Workspace ONE UEM Certificate Authority Integration with Microsoft ADCS Using DCOM

VMware Workspace ONE UEM 1810

vmware®

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

Workspace ONE UEM Integration with Microsoft ADCS via DCOM

<div align="right">1</div>

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 setup allows Workspace ONE UEM to take advantage of digital certificates by automating the issuing, renewal, and revocation process to mobile devices.

This chapter includes the following topics:

- System Requirements
- High Level Design

System Requirements

Software Requirements

- Microsoft Windows Server 2003, 2008, 2008 R2, 2012 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.
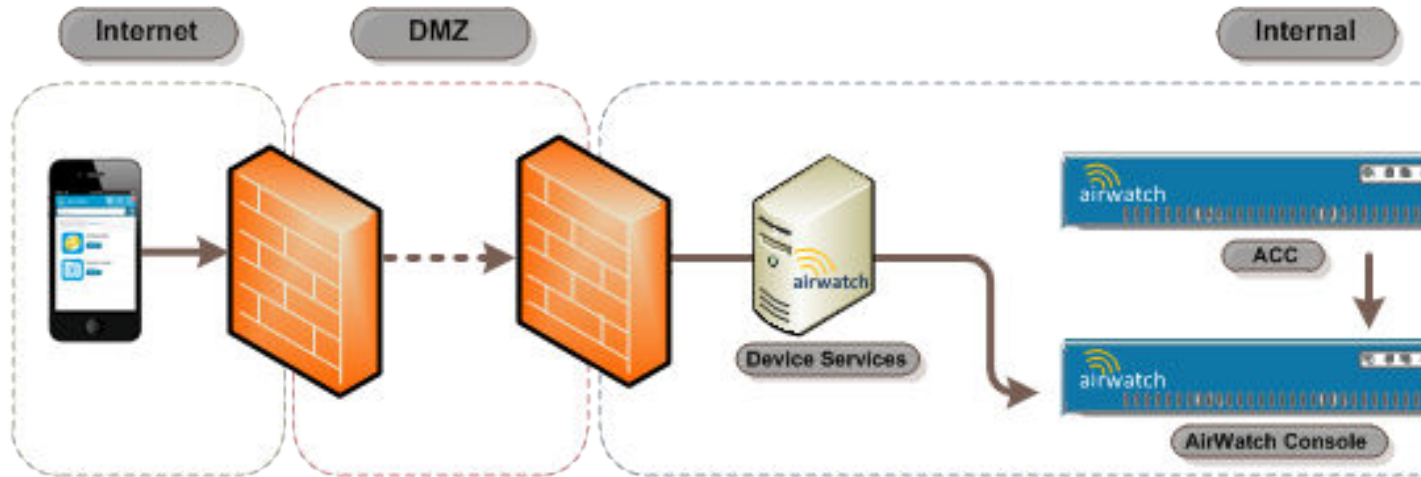
Scenario #1 – On Premise: All Workspace ONE UEM application servers are internal. VMware Enterprise Systems Connector is not installed.
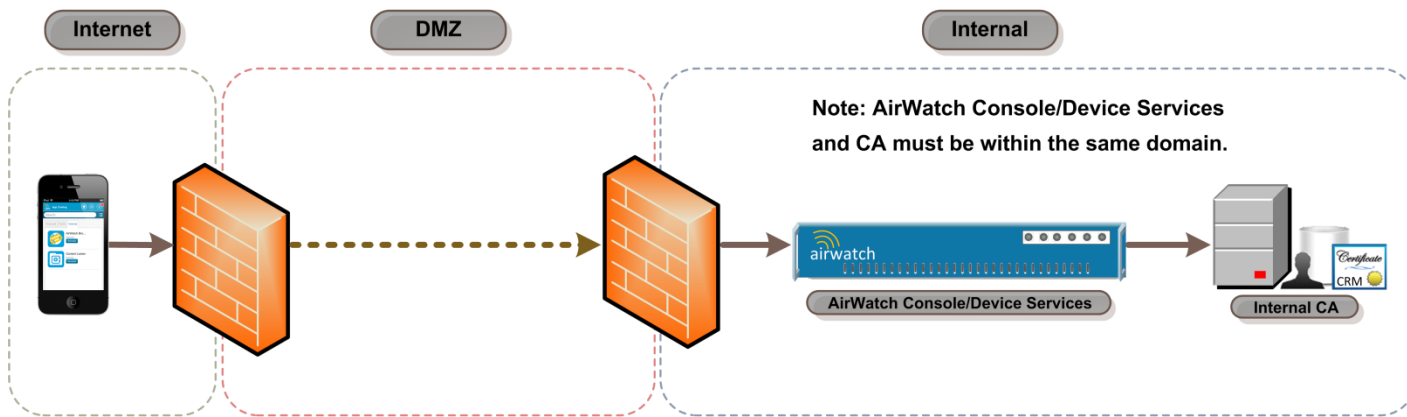
Scenario #2 – On Premise: Device Services is located in the DMZ. CA and Workspace ONE UEM servers are internal. VMware Enterprise Systems Connector is not installed.
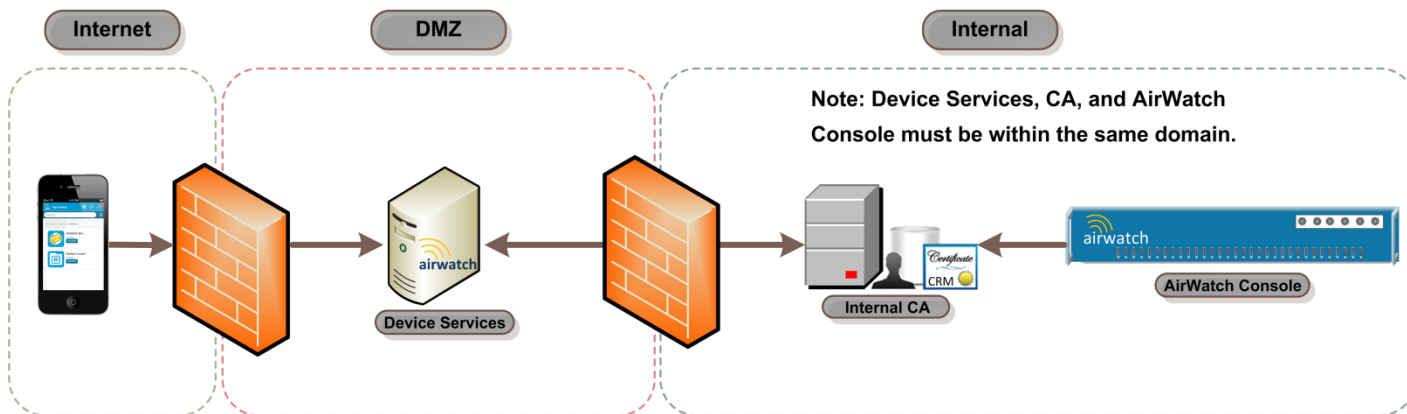
## Scenario #3 – On Premise: Devices Services, VMware Enterprise Systems Connector, Workspace ONE UEM servers, and CA are internal.

Scenario #4 – On Premise: Device Services is located in the DMZ. VMware Enterprise Systems Connector, Workspace ONE UEM servers, and CA are internal.
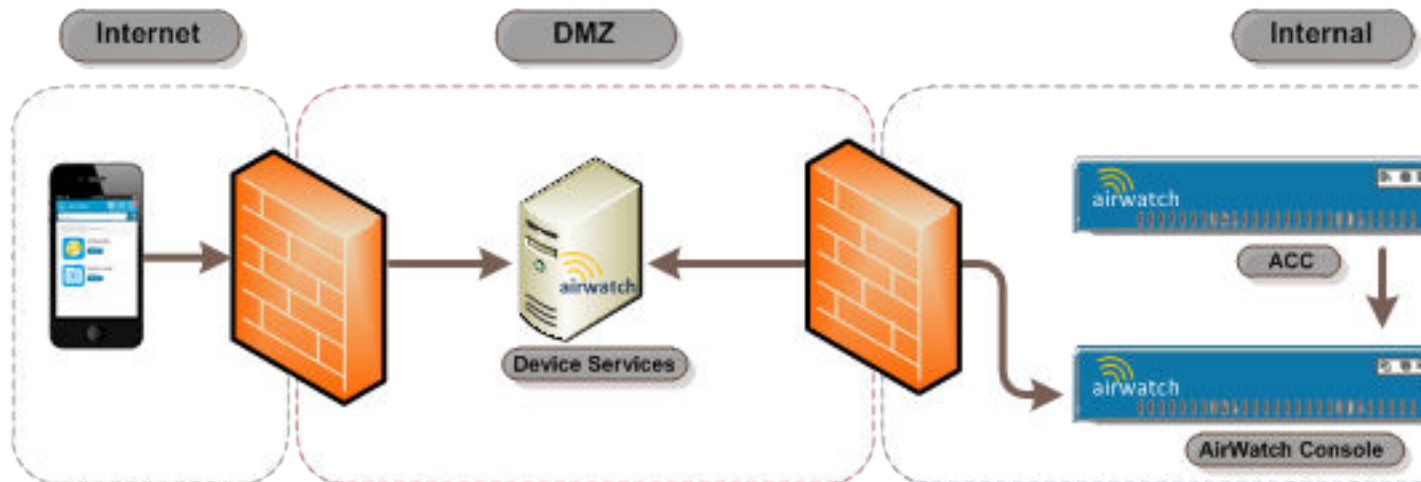
Scenario #5 – SaaS: Workspace ONE UEM is SaaS. VMware Enterprise Systems Connector and CA are internal.
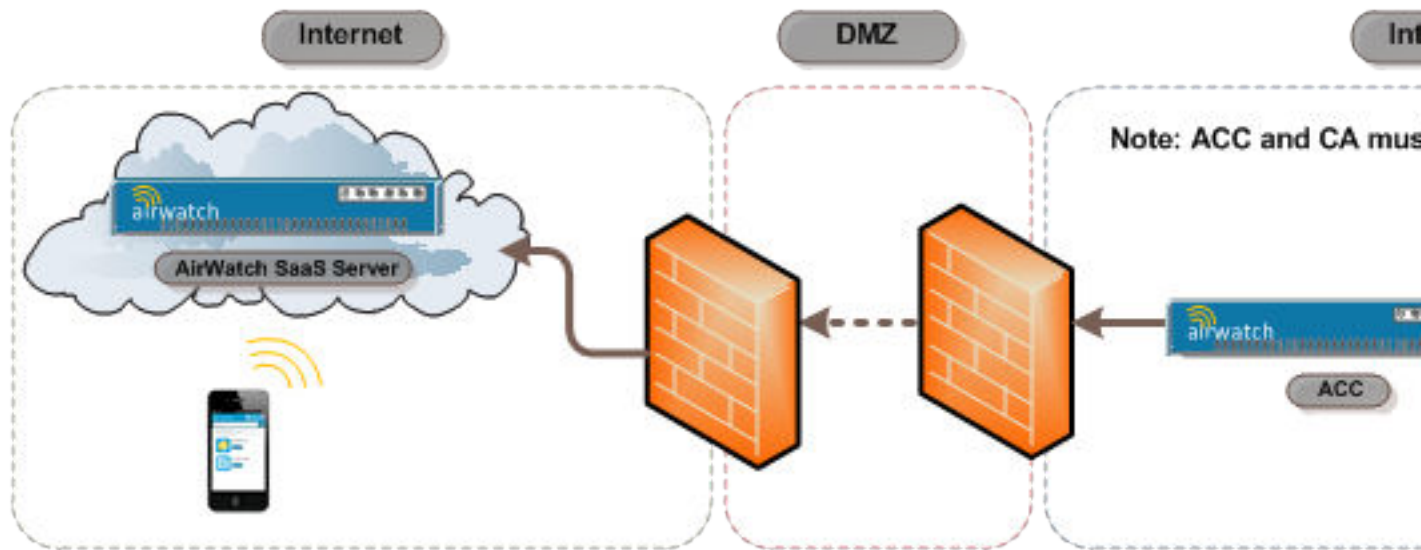
Install, Set Up, Configure Certificate

2

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.

This chapter includes the following topics:

- Step 1: Install the Microsoft CA Role

- Step 2: Configure Microsoft CA

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

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.
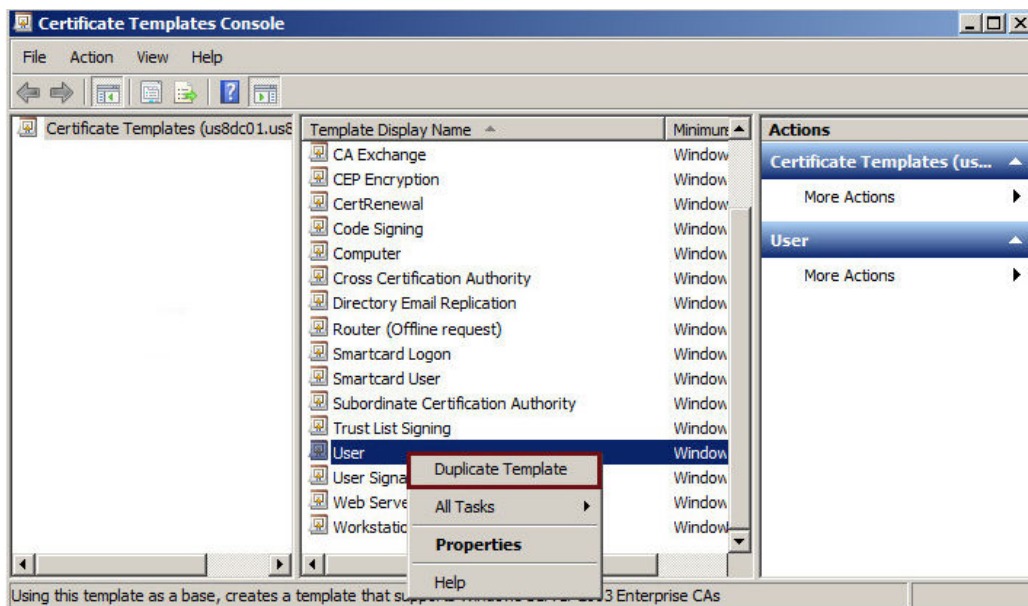
4   Select the **Windows Server** that represents the oldest enterprise version being used within the domain to ensure backward compatibility of the certificate that was issued.
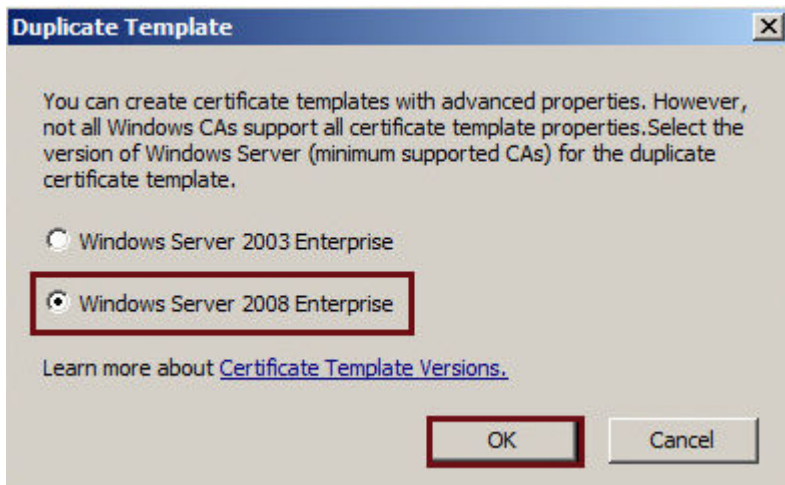
5   Click **OK**. The **Properties of New Template** dialog box displays.

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 **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**.