be set up in the same domain as the Workspace ONE UEM server.

There are several methods for Workspace ONE UEM to retrieve a certificate from the certificate authority. Each method requires the basic installation and configuration described in this documentation. Sample CA Configurations are shown below in the Workspace ONE UEM SaaS environment. Configurations will differ in on-premises environments.

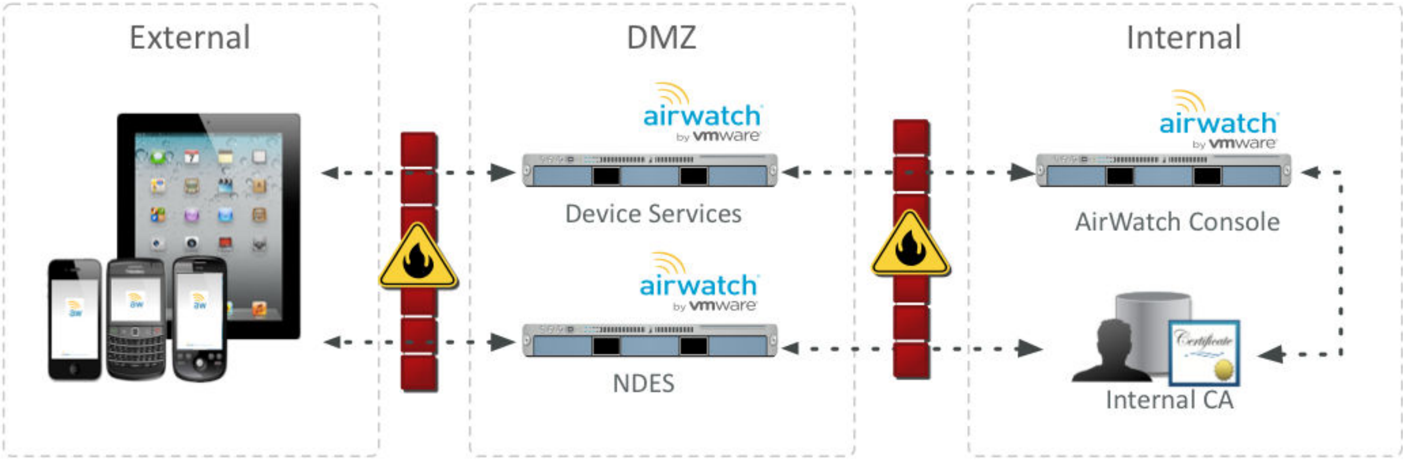
Scenario #1: Workspace ONE UEM to NDES/SCEP/MSCEP and then to Certificate Authority



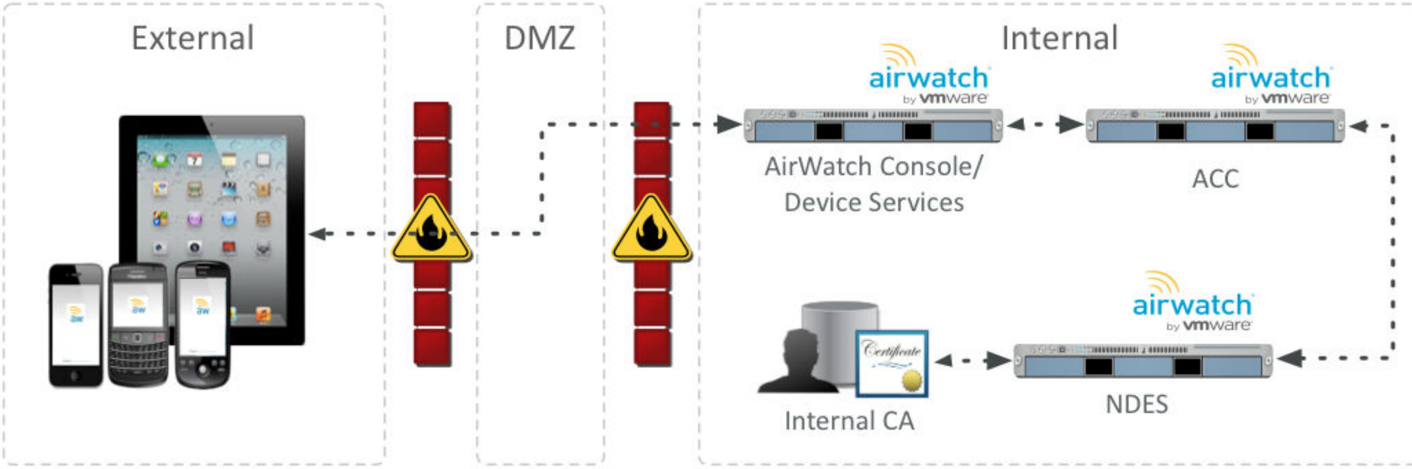
Scenario #2: Workspace ONE UEM to VMware Enterprise Systems Connector, then to NDES/SCEP/MSCEP, and then to Certificate Authority



Scenario #3: On-Premises DS and NDES in the DMZ with Internal AW Console and CA



Scenario #4: On-Premises with All Servers Internal and SCEP Proxy



Install, Set Up, Configure Certificate

This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console.

Take the following steps and procedures to integrate the certificate.

Step 1: Install the Microsoft CA Role

Add the ADCS Role

1 Click the **Server Manager** icon next to the **Start** button to open the **Server Manager** window.

2. Click **Roles** in the left pane.
3. Click **Add Role** in the right pane. An **Add Roles Wizard** window displays.
4. Under **Server Roles**, select the **Active Directory Certificate Services** checkbox.
5. Click **Next**.
6. Select the **Certification Authority** checkbox and then select **Next**.
7. Select **Enterprise** and then select **Next**.
8. Select **Root CA** and then select **Next**.

Define CA Private Key Settings

1. Select **Create a new private key** and then select **Next**.
2. Select your preferred **Key character length** (for example 4096).
3. Select your preferred algorithm (for example SHA256) from the **Select the hash algorithm for signing certificates issued by the CA** and then select **Next**.
4. Click **Common name for this CA** and enter the name of the CA or use the default CA displayed and then select **Next**.

   Make note of the name of the CA server. You will need to enter this information in Workspace ONE UEM when setting up access to the CA.
5. Select the desired length of time under **Set the validity period for the certificate generated for this CA** and then select **Next**.

   The length of time you select is the validity period for the CA, not the certificate. However, when the validity for the CA expires, so does the certificate.

Configure the ADCS Certificate Database

1. Click **Next** to accept the default information in the **Configure Certificate Database** screen.
2. Click **Next** to accept the **Confirm Installation Selections** screen.
3. Click **Install**. The installation begins. After the installation completes, the **Installation Results** window displays.
4. Click **Close**.

Step 2: Set Permissions for the NDES/SCEP/MSCEP Admin Account

Set the ‘Enroll’ permission on the CA for the NDES/SCEP/MSCEP Admin Account.

1. Launch the **Certification Authority Console** from the **Administrative Tools** in Windows.
2. Right-click the server name and select **Properties**.
3. Select the **Security** tab.

4 Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog box displays.

5 Click within the **Enter the object names to select** field and type the name of the SCEP Admin Account.

6 Click **OK**. The CA Properties dialog box displays.

7 Select the SCEP Admin Account from the **Group or user names** list.

8 Select the **Manage CA** permission **Allow** checkbox.

9 Select the **Request Certificates** permission **Allow** checkbox.

10 Click **OK**.

Step 3: Set Read and Enroll Permissions on the Certificate Template

Set the **Read** and **Enroll** permissions on the certificate template for the NDES/SCEP/MSCEP Service Account and the Device Administrator.

1 Launch the **Certificate Templates Console** by running `certtmpl.msc` from the Windows Desktop.

2 Right-click the required template and select **Properties**. The example here is ‘MobileUser’ from the CA Setup Document.

3 Select the **Security** tab.

4 Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog box displays.

5 Click within the **Enter the object names to select** field and type the name of the Service Account.

6 Click **OK**. The **Properties** dialog box displays.

7 Select the Service Account from the **Group or user names:** list.

8 Select the **Read** permission **Allow** checkbox.

9 Select the **Enroll** permission **Allow** checkbox.

10 Click **OK**.

Step 4: Install the NDES/SCEP/MSCEP Role

1 Launch the **Server Manager** on the server to be used as the NDES/SCEP/MSCEP server.

2 Select **Roles**.

3 Click **Add Roles**. The **Add Roles Wizard** displays.

4 Click **Next**. The **Select Server Roles** dialog box displays.

5 Select **Active Directory Certificate Services**.

6 Click **Next**. The **Select Role Services** dialog box displays.

7 Clear the **Certification Authority** checkbox.

8 Select **Network Device Enrollment Service** (or SCEP/MSCEP).

9 Click **Next**.

10 Click **Select User**. The user selected MUST be in the local IIS_USRS Group.

11 Enter the Username and Password for the account NDES/SCEP/MSCEP Admin Account.

12 Click **Next**. The **Specify CA for Network Device Enrollment Service** (or SCEP/MSCEP) dialog displays.

13 Select **CA Name.**

14 Click **Browse**.

15 Select the CA in the **Select Certification Authority** dialog.

16 Click **OK**.

17 In the **Specify Registration Authority** dialog box, select **Next**.

18 In the **Configure Cryptography for Registration Authority** dialog box, select **Next**.

19 Navigate through any additional required services or roles and then select **Install** and **Next**.

Step 5: Specify the NDES/SCEP/MSCEP Template

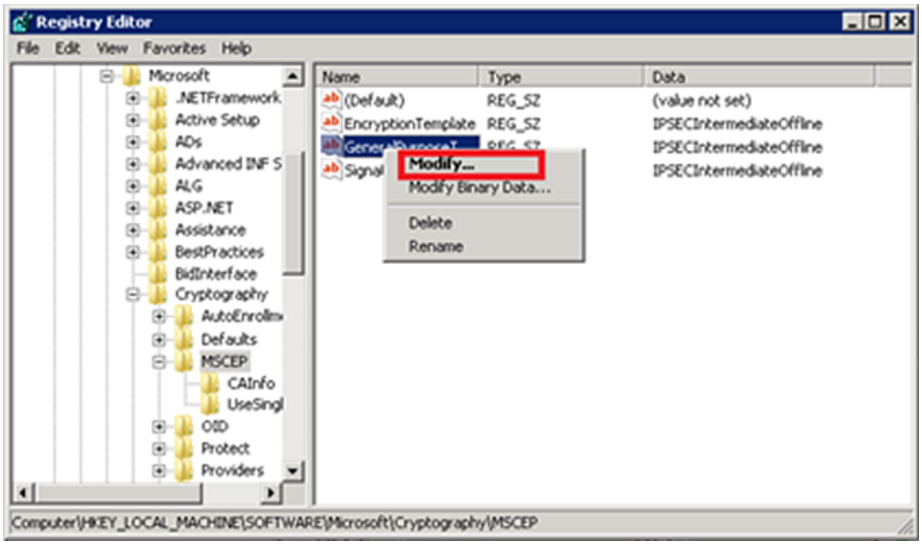
NDES/SCEP/MSCEP is designed to only use one template from the certificate authority. This template is specified in the registry and must be edited using **Registry Editor**.

1 Launch the **Registry Editor** by running `regedit.exe` from the Windows Desktop.

2 Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP` (or NDES/SCEP).

3 Right-click the **General Purpose Template** and select **Modify**.

4 Replace the value `IPSECIntermediateOffline` with the template name being used.



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	IPSECIntermediateOffline
GeneralPurposeT	REG_SZ	IPSECIntermediateOffline
Signat		IPSECIntermediateOffline

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

5 Close the Registry Editor.

6 Restart Internet Information Services by opening a command prompt and running iisreset.

Step 6: Configure IIS to Allow for Large Query Strings

When the device requests a certificate from NDES/SCEP/MSCEP, it sends a string of over 2700 characters as part of the request. This string is larger than the default size for query strings and will result in a 404.15 error. The default query string length must be increased to accommodate this large string.

1 Open a command prompt from the Windows Desktop.

2 Enter the following string:

```
c:\windows\system32\inetsrv\appcmd.exe set config –
section:system.webServer/security/requestFiltering /requestLimits.maxQueryString:
"3072" /commit:apphost
```

Step 7: Configure Certificate Authority and Certificate Template in Workspace ONE UEM

In order for Workspace ONE UEM to retrieve a certificate from a CA, you must correctly configure the Workspace ONE UEM console to use the certificate by performing the following:

- Configure the CA.
- Configure the certificate template.

Configure the CA

1 Log in to the Workspace ONE UEM console as a user with Workspace ONE UEM admin privileges, at minimum.

2 Navigate to **System > Enterprise Integration > Certificate Authorities**.

3 Click **Add**.

4 Enter details about the CA:

   - Select ‘Microsoft ADCS’ from the **Authority Type** drop-down menu. Configure this setting first, because dependent settings appear.
   - Enter the **Name** and **Description** of the new certificate authority.
   - Select the **Protocol**: ADCS or SCEP.
   - Select the **Version**: NDES 2008/2012 or SCEP 2003.
   - Enter the URL of the CA server in the **SCEP URL** field.
   - Select the **Challenge Type** that reflects whether a challenge phrase is required for authentication.

If you want basic authentication, select **Static** and enter an authentication phrase consisting of a singular key or password that is used to authenticate the device with the certificate enrollment URL.

To enable a new challenge to be generated for every SCEP enrollment request, select **Dynamic**.

- Enter the **Challenge Username/Challenge Password**. This user-name and password combination is used to authenticate the device making the request.

  For additional security, upload a certificate under **Challenge Client Certificate** for Workspace ONE UEM to present when fetching the dynamic challenge from the SCEP endpoint.

- Complete the **SCEP Challenge URL** field with a URL in the following format: `http://host/certsrv/mscep_admin/`.
- Advanced Options
  - Enter the **SCEP Challenge Length**, which represents the number of characters in the challenge password.
  - Enter the **Retry Timeout**, which is the time the system waits between retries.
  - Enter the **Max Retries When Pending**, which is the maximum number of retries the system allows while the authority is pending.
  - With **Enable Proxy** checked, Workspace ONE UEM acts as a proxy between the device and the SCEP endpoint defined in the CA configuration.
- Click **Test Connection**. If you select **Save** before **Test Connection**, a “Test is unsuccessful” error displays.

5 Click **Save**.

Configure the Certificate Template

1 Click the **Request Templates** tab.

2 Click **Add**.

3 Enter the following details about the template in the remaining fields:

- Enter the template **Name** and **Description**.
- Select the certificate authority that was just created from the **Certificate Authority** drop-down box.
- Enter the distinguished name in the **Subject Name** field. The text entered in this field becomes the Subject of the certificate, which lets the network administrator determine which devices receive the certificate.

  A typical entry in this field is “CN={EnrollmentUser}” or “CN={DeviceUid}” where the {} fields are Workspace ONE UEM lookup values.

  If you select Automatic Certificate Renewal for the certificate, add CN = {CertificateGUID} as part of the Certificate subject in the template.

- Select the private key length from the Private Key Length drop-down menu.

  This value is typically 2048 and should match the setting on the certificate template that is being used by NDES/SCEP/MSCEP.

- Select the applicable **Private Key Type**.

  This value can be **Signing**, **Encryption**, or both, and the value should match the certificate template being used by NDES/SCEP/MSCEP.

- You may optionally select any of the following:
  - If Workspace ONE UEM automatically renews the certificate when it expires, select **Automatic Certificate Renewal**. Enter the number of days before expiration that Workspace ONE UEM automatically reissues a certificate to the device in the **Auto Renewal Period (days)** field .
  - Select **Enable Certificate Revocation** to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.

    Note If you use the **Enable Certificate Revocation** feature, navigate to **Devices & Users > General > Advanced** and set the number of hours in the **Certificate Revocation Grace Period** field. This period is the amount of time in hours after the discovery that a required certificate is missing from a device that the system waits before actually revoking the certificate. Given the vagaries of wireless technology and network bandwidth performance, this field prevents false negatives or times when a certificate is falsely identified as not existing on a device.

  - Select **Publish Private Key** if the certificate is published to Active Directory or any other customer web service. Then select the proper destination by selecting the appropriate **Private Key Destination**, either **Directory Services** or a **Custom Web Service**.
  - Click **Add** to the right of **Eku Attributes** to insert an object identifier (OID) that represents any additional extended key usages that may be required. You may add multiple **Eku Attributes** to fit your needs.
  - Select **Force Key Generation On Device** to generate a public and private key pair on the device itself. This setting improves CA performance and security.

4 Click **Save**.

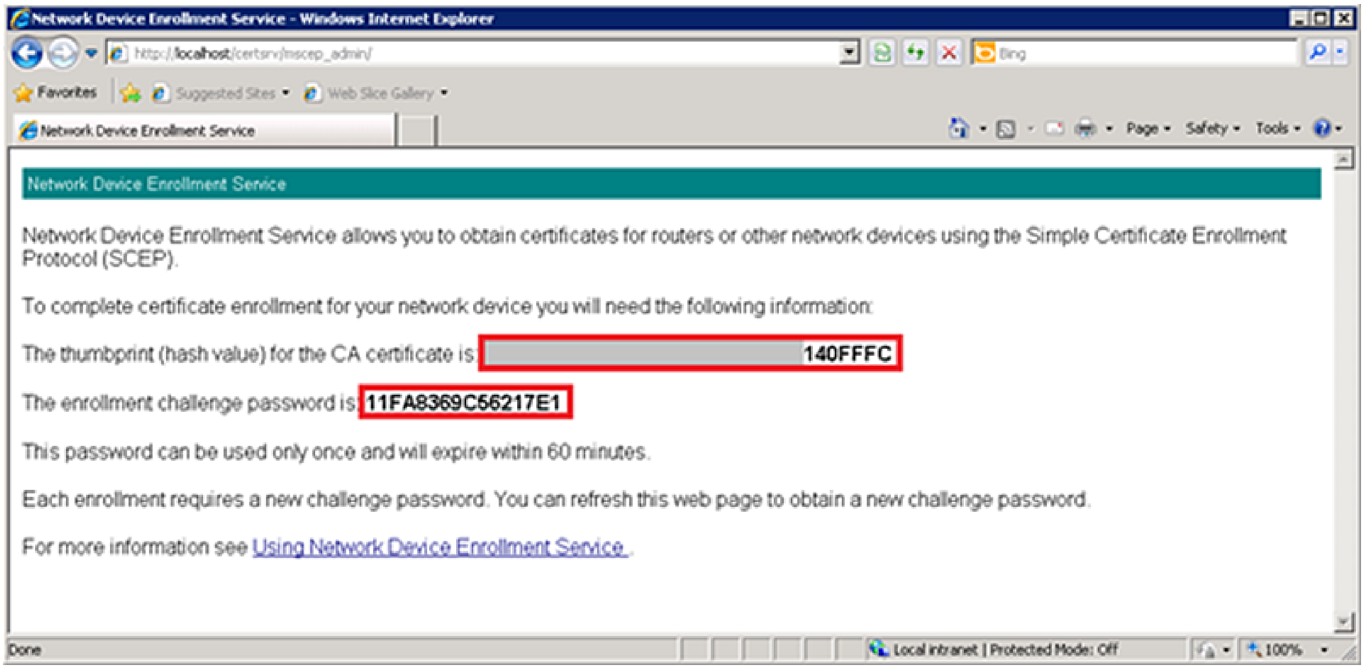
Step 8: Confirm and Test

Testing of the installation and configuration can be performed by browsing to the NDES/SCEP/MSCEP webpage, entering the service account credentials, and confirming the presence of a challenge.

1 Open a web browser and navigate to `http://<servername>/certsvr/mscep_admin/` where `<servername>` is the name of the server running NDES/SCEP/MSCEP. If confirmation and testing is being run from the NDES/SCEP/MSCEP server, the `<servername>` can be “localhost”.

2 Enter the NDES/SCEP/MSCEP Service Account username and password if prompted.

3 The webpage shows a thumbprint and a password if configured properly. If a problem exists with either the authentication of the Service Account or the template, an error displays.



Network Device Enrollment Service - Windows Internet Explorer
http://localhost/certsrv/mscep_admin/
Bing
Favorites
Suggested Sites
Web Slice Gallery
Network Device Enrollment Service
Page
Safety
Tools
Done
Local intranet | Protected Mode: Off
100%

Network Device Enrollment Service

Network Device Enrollment Service allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: [redacted] 140FFFC

The enrollment challenge password is: 11FA8369C56217E1

This password can be used only once and will expire within 60 minutes.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information see Using Network Device Enrollment Service .

Tips and Troubleshooting

- When configuring the certificate password settings, Workspace ONE UEM recommends using the default setting (dynamic password mode).
- Although Workspace ONE UEM supports the use of the registry setting for Single Password mode, Workspace ONE UEM does not recommend using the setting. The “Single Password” mode sets a static challenge password all devices can use which can expose security vulnerabilities.
- If the NDES/SCEP/MSCEP challenge cache is full, (an issue which could arise when publishing a profile, for example), edit the cache value by:

  a Run `regedit.exe` to edit the **PasswordMax** value.

  b The **PasswordMax** value is located at: `HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP` (or NDES/SCEP) within the registry.

  c Increase the **PasswordMax** value to a number greater than the default value of **5**.
- If you receive a "Password Not Present" error when installing the SCEP Profile to a device, confirm that the challenge response length setting in the UEM console matches the length setting associated with the certificate.

Workspace ONE UEM Integration with Microsoft ADCS via DCOM

3

This documentation explains the installation and setup of the Microsoft certificate authority (CA) for direct integration with Workspace ONE UEM over the DCOM protocol.

This chapter includes the following topics:

- System Requirements
- High Level Design
- Install, Set Up, Configure Certificate

System Requirements

Software Requirements

- Microsoft Windows Server 2003, 2008, 2008 R2, 2012 or 2016 Standard or Enterprise

  Workspace ONE UEM recommends using the Enterprise version of Windows server for 50 or more users.

Other Requirements

- Server must be a member of the same domain as the Workspace ONE UEM application server in order to install the Enterprise CA.
- Administrative access to the server.

Network Requirements

The Workspace ONE UEM console server, Workspace ONE UEM Cloud Connector (ACC) server if you are using ACC, must be able to communicate to the Microsoft CA over all configured DCOM ports.

- Port 135: Microsoft DCOM Service Control Manager.
- Ports 1025 - 5000: Default ports DCOM processes.
- Ports 49152 - 65535: Dynamic Ports.

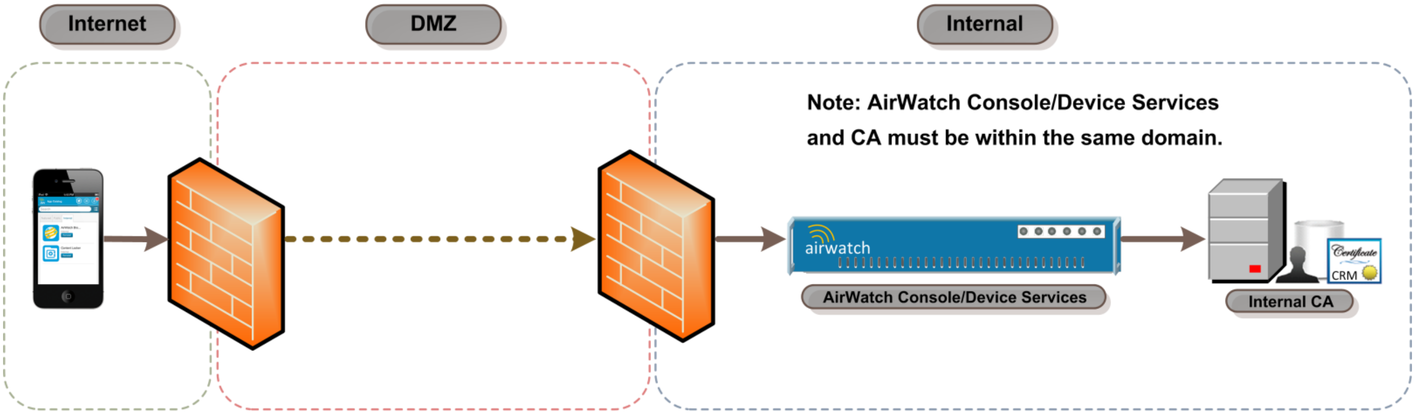
  This port range can be configured to be any number of non-standard ports depending on your DCOM implementation. However, these ports are utilized by default.

High Level Design

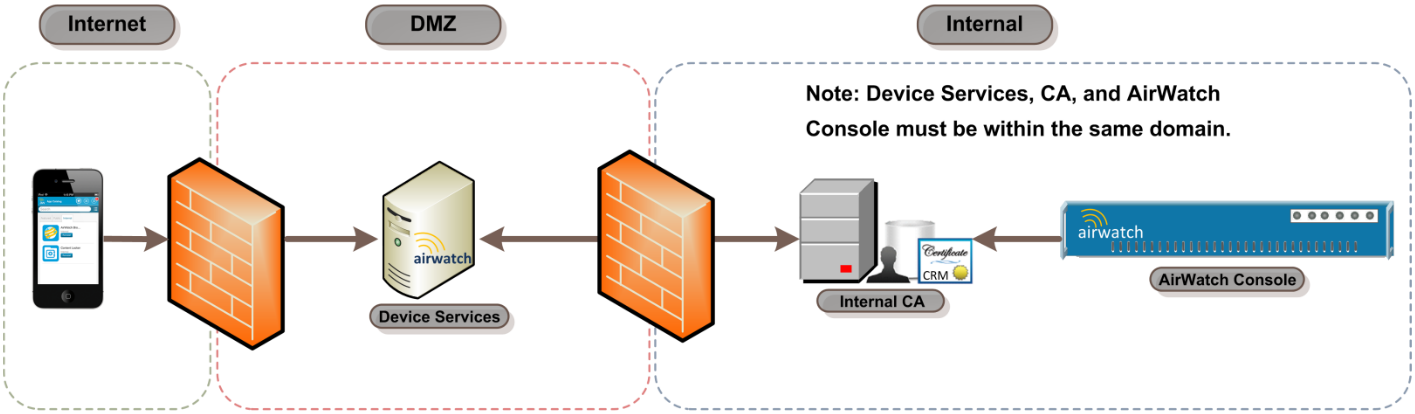
For Workspace ONE UEM to use a certificate in a profile used to authenticate a user, an enterprise CA must be set up in the domain. Additionally, the CA must be joined to the same domain as VMware Enterprise Systems Connector to successfully manage certificates within Workspace ONE UEM.

There are several methods for Workspace ONE UEM to retrieve a certificate from the CA. Each method requires the basic installation and configuration described in this documentation. Sample CA Configurations are shown below.

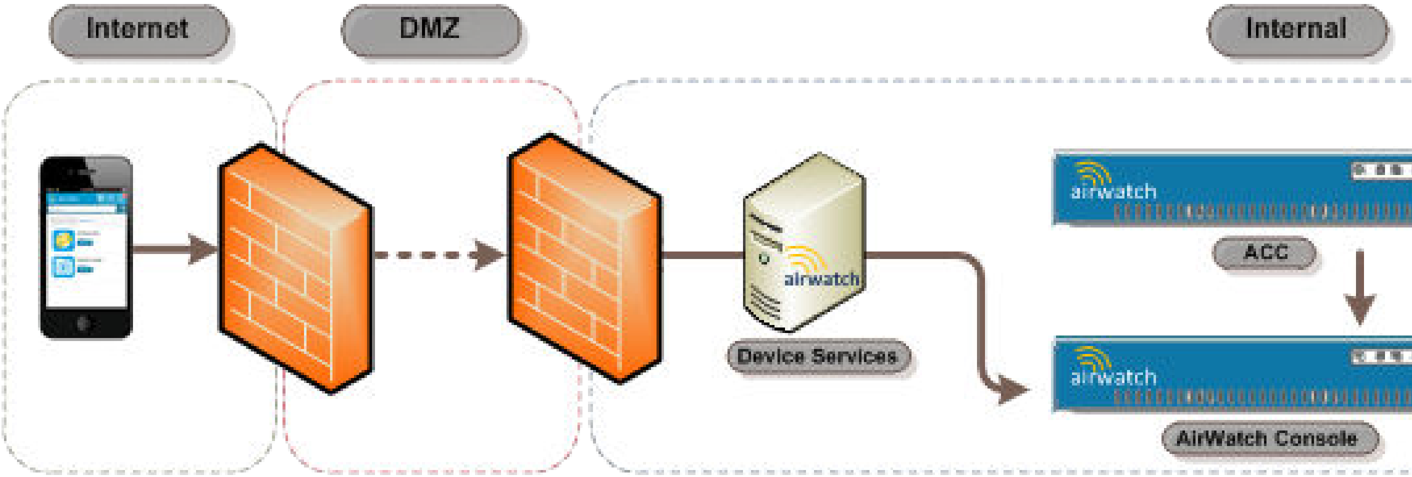
Scenario #1 – On Premise: All Workspace ONE UEM application servers are internal. VMware Enterprise Systems Connector is not installed.


Internet
DMZ
Internal
Note: AirWatch Console/Device Services
and CA must be within the same domain.
airwatch
AirWatch Console/Device Services
Certificate
CRM
Internal CA

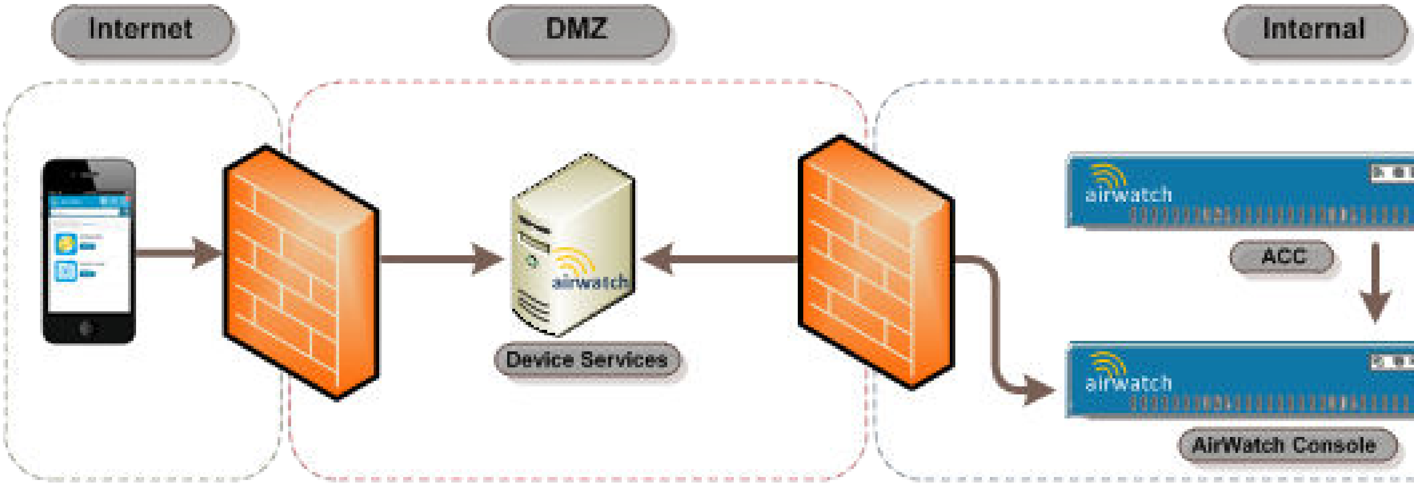
Scenario #2 – On Premise: Device Services is located in the DMZ. CA and Workspace ONE UEM servers are internal. VMware Enterprise Systems Connector is not installed.



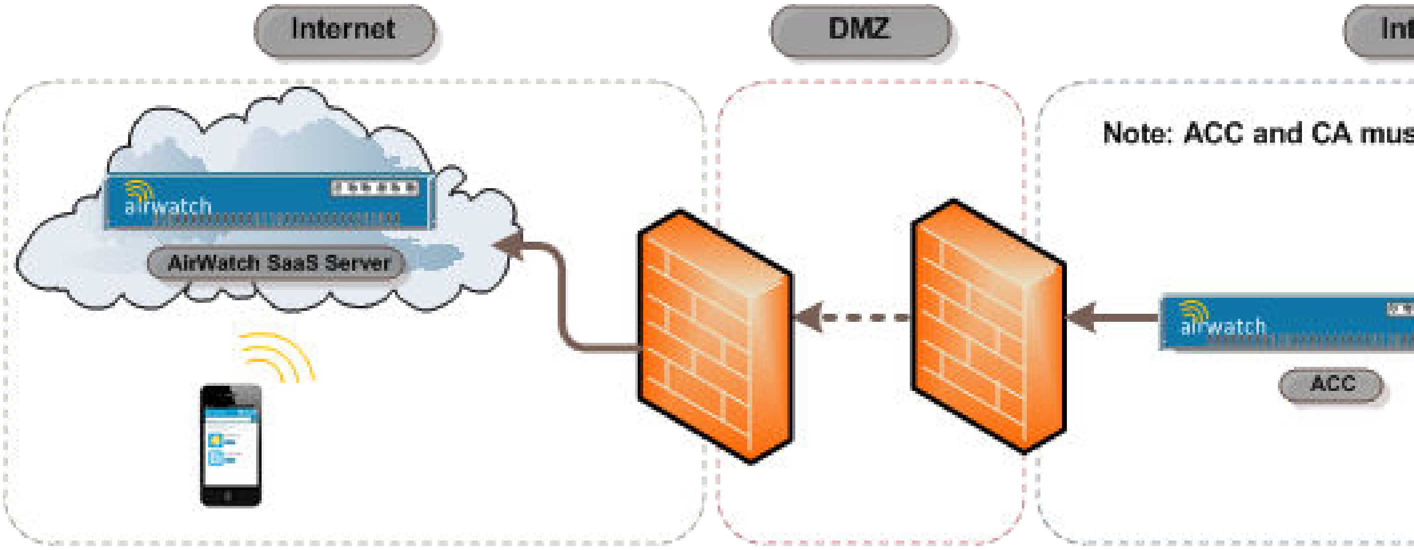
Scenario #3 – On Premise: Devices Services, VMware Enterprise Systems Connector, Workspace ONE UEM servers, and CA are internal.



Scenario #4 – On Premise: Device Services is located in the DMZ. VMware Enterprise Systems Connector, Workspace ONE UEM servers, and CA are internal.



Scenario #5 – SaaS: Workspace ONE UEM is SaaS. VMware Enterprise Systems Connector and CA are internal.



Install, Set Up, Configure Certificate

This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console.

Take the following steps and procedures to integrate the certificate.

Step 1: Install the Microsoft CA Role

Add the ADCS Role

1 Click the **Server Manager** icon next to the **Start** button to open the **Server Manager** window.

2 Click **Roles** in the left pane.

3 Click **Add Role** in the right pane. An **Add Roles Wizard** window displays.

4 Under **Server Roles**, select the **Active Directory Certificate Services** checkbox.

5 Click **Next**.

6 Select the **Certification Authority** checkbox and then select **Next**.

7 Select **Enterprise** and then select **Next**.

8 Select **Root CA** and then select **Next**.

Define CA Private Key Settings

1 Select **Create a new private key** and then select **Next**.

2 Select your preferred **Key character length** (for example 4096).

3 Select your preferred algorithm (for example SHA256) from the **Select the hash algorithm for signing certificates issued by the CA** and then select **Next**.

4 Click **Common name for this CA** and enter the name of the CA or use the default CA displayed and then select **Next**.

Make note of the name of the CA server. You will need to enter this information in Workspace ONE UEM when setting up access to the CA.

5 Select the desired length of time under **Set the validity period for the certificate generated for this CA** and then select **Next**.

The length of time you select is the validity period for the CA â€’not the certificate, however, when the validity for the CA expires, so does the certificate.

Configure the ADCS Certificate Database

1 Click **Next** to accept the default information in the **Configure Certificate Database** screen.

2 Click **Next** to accept the **Confirm Installation Selections** screen.

3 Click **Install**. The installation begins. After the installation completes, the **Installation Results** window displays.

4 Click **Close**.

Step 2: Configure Microsoft CA

Add a Service Account on the CA

1 Launch the **Certification Authority Console** from the Administrative Tools in Windows.

2 In the left pane, select **(+)** to expand the CA directory.

3 Right-click the name of the CA and select **Properties**. The **CA Properties** dialog box displays.

4 Click the **Security** tab.

5 Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog box displays.

6 Click within the **Enter the object names to select** field and type the name of the service account (e.g., **Ima Service**).

7 Click **OK**. The **CA Properties** dialog box displays.

8 Select the service account you added in the previous step (e.g., **Ima Service**) from the **Group or user names** list.

9 Select the **Read**, the **Issue and Manage Certificates**, and the **Request Certificates** checkboxes to assign permissions to the service account.

10 Click **OK**.

Configure the CA to use Subject Alternative Name in Certificates

1 Open a command prompt from the Windows Desktop and enter the following in the order they appear. These commands configure the CA to allow the use of the Subject Alternative Name (SAN) in a certificate.

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
```

```
net stop certsvc
```

```
net start certsvc
```

Add a Certificate Template on the CA

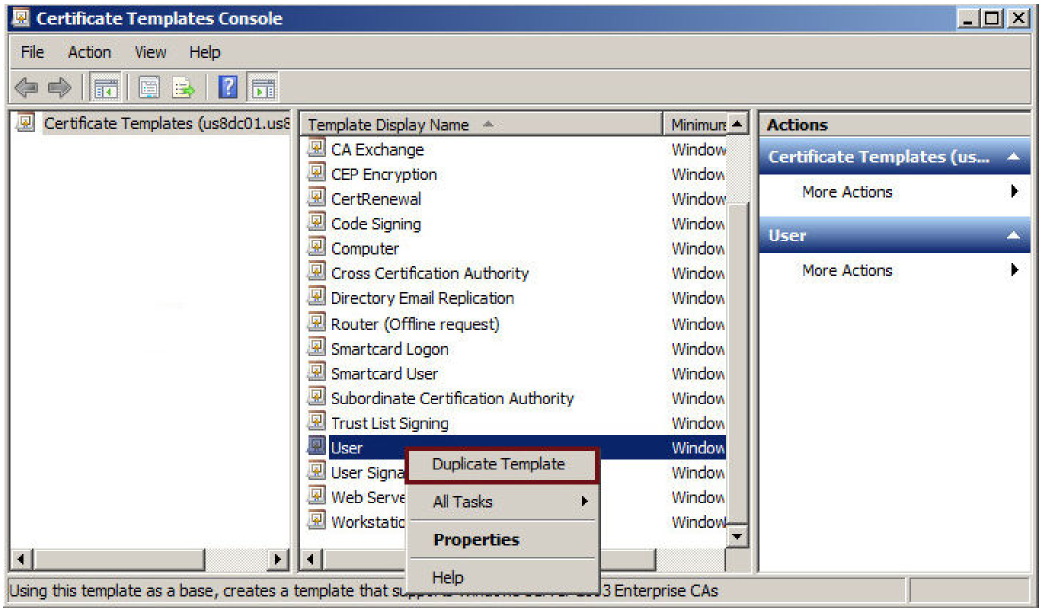
The CA (certsrv) window displays.

1 In the left pane, select **(+)** to expand the CA directory.

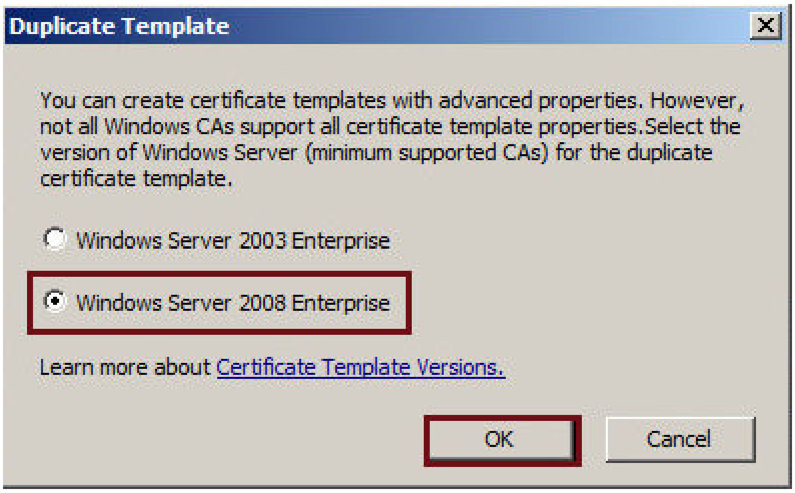
2 Right-click the **Certificate Template** folder and select **Manage**. The **Certificate Templates Console** window displays.

3 Select the desired template (e.g., User) under **Template Display Name**, and right-click **Duplicate Template**. The **Duplicate Template** dialog box displays.

Workspace ONE UEM will use the duplicate certificate template. The template you choose depends on the function being configured in Workspace ONE UEM. For Wi-Fi, VPN, or Exchange Active Sync (EAS) client authentication select User template.



4 Select the **Windows Server** that represents the oldest enterprise version being used within the domain to ensure backward compatibility of the certificate that was issued.



Duplicate Template

You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

○ Windows Server 2003 Enterprise

● Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

5 Click **OK**. The **Properties of New Template** dialog box displays.

Configure Certificate Template Properties

1 Click the **General** tab.

2 Type the name of the template displayed to users in the **Template display name** field. The **Template name** field auto-fills with the template display name without spaces.

You may use this default value or enter a new template name if desired. The template name may not contain spaces. Make note of the template name. You will need to enter this information in Workspace ONE UEM.

You will enter the **Template name** you just configured with no spaces in the Workspace ONE UEM console in the **Issuing Template** field within the **Configuring the Certificate Template** screen.

3 Select the desired length of time for the certificate to be active from the **Validity period** entry field/drop-down menu.

You should choose a length of time that is less than the time you chose for the Step 1: Install the Microsoft CA Role. By doing this the certificate will expire before the CA.

4 Click **Apply**.

5 Click the **Request Handling** tab.

6 Select the appropriate client authentication method from the **Purpose:** drop-down menu. This selection might be based on the application of the certificate being issued, although for general purpose client authentication, select **Signature and Encryption**.

7 Select the **Allow private key to be exported** checkbox.

For a certificate to be installed on an iOS device, this checkbox MUST be selected.

8 Click **Apply**.

9 Select the **Subject Name** tab.

10 Select **Supply in the request**. If **Supply in the request** is not selected, the certificate will be generated to the service account instead of the desired end user.

Enable the Template for Certificate Authentication

1 Click the **Extensions** tab.

2 Select **Application Policies** from the **Extensions included in this template:** field. This allows you to add client authentication.

3 Click **Edit**. The **Edit Application Policies Extension** dialog box displays.

4 Click **Add**. The **Add Application Policy** dialog box displays.

5 Select **Client Authentication** from the **Application policies:** field.

6 Click **OK**. The **Properties of New Template** dialog box displays.

Provide the AD Service Account Permissions to Request a Certificate

1 Click the **Security** tab.

2 Click **Add**. The **Select Users, Computers, Service Accounts or Groups** dialog box displays. This allows you to add the service account configured in Active Directory to request a certificate.

3 Enter the name of the service account (e.g., Ima Service) in the **Enter the object names to select** field.

4 Click **OK**. The **Properties of New Template** dialog box displays.

5 Select the service account you created in the previous step (e.g., Ima Service) from the **Group or user names:** field.

6 Select the **Enroll** checkbox under **Permissions for CertTemplate ServiceAccount**.

7 Click **OK**.

Enable the Certificate Template on the CA

1 Navigate to the **Certificate Authority Console**.

2 Click **(+)** to expand the CA directory.

3 Click **Certificate Templates** folder.

4 Right-click and select **New > Certificate Template to Issue**. The **Enable Certificates Templates** dialog box displays.

5 Select the name of the certificate template (e.g., Mobile User) that you previously created in Creating a Name for the Certificate Template.

6 Click **OK**.

Step 3: Configure CA and Certificate Template in Workspace ONE UEM

In order for Workspace ONE UEM to retrieve a certificate from a CA, you must correctly configure the Workspace ONE UEM console to use the certificate by performing the following.

- Configure the CA
- Configure the certificate template

Configure the CA

1. Login to the Workspace ONE UEM console as a user with Workspace ONE UEM Administrator privileges, at minimum.
2. Navigate to **System > Enterprise Integration > Certificate Authorities**.
3. Click **Add**.
4. Select **Microsoft ADCS** from the **Authority Type** drop-down menu. You need to select this option prior to populating other fields in the dialog so applicable fields and options display.
5. Enter the following details about the CA in the remaining fields.
    - Enter a name for the CA in the **Certificate Authority** field. This is how the CA will be displayed within the Workspace ONE UEM console.
    - Enter a brief **Description** for the new CA.
    - Select **ADCS** radio button in the **Protocol** section. If you select SCEP, note that there are different fields and selections available not covered by this whitepaper.
    - Enter the host name of the CA server in the **Server Hostname** field.
    - Enter the actual CA Name in the **Authority Name** field. This is the name of the CA to which the ADCS endpoint is connected. This can be found by launching the **Certification Authority** application on the CA server.
    - Select the radio button that reflects the type of service account in the **Authentication** section. **Service Account** causes the device user to enter credentials. **Self-Service Portal** authenticates the device without the user having to enter their credentials.
    - Enter the Admin **Username** and **Password**. This is the username and password of the ADCS Admin Account (created in the previous Step 2: Configure Microsoft CA) which has sufficient access to allow Workspace ONE UEM to request and issue certificates.
6. Click **Save**.

Configure the Certificate Template

1. Select the **Request Templates** tab.
2. Click **Add**.

3 Complete the certificate template information.

- Enter a friendly name for the new **Request Template**. This name is used by the Workspace ONE UEM console.
- Enter a brief **Description** for the new certificate template.
- Select the **Certificate Authority** that was just created from the certificate authority drop-down menu.
- Enter the name of the **Issuing Template** (e.g., MobileUser) that you configured in **Configuring Certificate Template Properties** in the **Template name** field. Make sure you enter the name with no spaces.
- Enter the **Subject Name** or Distinguished Name (DN) for the template. The text entered in this field is the “Subject” of the certificate, which can be used by the network administrator to determine who or what device received the certificate.

  A typical entry in this field is “CN={EnrollmentUser}” or “CN={DeviceUid}” where the {} fields are Workspace ONE UEM lookup values.
- Select the private key length from the **Private Key Length** drop-down menu.

  This is typically 2048 and should match the setting on the certificate template that is being used by DCOM.
- Select the **Private Key Type** using the applicable checkbox.

  This should match the setting on the certificate template that is being used by DCOM.
- Under **SAN Type**, select **Add** to include one or more Subject Alternate Names with the template. This is used for additional unique certificate identification. In most cases, this needs to match the certificate template on the server. Use the drop-down menu to select the SAN Type and enter the subject alternate name in the corresponding data entry field. Each field supports lookup values. **Email Address**, **User Principal Name**, and **DNS Name** are supported by ADCS Templates by default, and Workspace ONE UEM recommends that you use them.

  Select the checkbox for **Security Identifier** to include the AD SID in the certificate SAN.
- Select the **Automatic Certificate Renewal** checkbox to have certificates using this template automatically renewed prior to their expiration date. If enabled, specify the Auto Renewal Period in days.
- Select the **Enable Certificate Revocation** checkbox to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.

  Note If you are making use of the Enable Certificate Revocation feature, navigate to **Devices & Users > General > Advanced** and set the number of hours in the **Certificate Revocation Grace Period** field. This is the amount of time in hours after the discovery that a required certificate is missing from a device that the system will wait before actually revoking the certificate. Given the vagaries of wireless technology and network bandwidth performance, this field is designed to prevent false negatives or times when a certificate is falsely identified as not existing on a device.

- Select the **Publish Private Key** checkbox to publish the private key to the specified web service endpoint (Directory Services or custom web service).

  Publishing Private Key is only applicable when using Lotus Domino.

- Click **Add** to the right of **Eku Attributes** to insert an object identifier (OID) that represents any additional extended key usages that may be required. You may add multiple Eku Attributes to fit your needs.
- Select the **Force Key Generation on Device** checkbox to generate public and private key pair on the device which improves CA performance and security.

4 Click **Save**.