VMware AirWatch Integration with Microsoft NDES via SCEP

For VMware AirWatch

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

Table of Contents

Chapter 1:
Workspace ONE UEM Integration with Microsoft NDES via SCEP

This document explains the installation and setup of the Microsoft certificate authority (CA) for direct integration with Workspace ONE UEM over the NDES/SCEP/MSCEP protocol. This setup allows Workspace ONE UEM to take advantage of digital certificates by automating the issuing, renewal, and revocation process to mobile devices.

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

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, 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:** 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

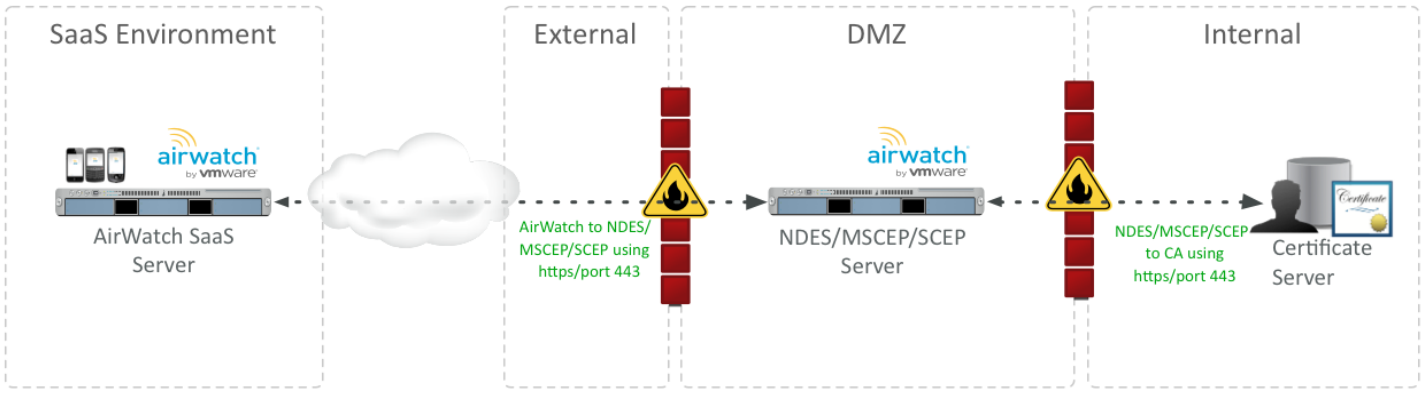
- SCEP endpoint must be accessible from the device in order for certificate enrollment to complete.
  - The exception to this requirement is when you utilize the **Enable Proxy** option in the **Certificate Authority - Add/Edit** page for non-generic SCEP protocol usage.
- An **Admin Account** must exist 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 on page 7 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 on page 8 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 on page 8 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 on page 8 below for information on setting permissions.
  - Member of the Local Administrator group (standalone).

High Level Design

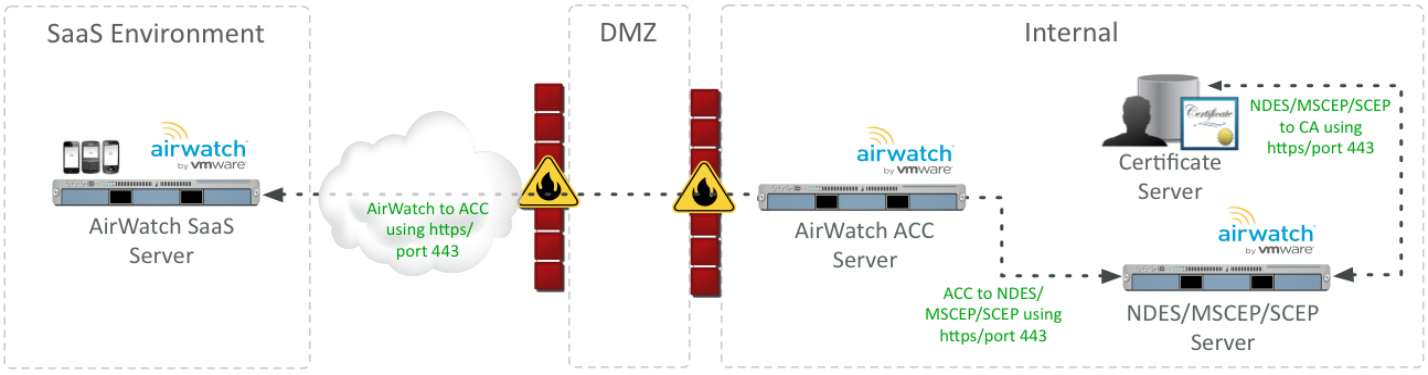
In order for Workspace ONE UEM to use a certificate in a profile, which is used to authenticate a user, an enterprise certificate authority does not need to be set up in the same domain as the Workspace ONE UEM server.

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 document. Sample CA Configurations are shown below in the Workspace ONE UEM SaaS environment. Configurations will differ in on-premises environments.

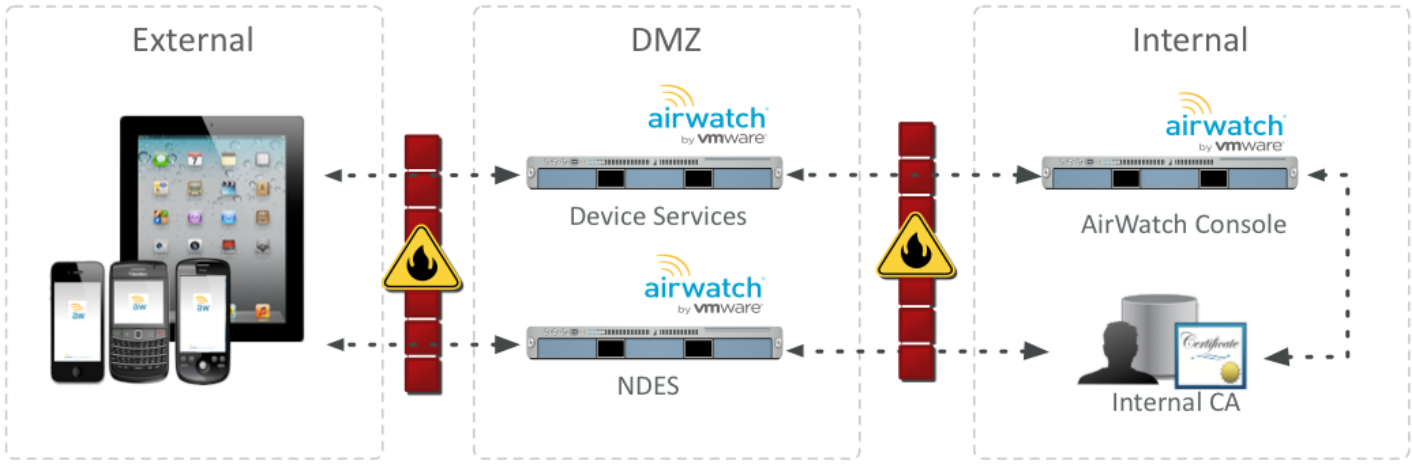
Scenario #1: Workspace ONE UEM to NDES/SCEP/MSCEP and then to Certificate Authority



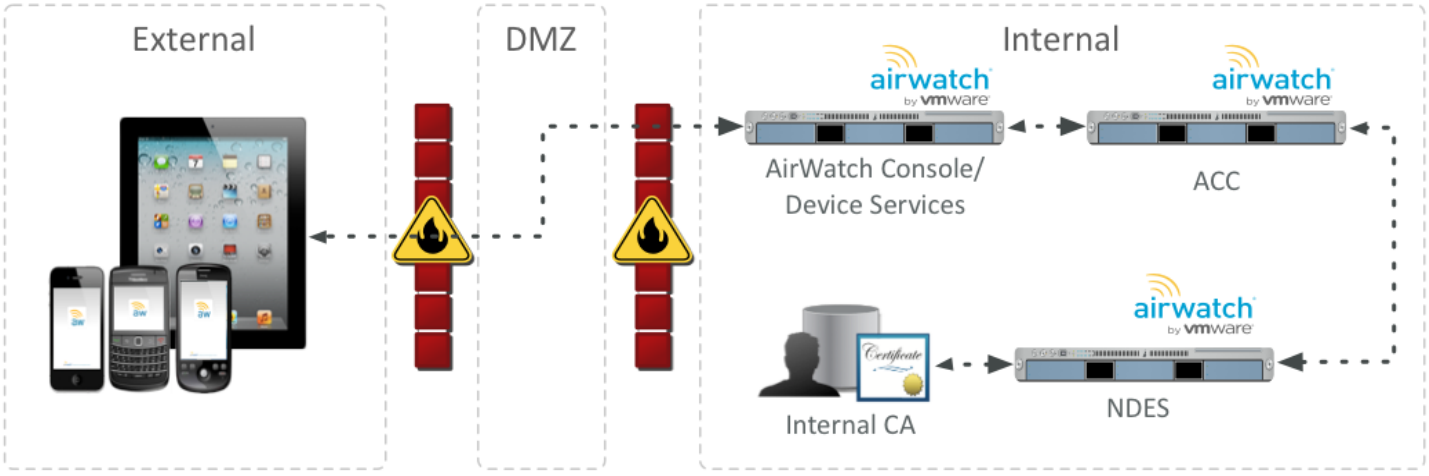
Scenario #2: Workspace ONE UEM to VMware Enterprise Systems Connector, then to NDES/SCEP/MSCEP, and then to Certificate Authority



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



Chapter 2:
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**.

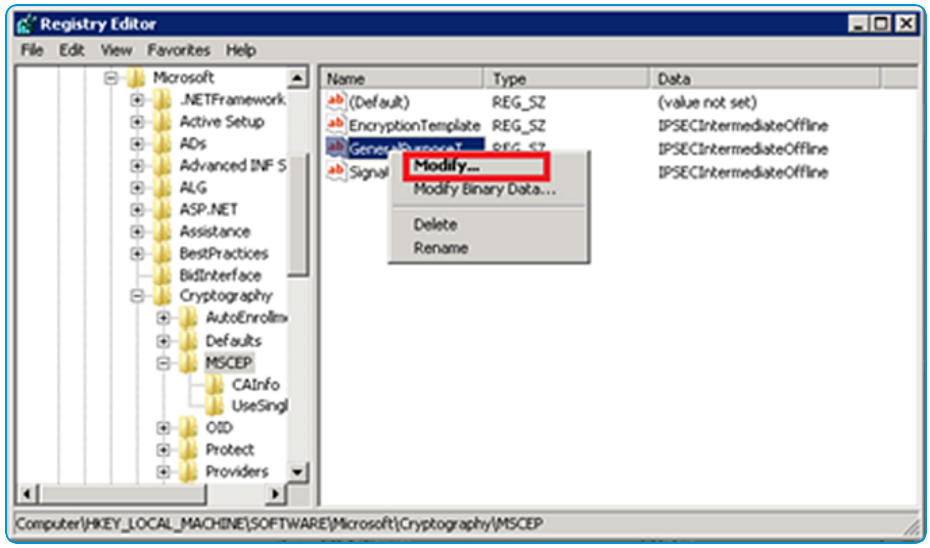
Step 4: Install the NDES/SCEP/MSCEP Role

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.



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.
   - 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.

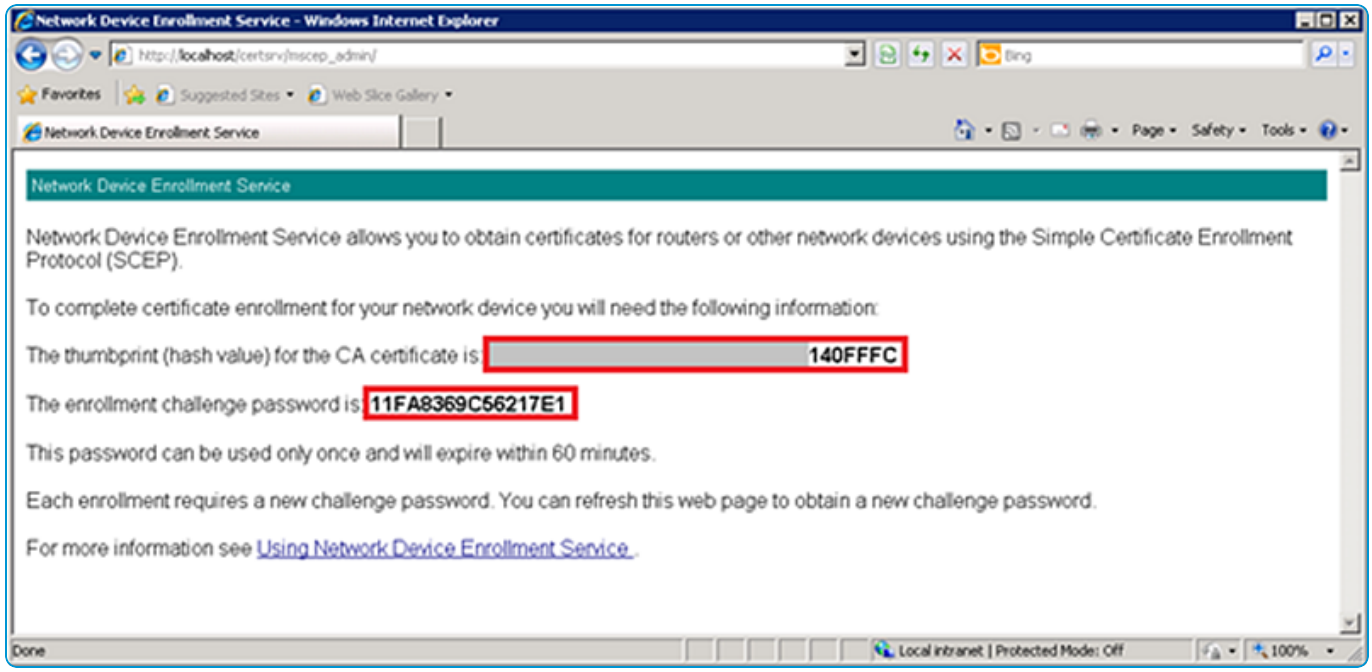
    Note: If you use the **Enable Certificate Revocation** feature, navigate to **Devices & Users > General > Advanced** and set the number of hours in the **Certificate Revocation Grace Period** field. This period is the amount of time in hours after the discovery that a required certificate is missing 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.



Chapter 3:
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:
  1. Run `regedit.exe` to edit the **PasswordMax** value.
  2. The **PasswordMax** value is located at: `HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP` (or NDES/SCEP) within the registry.
  3. Increase the **PasswordMax** value to a number greater than the default value of **5**.