

Certificate Authority Integrations

VMware Workspace ONE UEM 2203

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

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	Certificate Authority Integrations	5
	Compare Microsoft Certificate Authority Models	5
	Available Microsoft Certificate Authority Models	5
	Comparison Matrix by Protocol	6
	Workspace ONE UEM Directly to CA	6
	Device to CA with UEM as Delegate	7
	Workspace ONE UEM SCEP Proxy Between Device and CA	8
2	NDES for SCEP	10
	Prerequisites	13
	Procedure	14
	What to do next	20
3	Cisco IPSec VPN	22
	Prerequisites	23
	Procedure	23
	What to do next	26
4	SCEP	28
	Prerequisites	29
	Procedure	29
5	EOBO with AD CS via DCOM	32
	Prerequisites	34
	Procedure	35
	What to do next	41
6	SecureAuth	42
	Prerequisites	44
	Procedure	44
	What to do next	46
7	GlobalSign	48
	Prerequisites	49
	Procedure	49
	What to do next	50
8	Entrust ID Issuance	52

Prerequisites	52
Procedure	53
What to do next	55

Certificate Authority Integrations

1

Certificates help protect your infrastructure from brute force attacks, dictionary attacks, and employee error. If you use certificates, integrate your certificate authority with VMware Workspace ONE® UEM powered by AirWatch for increased stability, security, and authentication.

This chapter includes the following topics:

- [Compare Microsoft Certificate Authority Models](#)

Compare Microsoft Certificate Authority Models

Find out what Microsoft certificate authority (CA) models Workspace ONE UEM supports. View a high-level comparison of each CA type and consider which configuration might work best for your deployment.

- Available Microsoft Certificate Authority Models
- Comparison Matrix by Protocol
- Workspace ONE UEM Directly to CA
- Device to CA with UEM as Delegate
- Workspace ONE UEM SCEP Proxy Between Device and CA

Available Microsoft Certificate Authority Models

Workspace ONE UEM offers several deployment options for Microsoft certificate authorities.

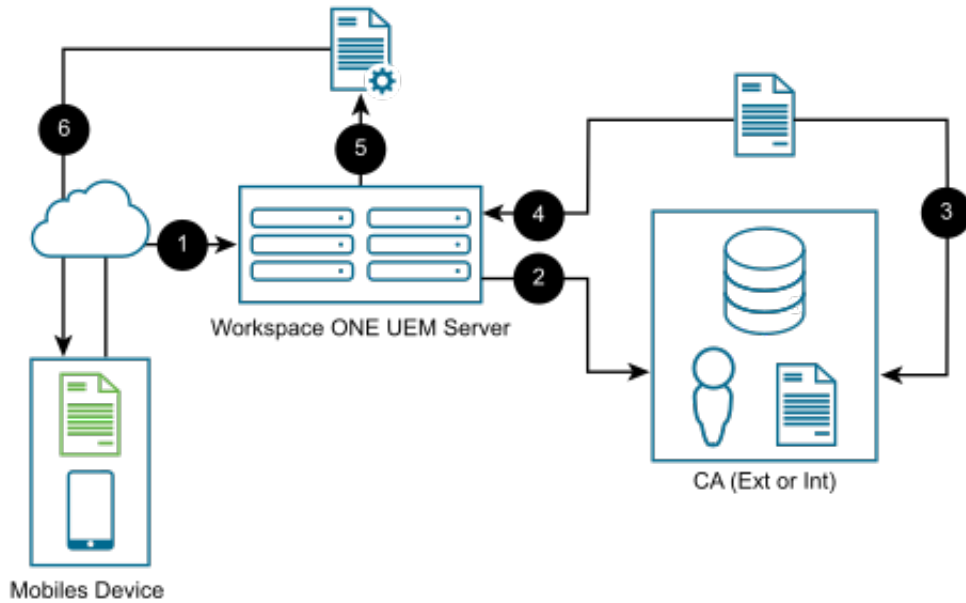
- Workspace ONE UEM to the CA - This model uses the DCOM protocol. Workspace ONE UEM communicates directly with the Microsoft CA or through the AirWatch Cloud Connector to the CA.
- Mobile Devices to the CA - This model uses the NDES (a Microsoft proprietary version of SCEP) or SCEP protocol. Workspace ONE UEM only delegates certificate transactions between the device and the Microsoft CA.
- Workspace ONE UEM SCEP Proxy - This model uses the NDES or SCEP protocol. Workspace ONE UEM is the proxy that sends certificate transactions between the device and the CA endpoint. The NDES/SCEP endpoint is not exposed to the Internet.

Comparison Matrix by Protocol

Considerations	DCOM Protocol: Workspace ONE UEM to CA	NDES/SCEP Protocol: Workspace ONE UEM as Delegate	NDES/SCEP Protocol: Workspace ONE UEM SCEP Proxy
Key Benefit	You can automate the certificate lifecycle management (certificate revocation and renewal).	Each device generates and has its own key pair.	The NDES/SCEP endpoint is not exposed to the Internet.
Devices Supported	<ul style="list-style-type: none"> ■ Android ■ iOS ■ Windows 10 ■ macOS 	<ul style="list-style-type: none"> ■ Android ■ iOS ■ Windows 10 ■ macOS 	<ul style="list-style-type: none"> ■ Android ■ iOS ■ Windows 10 ■ macOS
Architecture	Workspace ONE UEM servers must have DCOM access to the CA.	NDES/SCEP server must be externally available to the Internet.	Workspace ONE UEM must be able to reach the NDES/SCEP server.
Key Pair Generation	CA server handles the key pair generation.	Device handles the key pair generation.	Device handles the key pair generation.
Ports	DCOM Port 135: Microsoft DCOM Service Control Manager DCOM Ports 1025–5000: Default ports for DCOM processes but you can configure the port range to any non-standard ports.	HTTP/HTTPS 443 or 80	HTTP/HTTPS 443 or 80
Certificate Template	For example, a single CA supports Wi-Fi, VPN, and email certificates.	For example, Wi-Fi, VPN, and email certificates require three separate templates.	Single template per instance. For example, Wi-Fi, VPN, and email certificates require three separate templates.
Certificate Renewal	Automatic renewal available.	SCEP - Requires manual renewal by profile repush. NDES - Automatic renewal available.	SCEP - Requires manual renewal by profile repush. NDES - Automatic renewal available.
Certificate Revocation	Supported	Not supported	Not supported

Workspace ONE UEM Directly to CA

Direct CA integration with Workspace ONE UEM over DCOM provides functionality for mobile certificate management. With direct CA integration, unlike with regular SCEP, there are no exposed endpoints of your Public Key Infrastructure (PKI) left open and vulnerable to attack. Plus, it offers additional features such as the ability to issue multiple certificate templates and revoke certificates from the CA by including them in a Certificate Revocation List (CRL).

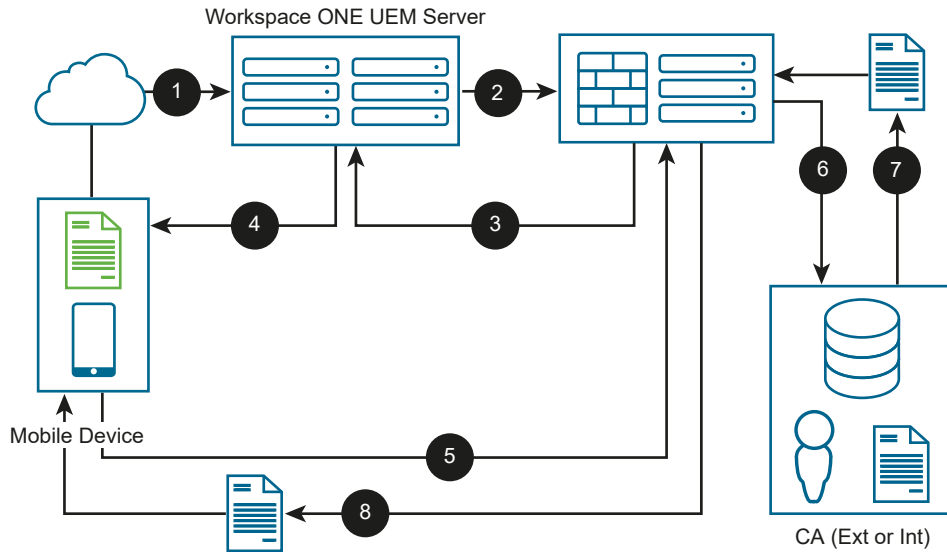


For on-premises, Workspace ONE UEM can directly communicate to your CA within the internal network. For SaaS, you can use the AirWatch Cloud Connector to securely connect Workspace ONE UEM to your CA.

- 1 The device enrolls with Workspace ONE UEM.
- 2 Workspace ONE UEM sends a request to the CA to issue a certificate for the enrolled device using domain credentials.
- 3 The CA issues a certificate for the enrolled device.
- 4 The CA sends the device's certificate to Workspace ONE UEM.
- 5 Workspace ONE UEM generates a configuration profile for the enrolled device and attaches the certificate to the profile.
- 6 Workspace ONE UEM sends the configuration profile and the certificate to the enrolled device.

Device to CA with UEM as Delegate

Workspace ONE UEM can act as a delegate between the device and the CA, sending certificate transactions between the device and the CA over NDES/SCEP. This integration with NDES/SCEP and the device positions Workspace ONE UEM to never come in contact with the device certificate. Workspace ONE UEM only acts as a delegate so that the device receives its certificate from the CA.

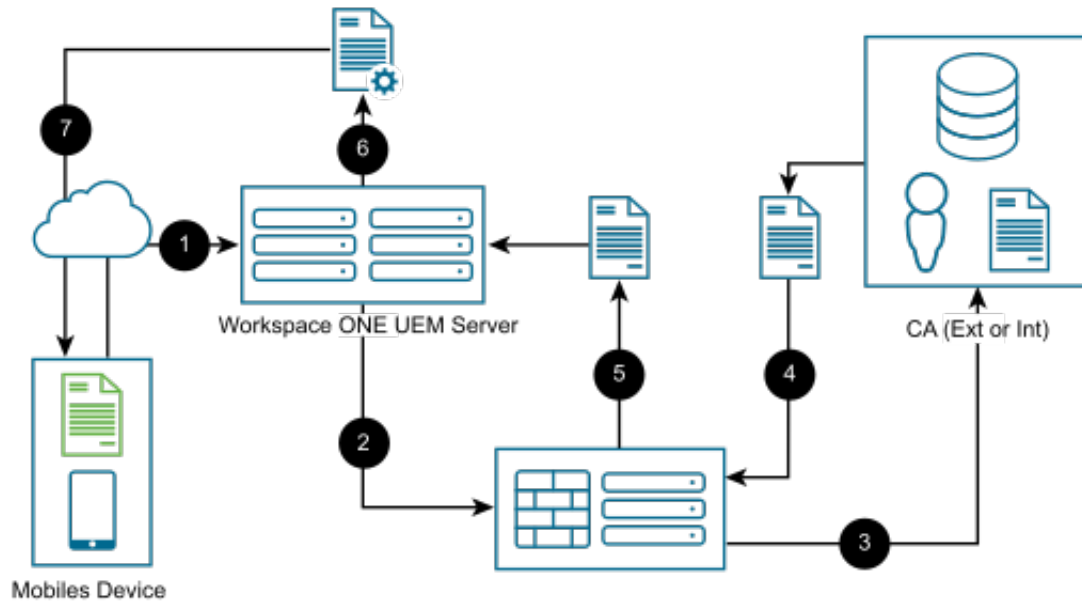


This is the typical NDES/SCEP configuration currently found in most existing implementations that include Wi-Fi access points, routers, and other network equipment. In this scenario, Workspace ONE UEM is not given the responsibility of managing the device certificate. Also, the token is transmitted to the device over the Internet so there is an added risk that an unauthorized person can intercept the certificate.

- 1 The device enrolls with Workspace ONE UEM.
- 2 Workspace ONE UEM sends information using NDES/SCEP to the device.
- 3 The NDES/SCEP server authorizes approval and sends Workspace ONE UEM a token for the enrolled device.
- 4 Workspace ONE UEM notifies the enrolled device about the approval, the token, and server information.
- 5 The enrolled device communicates directly with the NDES/SCEP server because it has approval.
- 6 The NDES/SCEP server requests that the CA generates a certificate for the enrolled device.
- 7 The CA generates a certificate and returns it to the NDES/SCEP server.
- 8 The NDES/SCEP service sends the certificate to the device.

Workspace ONE UEM SCEP Proxy Between Device and CA

If you do not want to expose your NDES/SCEP endpoints to external devices, you can use the Workspace ONE UEM SCEP Proxy. The SCEP Proxy allows Workspace ONE UEM to act as an intermediary between the NDES/SCEP server and the device. It forwards and returns requests and responses between the two components. Workspace ONE UEM does not have the NDES/SCEP server's private key, so it cannot parse requests from devices.



For on-premises, Workspace ONE UEM can proxy to a CA on the same or different domains. For SaaS, use the AirWatch Cloud Connector to securely connect Workspace ONE UEM to your CA.

- 1 The device enrolls with Workspace ONE UEM.
- 2 Workspace ONE UEM sends information to the NDES/SCEP server to request that the CA issue a certificate to the enrolled device.
- 3 The NDES/SCEP service requests that the CA generate a certificate for the enrolled device.
- 4 The CA generates a certificate and sends it to the NDES/SCEP service.
- 5 The NDES/SCEP server receives the certificate and sends it to Workspace ONE UEM.
- 6 Workspace ONE UEM generates a configuration profile for the enrolled device and attaches the certificate to the profile.
- 7 Workspace ONE UEM sends the configuration profile and the certificate to the enrolled device.

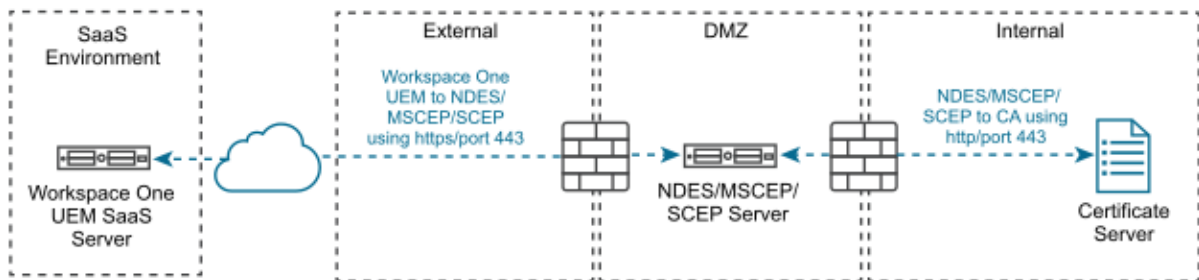
NDES for SCEP

2

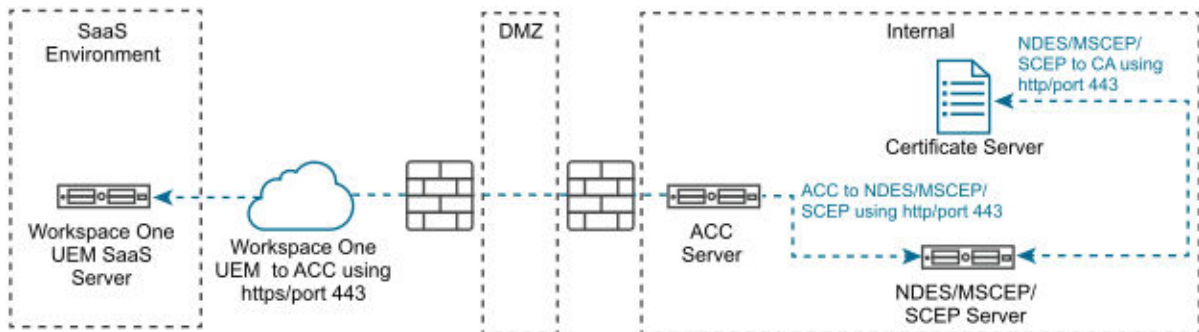
Install and set up the Microsoft certificate authority (CA) over the NDES for SCEP protocol for integration with Workspace ONE UEM.

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. See sample CA Configurations for Workspace ONE UEM SaaS environments. Configurations differ in on-premises environments.

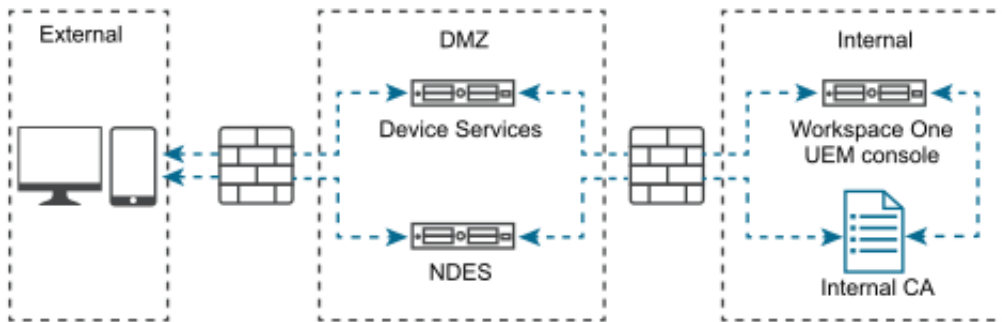
- Workspace ONE UEM to NDES/SCEP and then to Certificate Authority



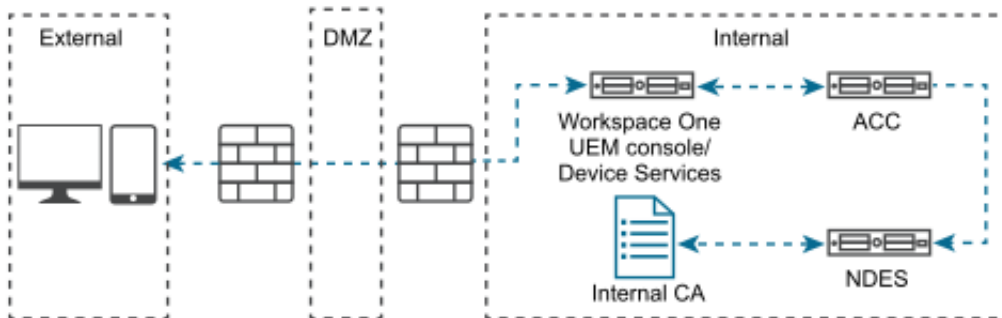
- Workspace ONE UEM to AirWatch Cloud Connector, then to NDES/SCEP, and then to Certificate Authority



- On-premises DS and NDES in the DMZ with Internal Workspace ONE UEM and CA

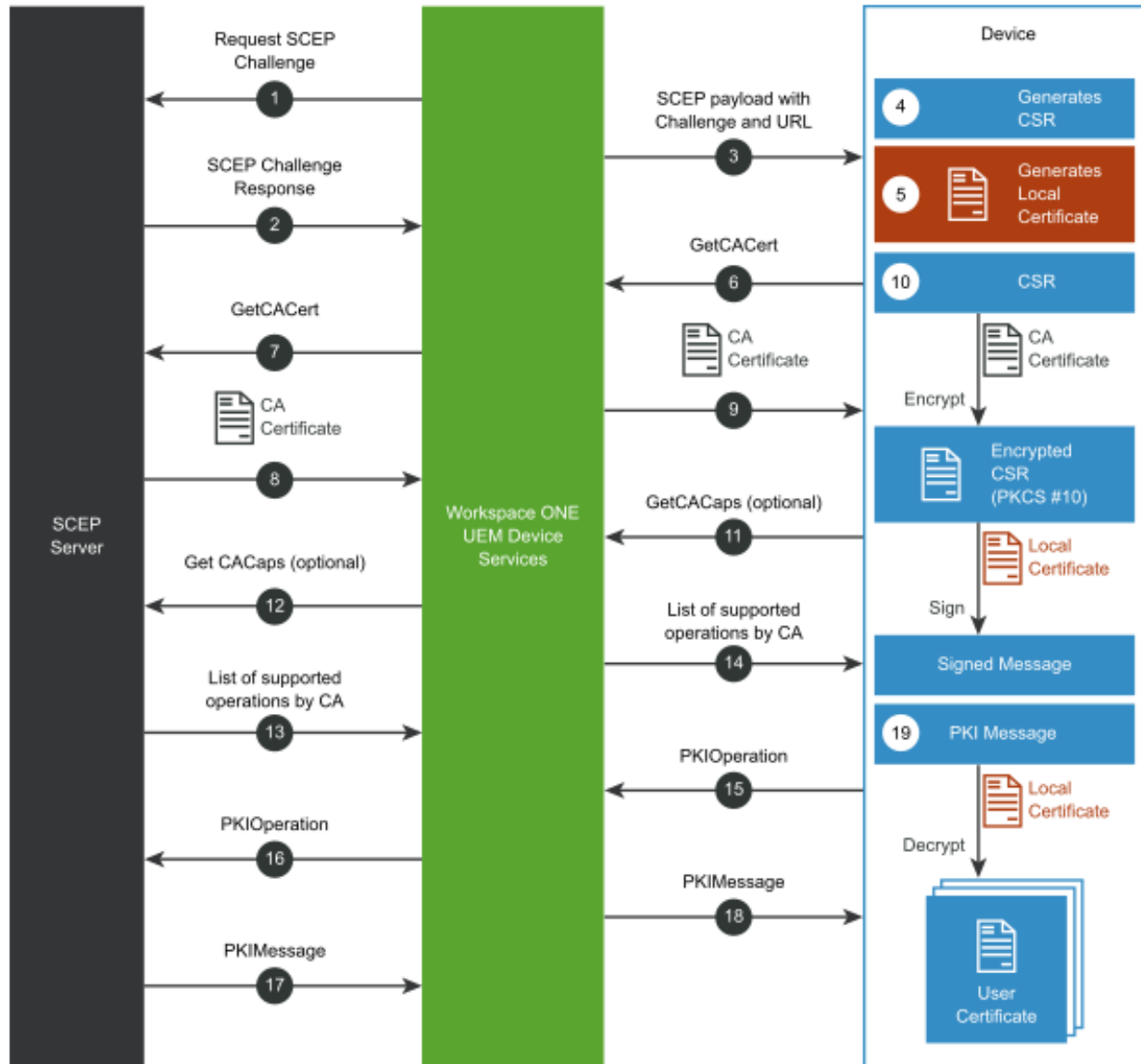


■ On-premises with All Servers Internal and SCEP Proxy



If you do not want to expose your SCEP endpoints to external devices, you can use the SCEP Proxy. This feature, **Enable Proxy**, is an advanced feature when you configure the CA in the Workspace ONE UEM console. The SCEP Proxy allows Workspace ONE UEM to act as an intermediary between the SCEP server and the device. It forwards and returns requests and responses between the two components. Workspace ONE UEM does not have the SCEP server's private key, so it cannot parse requests from devices.

Traffic flows in the following sequence.



- 1 Workspace ONE UEM Device Services (where the SCEP Proxy is located) requests a SCEP challenge from the CA's SCEP server.
- 2 The CA responds with a SCEP challenge phrase.
- 3 Device Services builds the SCEP payload and sends it to the device. The payload contains the SCEP challenge phrase, the SCEP URL, and other attributes (for example, Subject Name, Key Usage, and SAN). The SCEP URL has the SCEP enrollment token that is associated with the CA and certificate template.
- 4 The device receives the SCEP payload and it generates a certificate signing request (CSR) based on all the attributes in the payload.
- 5 The device generates a local certificate with a private key.
- 6 The device sends a GetCACert request to the Workspace ONE UEM SCEP Proxy.

- 7 The Workspace ONE UEM SCEP Proxy resolves the GUID to the CA's SCEP endpoint and forwards the request to the respective SCEP endpoint.
- 8 The CA responds with a CA certificate to the Workspace ONE UEM SCEP Proxy.
- 9 The Workspace ONE UEM SCEP Proxy forwards the CA certificate to the device.
- 10 The CA certificate encrypts the CSR the device generated. The local device certificate signs the encrypted CSR to build a signed message.
- 11 Optionally, the device sends a GetCACaps request to the Workspace ONE UEM SCEP Proxy.
- 12 The Workspace ONE UEM SCEP Proxy forwards the request to the CA's SCEP endpoint.
- 13 If the CA supports the GetCACaps request, the CA returns a list of all the supported operations to the Workspace ONE UEM SCEP Proxy.
- 14 The Workspace ONE UEM SCEP Proxy forwards the list of supported operations to the device.
- 15 The device sends a PKIOperation request to the Workspace ONE UEM SCEP Proxy. The request includes the generated signed message.
- 16 The Workspace ONE UEM SCEP Proxy validates that the SCEP enrollment token is compliant and enrolled with Workspace ONE UEM. If the validation is successful, it forwards the request to the CA SCEP endpoint.
- 17 If the PKIOperation is valid, the CA responds with PKIMessage that contains the user certificate.
- 18 The Workspace ONE UEM SCEP Proxy sends the response to the device.
- 19 The CA certificate signs the PKIMessage, it decrypts it using the local device certificate, and it installs the user certificate on the device.

This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)

Prerequisites

Meet the list requirements to configure the protocol.

- NDES is available in the Enterprise version of Microsoft Server 2008, 2008 R2, and 2012 or 2016 Standard and Enterprise.
- A Certificate Authority (CA) installed, configured, and made available to the NDES/SCEP/MSCEP server.
 - You can install the CA and NDES for SCEP on the same server or on different servers. If you do put them both on the same server, complete the CA installation first and restart the server before installing NDES for SCEP.
- You need certificate templates during NDES for SCEP setup and service certificate renewal:
 - Exchange Enrollment Agent (Offline request)

- CEP Encryption

Note: It is possible for all the following accounts to be the same account. However, using a single account has security concerns.

Connection Requirements

- The SCEP endpoint must be accessible from the device in order for certificate enrollment to finish. * The exception to this requirement is when you use the **Enable Proxy** menu item in the **Certificate Authority - Add/Edit** page for non-generic, SCEP protocol use.
- 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 the NDES for SCEP service certificate templates (Enterprise).
- A **Service Account** must exist. It is used by the NDES for SCEP application pool and must meet the following requirements.
 - Member of the local IIS_USRS group. If this setting is not configured, role installation fails.
 - 'Request' permission on the configured CA. 'Read' and 'Enroll' permissions on configured device certificate templates.
 - A Service Principal Name (SPN) must be added by using: `SetSpn -a HTTP/<ComputerName><AccountName>`.
- <ComputerName> is the name of the computer where NDES for SCEP 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 for SCEP must meet the following requirements.
 - 'Enroll' permissions on all configured device certificate templates (Enterprise).
 - Member of the Local Administrator group (standalone).

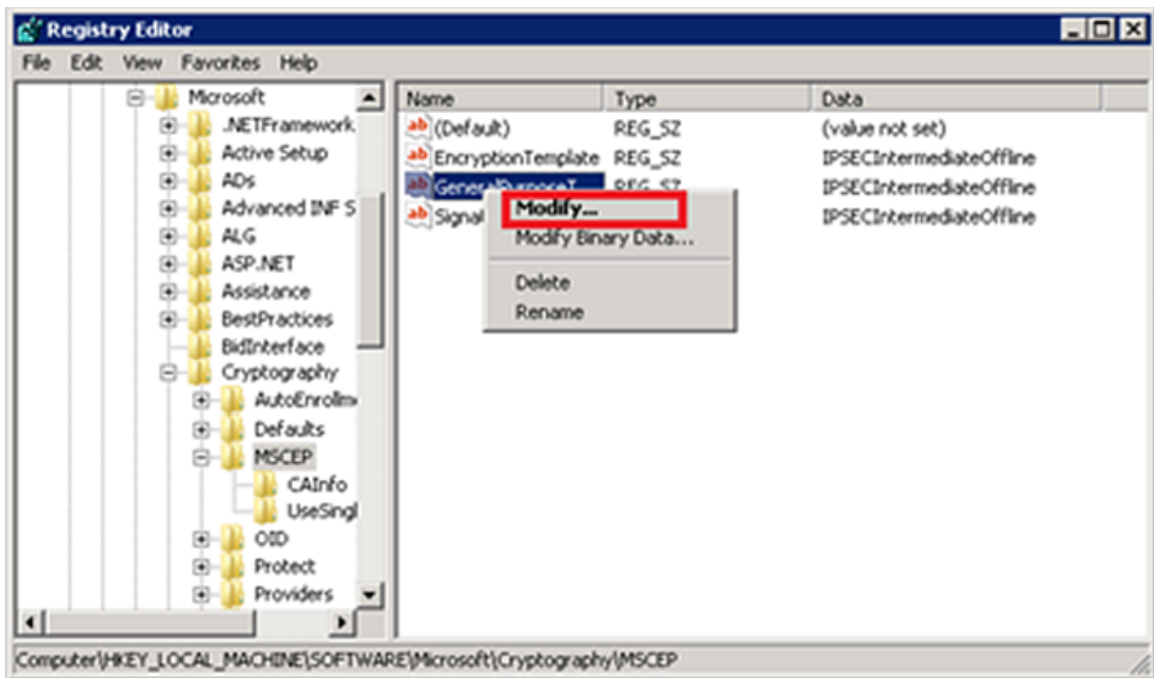
Procedure

- 1 Install the Microsoft CA role.
 - a Add the ADCS role.
 - 1 Click the **Server Manager** icon next to **Start** 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** check box.

- 5 Click **Next**.
- 6 Select the **Certification Authority** check box and then select **Next**.
- 7 Select **Enterprise** and then select **Next**.
- 8 Select **Root CA** and then select **Next**.
- b 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**. Note the name of the CA server. You must 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.
- c 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**.
- 2 Set permissions for the NDES/SCEP Admin Account.
 - a Run the **Certification Authority Console** from the **Administrative Tools** in Windows.
 - b Right-click the server name and select **Properties**.
 - c Select the **Security** tab.
 - d Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog box displays.
 - e Click within the **Enter the object names to select** text box and type the name of the SCEP Admin Account.
 - f Click **OK**. The CA Properties dialog box displays.
 - g Select the SCEP Admin Account from the **Group or user names** list.
 - h Select the **Manage CA** permission **Allow** check box.

- i Select the **Request Certificates** permission **Allow** check box.
 - j Click **OK**.
- 3 Set the **Read** and **Enroll** permissions on the certificate template for the NDES/SCEP Service Account and the Device Administrator.
- a Run the **Certificate Templates Console** by running `certtmpl.msc` from the Windows Desktop.
 - b Right-click the required template and select **Properties**. The example here is 'MobileUser' from the CA Setup Document.
 - c Select the **Security** tab.
 - d Click **Add**. The **Select Users, Computers, Service Accounts, or Groups** dialog box displays.
 - e Click within the **Enter the object names to select** text box and type the name of the Service Account.
 - f Click **OK**. The **Properties** dialog box displays.
 - g Select the Service Account from the **Group or user names:** list.
 - h Select the **Read** permission **Allow** check box.
 - i Select the **Enroll** permission **Allow** check box.
 - j Click **OK**.
- 4 Install the NDES/SCEP role.
- a Run the **Server Manager** on the server to be used as the NDES/SCEP/MSCEP server.
 - b Select **Roles**.
 - c Click **Add Roles**. The **Add Roles Wizard** displays.
 - d Click **Next**. The **Select Server Roles** dialog box displays.
 - e Select **Active Directory Certificate Services**.
 - f Click **Next**. The **Select Role Services** dialog box displays.
 - g Clear the **Certification Authority** check box.
 - h Select **Network Device Enrollment Service** (or SCEP).
 - i Click **Next**.
 - j Click **Select User**. The user selected MUST be in the local IIS_USRS Group.
 - k Enter the Username and Password for the account NDES/SCEP Admin Account.
 - l Click **Next**. The **Specify CA for Network Device Enrollment Service** (or SCEP) dialog box displays.
 - m Select **CA Name**.

- n Click **Browse**.
 - o Select the CA in the **Select Certification Authority** dialog box.
 - p Click **OK**.
 - q In the **Specify Registration Authority** dialog box, select **Next**.
 - r In the **Configure Cryptography for Registration Authority** dialog box, select **Next**.
 - s Navigate through any additional required services or roles and then select **Install** and **Next**.
- 5 Specify the NDES/SCEP template. NDES/SCEP uses one template from the certificate authority. This template is specified in the registry and must be edited using **Registry Editor**.
- a Run the **Registry Editor** by running `regedit.exe` from the Windows Desktop.
 - b Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP` (or NDES/SCEP).
 - c Right-click the **General Purpose Template** and select **Modify**.
 - d Replace the value `IPSECIntermediateOffline` with the template name being used.



- e Close the Registry Editor.
 - f Restart Internet Information Services by opening a command prompt and running `iisreset`.
- 6 Configure IIS to allow for large query strings. When the device requests a certificate from NDES/SCEP, 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 results in a 404.15 error. The default query string length must be increased to accommodate this large string.
- a Open a command prompt from the Windows Desktop.

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

7 Configure the CA and the certificate template in Workspace ONE UEM so that Workspace ONE UEM can retrieve a certificate from a CA.

a 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:
 - a Select 'Microsoft AD CS' from the **Authority Type** drop-down menu. Configure this setting first, because dependent settings appear.
 - b Enter the **Name** and **Description** of the new certificate authority.
 - c Select the **Protocol**: AD CS or SCEP.
 - d Select the **Version**: NDES 2008/2012 or SCEP 2003.
 - e Enter the URL of the CA server in the SCEP URL field. Note: The URL for NDES must follow the format `http:///certsrv/mscep/mscep.dll`

Select the **Challenge Type** that reflects whether a challenge phrase is required for authentication.

- a 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.
- b 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.

Finish the **SCEP Challenge URL** text box with a URL in the following format:

`http://host/certsrv/mscep_admin/.`

Advanced Options

- a Enter the **SCEP Challenge Length**, which represents the number of characters in the challenge password.

- b Enter the **Retry Timeout**, which is the time the system waits between retries.
 - 1 For Windows 10 devices, this should be a non-zero value.
- c Enter the **Max Retries When Pending**, which is the maximum number of retries the system allows while the authority is pending.
- d With **Enable Proxy** selected, 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.

Click **Save**.

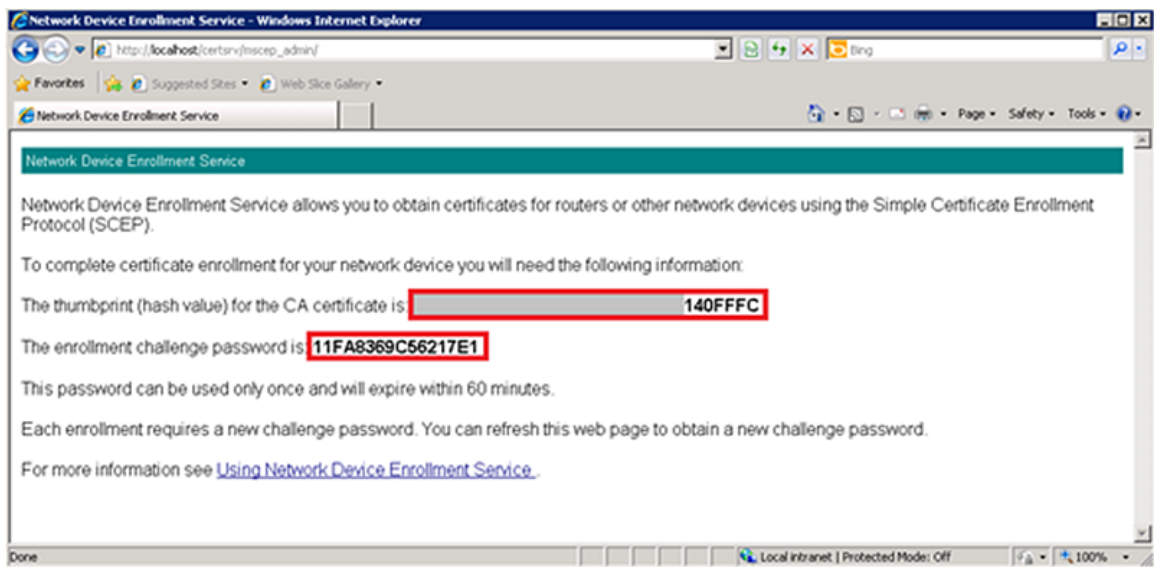
Configure the certificate template.

- 1 Click the **Request Templates** tab.
- 2 Click **Add**.
- 3 Enter the following details about the template in the remaining text boxes:
 - a Enter the template **Name** and **Description**.
 - b Select the certificate authority that was created from the **Certificate Authority** drop-down box.
 - c Enter the distinguished name in the **Subject Name** text box. The text entered in this text box becomes the Subject of the certificate, which lets the network administrator determine which devices receive the certificate. A typical entry in this text box is “CN={EnrollmentUser}” or “CN={DeviceUid}” where the {} text boxes are Workspace ONE UEM lookup values.
 - d Select the private key length from the Private Key Length drop-down menu. This value is typically 2048 matches the setting on the certificate template that is being used by NDES/SCEP.
 - e Select the applicable **Private Key Type**. This value can be **Signing**, **Encryption**, or both, and the value matches the certificate template being used by NDES/SCEP.
 - f You can optionally select any of the following:
 - 1 If Workspace ONE UEM renews the certificate when it expires, select **Automatic Certificate Renewal** and make sure the assignment is set to **Auto**. Enter the number of days before expiration that Workspace ONE UEM automatically reissues a certificate to the device in the **Auto Renewal Period (days)** text box .
 - 2 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**.

- 3 Click **Add** to the right of **Eku Attributes** to insert an object identifier (OID) that represents any additional extended key usages that might be required. You can add multiple **Eku Attributes** to fit your needs.
 - a The Eku Attribute is required for Windows 10 devices.
 - 4 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**.

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

- 1 Open a web browser and navigate to `http://<servername>/certsrv/mscep_admin/` where `<servername>` is the name of the server running NDES/SCEP. If confirmation and testing are being run from the NDES/SCEP server, the `<servername>` can be "localhost".
- 2 Enter the NDES/SCEP Service Account user name 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.



What to do next

Review some tips and troubleshooting steps for the integration.

- configuring the certificate password settings, use the default setting (dynamic password mode).
- Although Workspace ONE UEM supports the use of the registry setting for Single Password mode, consider not using it. The "Single Password" mode sets a static challenge password all devices can use which can expose security vulnerabilities.

- If the NDES/SCEP challenge cache is full, (an issue which can 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 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 Workspace ONE UEM console matches the length setting associated with the certificate.

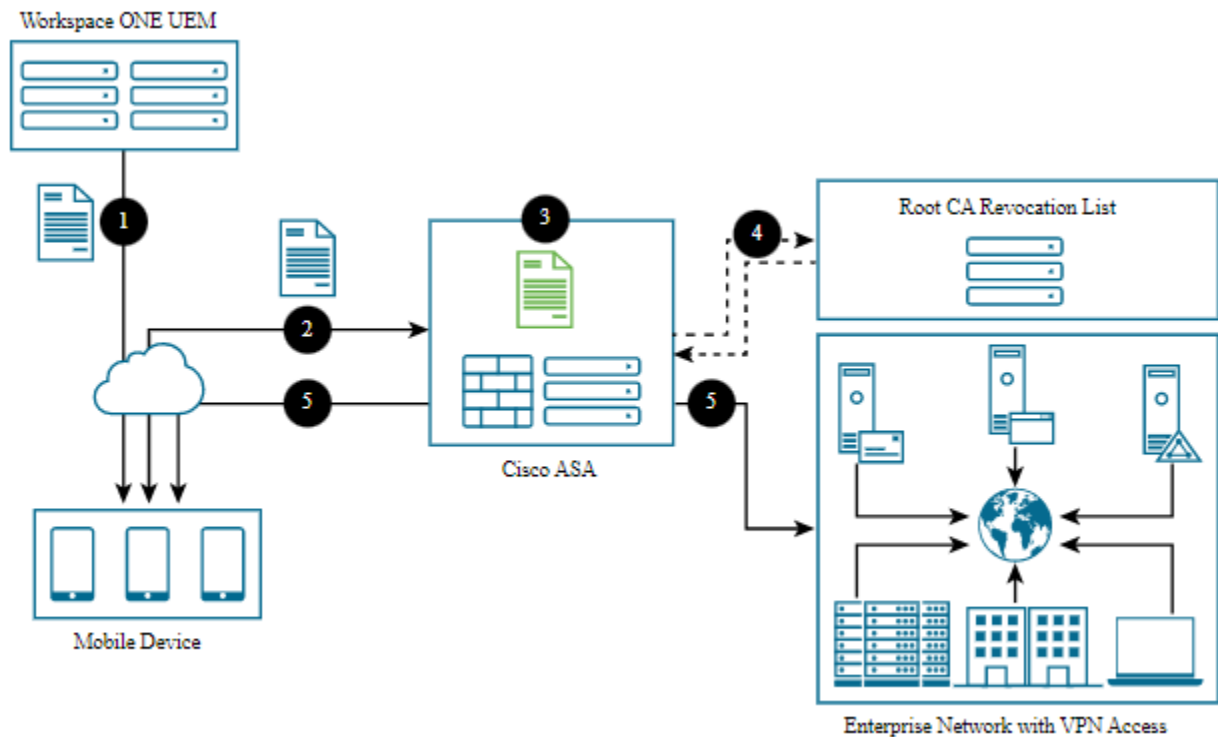
Cisco IPsec VPN

3

Configure Workspace ONE UEM so that managed Apple and select Android devices can connect to an enterprise network through Cisco IPsec using a certificate for authentication.

Certificate authentication is handled from the point where the user's device enrolls into Workspace ONE UEM to when the user has VPN access to the protected enterprise network.

- 1 After the device enrolls, Workspace ONE UEM sends the device a profile that contains the user's identity certificate and Cisco IPsec VPN configuration settings.
- 2 When the device uses VPN, the device sends the identity certificate to ASA's VPN endpoint for authentication.
- 3 ASA verifies that the device identity certificate came from the same CA as its own identity certificate and both were signed with the CA's certificate.
- 4 Optionally, if CRL Checking is enabled, the ASA regularly receives, parses, and caches the CA's CRL to validate the device identity certificate has not been revoked.
- 5 ASA grants the device VPN access. The device can now securely access internal enterprise resources.



This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)
- [What to do next](#)

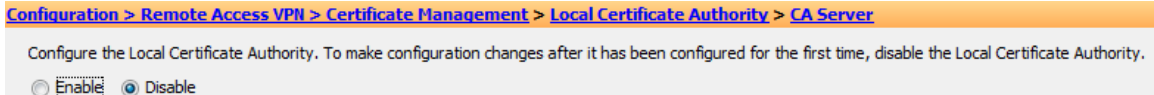
Prerequisites

- Use an external CA server. The CA must be an external Enterprise CA as opposed to a standalone CA. A standalone CAs do not allow for the configuration and customization of templates.
- For IPSec, you must have a Cisco Adaptive Security Appliance (ASA) connected to your network.

Procedure

- 1 Disable the local CA on the ASA firewall to ensure that certificates are authenticated against the external CA.
 - a Log into the Cisco Adaptive Security Device Manager (ASDM) to configure your ASA firewall.
 - b Navigate to **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**.

- c Select **Disable**.



- d Select **OK**.

2 Configure IPsec VPN.

- a Create a CSR on the ASA firewall and send it to the external CA. This is because the ASA needs an Identity Certificate signed by the external CA. For assistance, follow Cisco's instructions for Generating a CSR on the ASA firewall. After you have completed all the steps, a CER file (for example, cert_client_id.cer) downloads to your local machine that was obtained from the external CA.
- b Download the certificate from the external CA and install it on the ASA firewall to authenticate that the external CA is a trusted source. Follow Cisco's instructions on how to install the external CA's certificate.
- c Configure the IKE policies, tunnel properties and policies, group policies, available VPN client IP addresses (pool), user accounts and group assignments, and associate these configurations to create an IPsec profile used by the VPN clients. Visit the Cisco website for instructions on creating a remote access connection profile and tunnel group on the ASA for IPsec VPN clients. Complete the steps necessary to configure the external CA and ASA firewall to create a trust using certificates and configure a remote access connection profile and tunnel group so that IPsec VPN certificate authentication can be used by your VPN clients to gain access into your enterprise network.

3 Integrate Workspace ONE UEM with the external CA so that Workspace ONE UEM can request and deploy Identity Certificates. Configure the CA and the request template in the Workspace ONE UEM console.

- a Configure the CA.
 - 1 Log in to the Workspace ONE UEM console as a user with Workspace ONE UEM Administrator privileges, at minimum.
 - 2 Navigate to **Devices > Certificates > Certificate Authorities**.
 - 3 Select **Add** and complete the settings.

Setting	Description
Authority Type	Microsoft ADCS
Protocol	ADCS If you select SCEP, then there are different text boxes and selections available not covered by this documentation.
Server Hostname	Enter the host name of the CA server.

Setting	Description
Authority Name	Enter the actual CA name. This value is the name of the CA to which the AD CS endpoint is connected. This value can be found by launching the Certification Authority application on the CA server.
Authentication	Select Service Account so the device user enters credentials.
User name	This value is the user name of the AD CS Admin Account which has sufficient access to allow Workspace ONE UEM to request and issue certificates.
Password	This value is the password of the AD CS Admin Account which has sufficient access to allow Workspace ONE UEM to request and issue certificates.
Additional Options	None

4 Select **Save**.

- 4 Deploy a device profile from Workspace ONE UEM console with IPsec VPN and Certificate payloads to devices. This device profile deploys an Identity Certificate and IPsec VPN settings to configure all assigned devices.
 - a Navigate to **Devices > Profiles > List View** from the Workspace ONE UEM console main menu.
 - b Select **Add**.
 - c Select the applicable device platform to open the **Add a New Profile** screen.
 - d Configure the **General** settings for the profile. The **General** settings determine how the profile is deployed and who receives it and other overall settings.
 - e Select **Credentials** from the profile options at left and then select **Configure**.
 - f Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.
 - g Select the external CA created previously from the **Certificate Authority** drop-down menu.
 - h Select the certificate template created previously from the **Certificate Template** drop-down menu.
 - i Select **VPN** from the profile options at left and then select **Configure**. Credentials profile settings must be configured before the VPN profile settings because the VPN configuration refers to the credential that was just configure. Also, some of the configuration settings described here are not applicable to all device platforms.
 - j Configure the following VPN profile settings.

Setting	Description
Connection Type	IPSec (Cisco)
Connection Name	Enter a name that helps identify this specific VPN.
Server	Enter the URL that users connect to for establishing their VPN connection.

Setting	Description
Account	If your VPN has been configured to apply user credentials in addition to a certificate for authentication, then specify an account to pass to the VPN endpoint. To pass Workspace ONE UEM User Account names to the VPN endpoint, use the {EnrollmentUser} lookup value.
Machine Authentication	Certificate
Identity Certificate	Select the credential configured for the certificate.
Include User PIN	Ensure this is not selected. Unselect this option.
Enable VPN On Demand	Ensure this is not selected. Unselect this option.

- k Select **Save** or **Save & Publish** to push the profile to a device.

What to do next

You can confirm that the VPN certificate is operational by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured ASA firewall. If the device is not connecting and shows a message that the certificate cannot be authenticated or the account cannot connect to the ASA firewall, then there is a problem in the configuration.

- Make sure that a certificate is being issued by the external CA to the device by checking the following information.
 - Go to the external CA's server, launch the certification authority application, and browse to the "issued certificates" section.
 - Find the last certificate that was issued and it should have a subject that matches the one created in the certificate template section earlier in this documentation. If there is no certificate then there is an issue with the external CA, client access server (e.g., ADCS), or with the Workspace ONE UEM connection to the client access server.
 - Check that the permissions of the client access server (e.g., ADCS) Admin Account are applied correctly to the external CA and the template on the external CA.
 - Check that the account information is entered correctly in the Workspace ONE UEM configuration.
- If the certificate is being issued, make sure that it is in the Profile payload and on the device.
 - Navigate to **Devices > Profiles > List View**. In the **Device Profiles** screen for the user's device, select **Actions** and then, select **</ > View XML** to view the profile XML. There is certificate information that appears as a large section of text in the payload.
 - On the device, go to the profiles list, select details and see if the certificate is present.
- If the certificate is on the device and contains the correct information, then the problem is most likely with the security settings on the ASA firewall. Confirm that the address of the VPN endpoint is correct in the Workspace ONE UEM profile and that all the security settings have been adjusted for allowing certificate authentication on the firewall.

- A very good test to run is to manually configure a single device to connect to IPSec VPN using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect to IPSec VPN with a certificate.

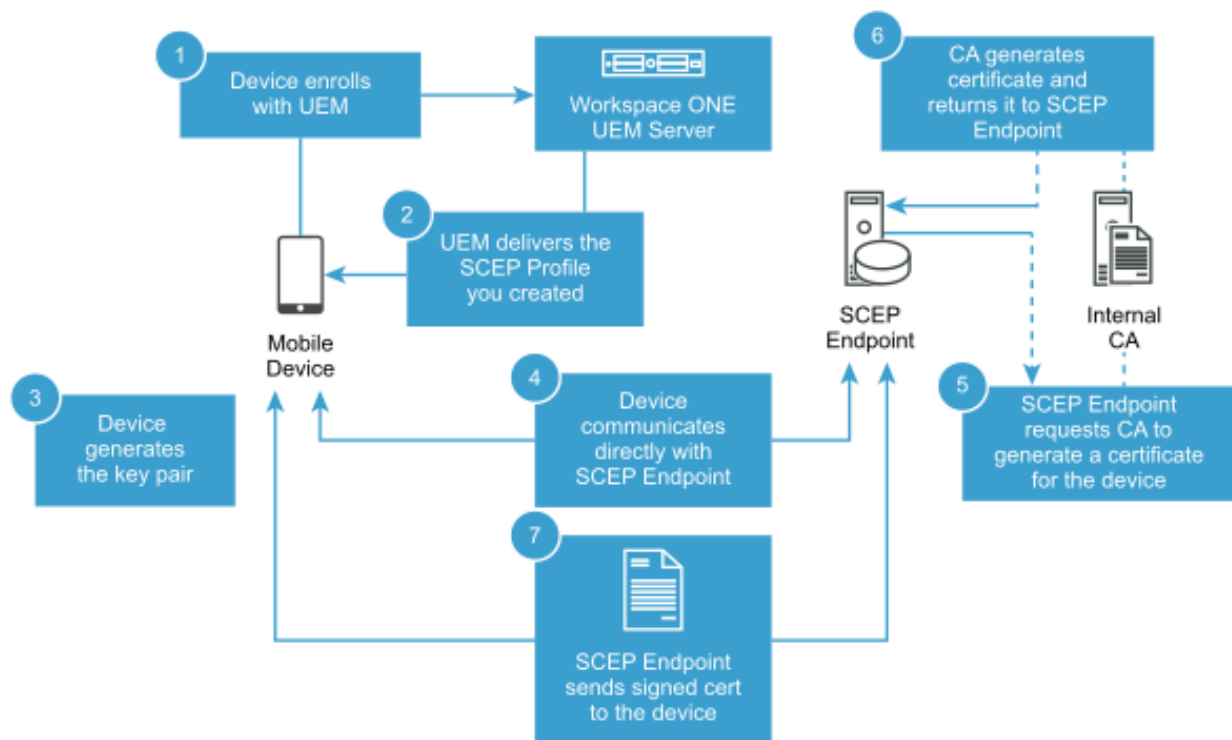
SCEP

4

Workspace ONE UEM supports SCEP (Simple Certificate Enrollment Protocol) for iOS and macOS devices. The integration includes the use of key pairs and the submission of the certificate signing request (CSR) that results in a signed certificate from the SCEP endpoint to devices.

If you're looking to leverage certificates as part of your mobile deployment, SCEP allows you to securely deploy certificate enrollment requests to iOS devices, even when Workspace ONE UEM does not natively support your PKI infrastructure of choice.

Workspace ONE UEM provisions the device with the parameters to generate the key pair and submit the CSR to the SCEP endpoint. The SCEP endpoint returns a signed certificate back to the mobile device. The device manages the certificate and its private key. The benefit to SCEP is that the private key never leaves the mobile device.



This chapter includes the following topics:

- Prerequisites

■ Procedure

Prerequisites

- Workspace ONE UEM 9.5 or later
- iOS 5.0 or later
- macOS 10.9 or later
- CA or SCEP endpoint must support SCEP as per the Internet Engineering Task Force's Simple Certificate Enrollment Protocol draft document.
- SCEP endpoint must be accessible from the device in order for the certificate enrollment to finish.
 - The exception to this requirement is when you use the Enable Proxy item in the Certificate Authority - Add/Edit page.

Note: Renewal and revoke are not supported.

Procedure

- 1 Configure the SCEP CA in the Workspace ONE UEM console.
 - a Navigate to Devices > Certificates > Certificate Authorities, and select Add.
 - b Select Generic SCEP from the Authority Type drop-down.
 - c Enter the information pertaining to your SCEP Endpoint.

Settings	Description
Name	The friendly name of your certificate authority in Workspace ONE UEM.
Description	An optional field that you can use to give details about this defined-CA and its uses.
Authority Type	The type of certificate authority being defined in Workspace ONE UEM.
SCEP Provider	The type of SCEP provider Workspace ONE UEM is integrating with. Basic is the only option supported currently. (This field cannot be changed.)
SCEP URL	The URL the device uses during certificate enrollment.
Challenge Type	Allows the admin to choose between static challenge and no challenge.
Static Challenge	If static challenge is selected, this is the necessary challenge the device must have in order to get its CSR signed by the CA.

- 1 Select **Save**.
- 2 Configure the request template in Workspace ONE UEM console.
 - a Navigate to **Devices > Certificates > Certificate Authorities**. Select the **Request Templates** tab. Select **Add**.

- b Enter the following information pertaining to your request template.

Settings	Description
Name	The friendly name given to the request template defined in Workspace ONE UEM.
Description	An optional field you can use to describe the details, usages, etc. of the request template.
Certificate Authority	The certificate authority you defined previously.
Subject Name	The subject given to device when it generates its key pair. Use the lookup value button to the left of the field for dynamic values.
Private Key Length	The length of the key pair to be generated.
Private Key Type	This tells the device what the private key is to be used for.

- c For **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 SCEP templates by default, and Workspace ONE UEM recommends that you use them.
- d Select **Save**.
- 3 Create a SCEP profile in the Workspace ONE UEM console. Define a certificate authority, then configure a Credentials payload alongside your EAS, Wi-Fi or VPN payload. Each of these payloads has settings for associating the certificate authority defined in the Credentials payload.
- a Navigate to **Devices > Profiles > List View > Add** and select **iOS** from the platform list.
- b Configure General profile settings as appropriate.
- c Select either an **EAS**, **Wi-Fi** or **VPN** payload to configure. Fill out the necessary information, depending on the payload you selected.
- d Select the **SCEP* payload and select your **SCEP Certificate Authority** and **Certificate Template** from the drop-down lists. Navigate back to the previous payload for EAS, Wi-Fi or VPN.
- e Specify the **Identity Certificate** in the payload.
- EAS – Select the Payload Certificate under Login Information.
 - Wi-Fi – Select a compatible Security Type (WEP Enterprise, WPA/WPA2 Enterprise or Any (Enterprise)) and select the Identity Certificate under Authentication.
 - VPN – Select a compatible Connection Type (for example, CISCO AnyConnect, F5 SSL) and select Certificate from the User Authentication drop-down. Select the Identity Certificate.

- f Select **Save and Publish** when you are done configuring any remaining settings.

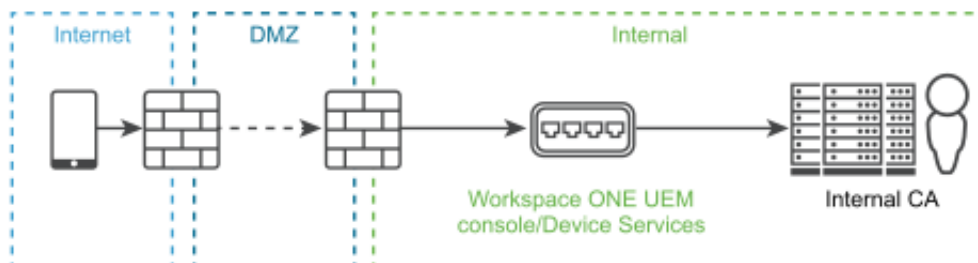
EOBO with AD CS via DCOM

5

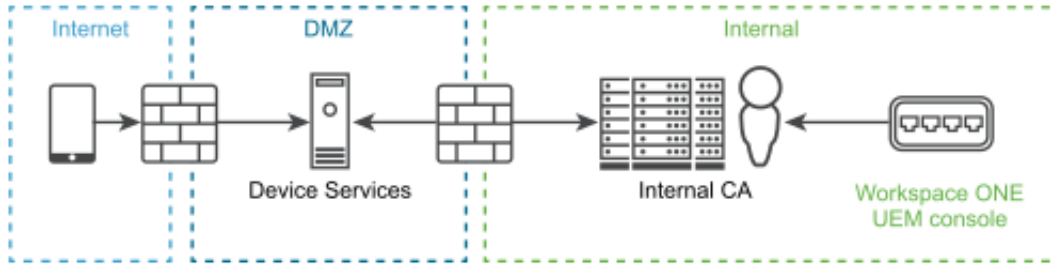
If you have a strong security policy for certificates and you want to use Microsoft's Certificate Enroll On Behalf of Others (EOBO) function, integrate an Enrollment Agent Signing Certificate with Workspace ONE UEM powered by AirWatch8. This process uses Active Directory Certificate Services (AD CS) by means of the Distributed Component Object Model (DCOM) remote protocol for integration. By default, only domain administrators are granted permission to request a certificate on behalf of another user. However, you can grant a user or computer account other than a domain administrator permission to become an enrollment agent. To be an enrollment agent, the user or computer account registers for an Enrollment Agent certificate.

Note: For integration with Workspace ONE UEM, the user is a computer account. After an agent has an Enrollment Agent certificate, that agent registers for a smart card certificate and generates a smart card on behalf of anyone in the organization. The smart card user can log on to the network and impersonate the real user. Because of the powerful capability of the Enrollment Agent certificate, it is best that your organization maintain very strong security policies for these certificates. For Workspace ONE UEM to use a certificate in a profile used to authenticate a user, set up an enterprise certificate authority (CA) in the domain in an on-premises environment. Additionally, you must join the CA to the same domain as VMware AirWatch Cloud Connector in order to successfully manage certificates within Workspace ONE UEM. There are several methods for Workspace ONE UEM to retrieve a certificate from the CA.

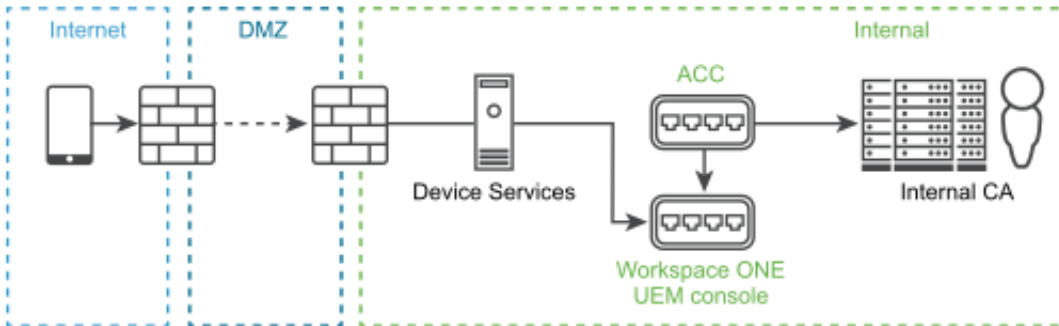
- On-Premises - Components are Internal with no VMware AirWatch Cloud Connector - In an on-premises environment, all Workspace ONE UEM application servers are internal and the VMware AirWatch Cloud Connector is not installed.



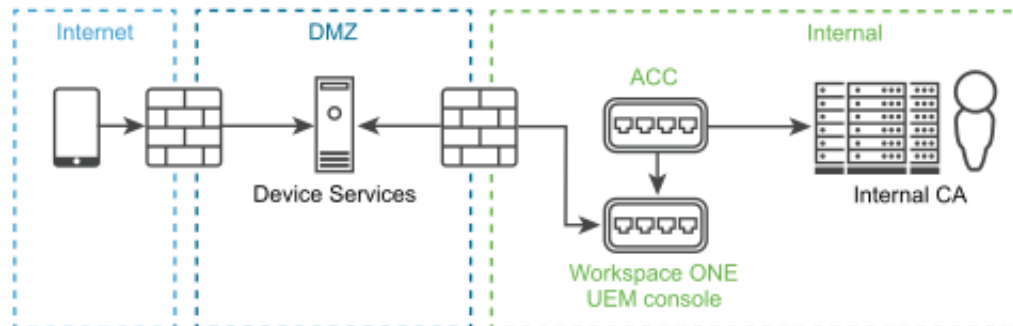
- On-Premises - Devices Services in a DMZ with no VMware AirWatch Cloud Connector - In an onpremises environment, Devices Services is located in a DMZ and the CA and Workspace ONE UEM servers are internal. The VMware AirWatch Cloud Connector is not installed.



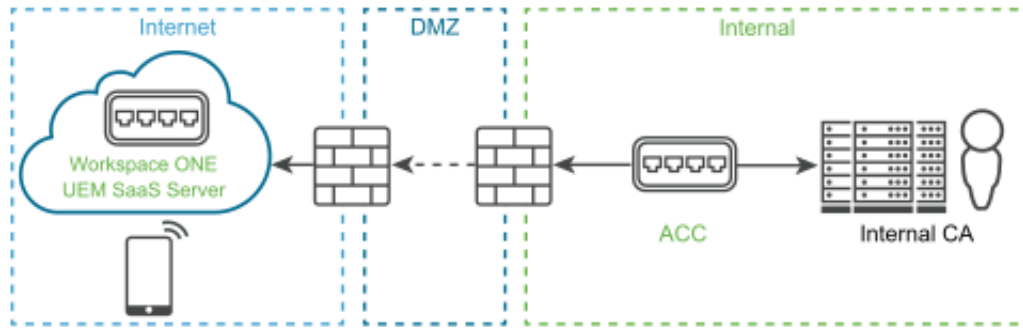
- On-Premises – Components are Internal with VMware AirWatch Cloud Connector - In an on-premises environment, Devices Services, Workspace ONE UEM server, the CA, and VMware AirWatch Cloud Connector are internal.



- On Premises - Device Services in a DMZ with VMware AirWatch Cloud Connector - In an onpremises environment, Devices Services is located in the DMZ and Workspace ONE UEM server, CA, and VMware AirWatch Cloud Connector are internal.



- SaaS – Components in the Cloud with VMware AirWatch Cloud Connector - In a SaaS environment, Devices Services, Workspace ONE UEM server, and the CA are in the cloud. The VMware AirWatch Cloud Connector and an internal CA are internal and must be in the same domain.



This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)
- [What to do next](#)

Prerequisites

- Use an on-premises Workspace ONE UEM environment.

Note: There is one scenario where a SaaS Workspace ONE UEM environment is supported.

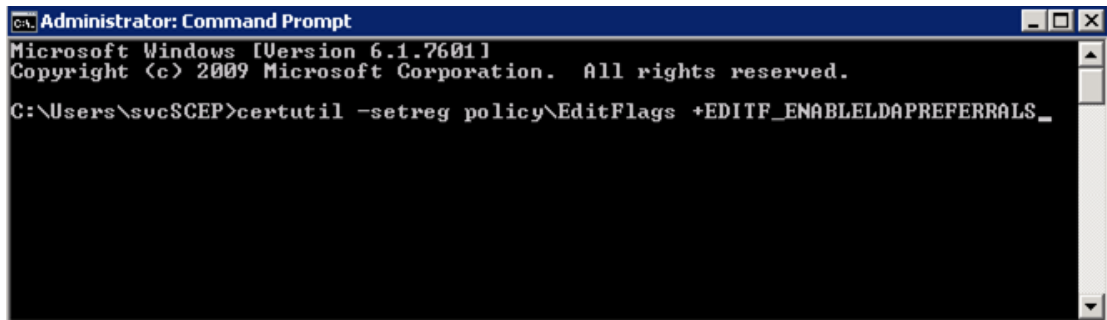
- The certificate authority used in certificate integration must be a member of the same domain as the Workspace ONE UEM application server to install the Enterprise CA.
- Use a service account with administrative access to the certificate authority server.
- Use Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016.
- The Workspace ONE UEM console server and the VMware AirWatch Cloud Connector server (if you are using it), must communicate to the Microsoft Certificate Authority over all configured DCOM ports.

Note: If using VMware AirWatch Cloud Connector, the VMware AirWatch Cloud Connector server must comply with the hardware sizing requirements mentioned in the [Workspace ONE UEM Recommended Architecture](#). Refer to the guidelines described for the Admin Console server.

- You can configure the port range to be any number of non-standard ports depending on your DCOM implementation. However, the listed ports are utilized by default.
- Port 135: Microsoft DCOM Service Control Manager.
- Ports 1025 - 5000: Default ports DCOM processes.
- Ports 49152 - 65535: Dynamic Ports.

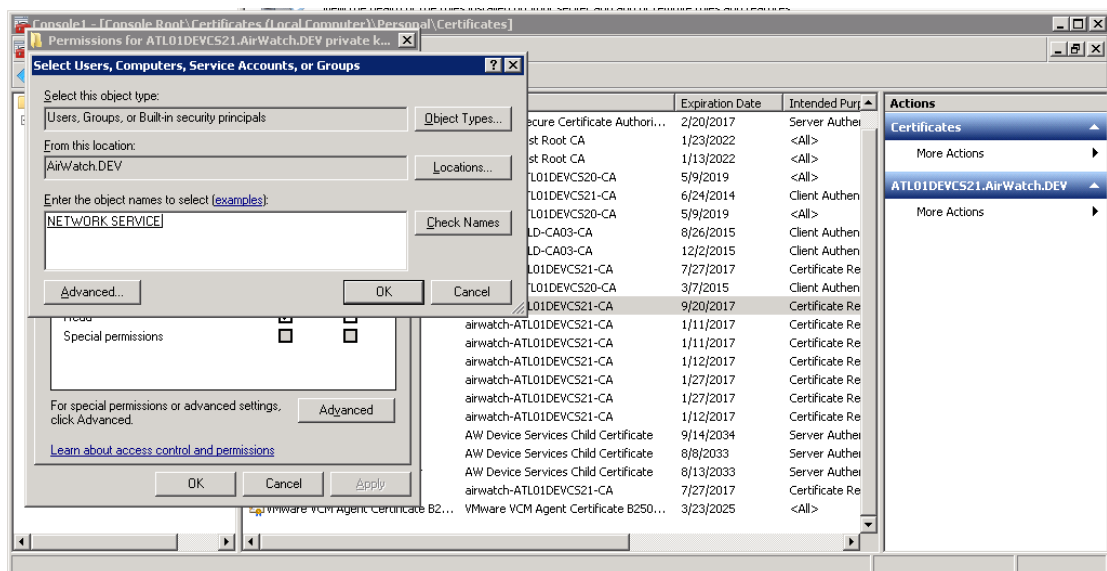
Procedure

- 1 Set up the restricted enrollment agent signing certificate on the CA server.
 - a Enable LDAP referrals. Active Directory Certificate Services (AD CS) Certificate Authority (CA) requires enabling LDAP referrals so that Workspace ONE UEM can request certificates on behalf of some other service account user.
 - 1 Stop certificate services by running the following command, `net stop certsvc`.
 - 2 Enable LDAP Referrals, `certutil -setreg policy\EditFlags +EDITF_ENABLELDAPREFERRALS`.



- 3 Start certificate services by running the following command, `net start certsvc`.
 - b Create a Restricted Enrollment Agent Certificate so you can generate a Restricted Enrollment Agent Signer Certificate.
 - 1 Open the **Certificate Authority (CA)**.
 - 2 Expand the CA Name, Right click **Certificate Templates**, and select **Manage**.
 - 3 Right click the **Enrollment Agent (Computer)** template and select **Duplicate Template**. Name it per your preference.
 - 4 Select your Windows Server version.
 - 5 On the **Request Handling** tab, select **Allow Private Key to be Exported**.
 - 6 On the **Subject Name** tab, make sure **Build from this Active Directory Information** is activated and **Subject Name format** is set to **Fully distinguished name**.
 - 7 On the **Security** tab, give the enrollment agent servers **Read** and **Enroll** permissions.
 - 8 Click **OK**.
 - 9 Navigate back to the **CA**, right click **Certificate Templates**, select **New**, and select **Certificate Template to Issue**.
 - 10 Select the duplicate copy of the template created in the previous step.
 - 11 Click **OK**.

- c Generate the Restricted Enrollment Agent Signer Certificate on any server that can connect to the Certificate Authority.
 - 1 Log in with a local admin account on the server when requesting the Enrollment Agent certificate on the ACC/DS/CN server.
 - 2 Open Microsoft Management Console, (MMC).
 - 3 Click **File** and select **Add/Remove Snap in**.
 - 4 Select **Certificates**.
 - 5 Select **Computer Account**.
 - 6 Select **Local Computer** and select **Finish**.
 - 7 Click **OK**.
 - 8 Expand **Certificates (Local Computer)**, double click **Personal**, right click **Certificates**, select **All Tasks**, and select **Request New Certificate**.
 - 9 Click **Next**.
 - 10 Select **Active Directory Enrollment Policy** and select **Next**.
 - 11 Check the duplicate template created in earlier steps and select **Enroll**.
 - 12 Once completed, select **Finish**.
- d Configure the certificate to make the private, if needed, and public keys using the network service.
 - 1 Right click the restricted enrollment agent signer certificate and select **All Tasks** followed by **Manage Private Keys**.
 - 2 Click **Add**.
 - 3 Type **Network Service** and select **Check Names**. Once added, select **OK** twice.



Another option to using the network service is adding the service account to manage the private keys. This option requires that the AirWatch Cloud Connector service logs on as the service account.

- e Depending on the need to install certificates on multiple servers, either export the public key or both the public and private keys.
 - If the certificate needs to be installed on multiple Device Services servers or VMware AirWatch Cloud Connector servers, export the public and the private key. When exporting the certificate to install on additional AirWatch Cloud Connector servers, the subject name is the name of the server the certificate was requested from (for example, requested from ACC1). Even though the subject name does not match the other servers you are importing the certificate to (for example, importing to ACC2 and ACC3), this disparity does not cause issues because the private key is also imported along with the certificate.
 - 1 Right click the issued certificate, select **All Tasks** followed by **Export**.
 - 2 Click **Next**.
 - 3 Select **Yes, export the private key** and select **Next**. Select **Include all certificates in the certification path if possible** as well as **Export all extended properties**. Click **Next**.
 - 4 Set a password and select **Next**.
 - 5 Select a folder in which to save the exported certificate.
 - 6 Click **Finish**.
 - If the certificate is installed on a single Device Services server or VMware AirWatch Cloud Connector server, export only the public key.
 - 1 Right click the issued certificate, select **All Tasks** followed by **Export**.
 - 2 Select **No, do not export the private key**, select **Next**.
 - 3 Select **DER encoded binary X.509 (.CER)**, select **Next**.
 - 4 Select a destination for the exported certificate and select **Next**.
 - 5 Click **Finish**.
 - 6 If you have other DS servers or VMware AirWatch Cloud Connector (ACC) servers, you must import the certificate that was exported in previous steps. Skip this section if you have no other DS or ACC servers.
- 7 Open Microsoft Management Console (MMC).
- 8 Click **File** and select **Add/Remove Snap in**.
- 9 Select **Certificates**.
- 10 Select **Computer Account** and select **Next**.
- 11 Select **Local Computer** and select **Finish**.
- 12 Click **OK**.

- 13 Expand **Certificates (Local Computer)** and select **Personal**. Right click **Certificates**, select **All Tasks** and select **Import...**
 - 14 Select the PFX file exported in previous steps and select **Next**.
 - 15 Enter the password created for this file in previous steps, make sure **Include all extended properties** is checked and select **Next**.
 - 16 Ensure **Place all certificate in the following store** is set to **Personal** and select **Next**.
 - 17 Click **Finish**.
- 2 Create a custom user template if you do not want to use the default Microsoft Certificate template to issue certificates to the end user. If using the default Microsoft Certificate template, consider using the template for client authentication certificates.
 - a On the CA server, under the **Certificate Authority Name**, right click **Certificate Templates** and select **Manage**.
 - b Right click a default template that is closest to your needs and select **Duplicate Template**.
 - c Select your Windows Server and select **OK**.
 - d Enter the **Template display name** and select **Apply**.
 - e Select the **Issuance Requirements** tab and select **This number of authorized signatures**. Under the **Application policy** drop-down field, select **Certificate Request Agent** and select **Apply**.
 - f On the **Subject Name** tab, select **Build from Active Directory Information**. Configure the name format as **Fully Distinguished Name** along with including the **Email** and **User Principal Name**. If you do not configure the subject name, the subject is blank and the certificate request fails.
 - g On the **Security** tab, give the service account **Read**, **Enroll**, and **Auto Enroll** permissions.
 - h Right click **Certificate Templates** under the CA name, select **New**, and select **Certificate Template to Issue**.
 - i Select the template that was just created and select **OK**.
 - 3 SaaS environments can configure the VMware AirWatch Cloud Connector to deploy Enrollment On Behalf Of (EOBO) with ADCS on Microsoft's Distributed Component Object Model (DCOM) substrate. If your Workspace ONE UEM deployment is strictly on-premises, you do not need to perform this step.
 - a On the VMware AirWatch Cloud Connector server, run services.msc.
 - b Stop the Cloud Connector service.
 - c Right-click the Cloud Connector service.
 - d Select **Properties**.
 - e Select the **Log On** tab.

- f Under **Log on as:**, choose **Local System account** and enable the check box **Allow Service to Interact with Desktop**.
 - g Click **OK** to save settings and close the **Properties** page.
- 4 Connect Workspace ONE UEM to the certificate authority and upload your public key to the console.
- a In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities > Certificate Authorities** tab and select **Add**.
 - b Complete required text boxes and make the listed configurations.

Option	Description
Authority Type	Select Microsoft AD CS .
User name	Enter the username and its corresponding password that has administrative access to the certificate authority server.
Additional Options	Select Restricted Enrollment Agent.

- c Upload the public key file (.cer) you exported when you set up the Restricted Enrollment Agent.
 - d Select **Save**.
- 5 Configure the request template in Workspace ONE UEM so that services in the console, like wifi, email, and VPN, can request secure communication with the configured certificate authority.
- a In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities > Request Templates** tab and select **Add**.
 - b Select the certificate authority you created previously. This step sets up the available options in the **Certificate Template - Add/Edit** window.
 - c Set the **Issuing Template** to either the default user template or the custom user template you configured earlier.
 - d Set the **Requester Name** to the lookup values **{EmailDomain}{EnrollmentUser}** for best results. Select user-specific lookup values. Device-specific lookup values are not supported.
 - e Click **Save**. You can stop here in the process unless you need to establish permissions on the VMware AirWatch Cloud Connector.

- 6 In some cases, steps used to configure the VMware AirWatch Cloud Connector may not be sufficient to establish the proper permissions required to log in to the server. Troubleshoot the permissions using a suggested method.
 - a Create a service account with full permissions. A service account runs the VMware AirWatch Cloud Connector servic5. Current service account permissions are subject to change if the permission levels can be successfully lowered.
 - 1 Add permissions for members of the following groups in Active Directory.
 - Domain Users
 - Enterprise Admins
 - Remote Desktop Users For example, the screen shot displays the permissions for the service account 'caadmin'.
 - 2 Configure permission on the certificate authority (CA) server.
 - Member of Local Administrator Group. For example, the screen shot displays Local Administrator Group permissions on the CA Server.
 - Full permissions on the Certification Authority. For example, the screen below displays the full compliment of available permissions for 'caadmin'.
 - b Use alternate VMware AirWatch Cloud Connector configuration.
 - 1 On the VMware AirWatch Cloud Connector server, run **services.msc**.
 - 2 Locate and stop the **Cloud Connector** service.
 - 3 Right-click the **Cloud Connector** service.
 - 4 Select **Properties**.
 - 5 Select the **Log On** tab.
 - 6 Under **Log on as:**, choose **This account** and **Browse** for the service account you created.
 - 7 Enter and confirm the password.
 - 8 Launch the Microsoft Management Console (mmc.exe) and open the personal certificate store of the local computer. Ensure you are logged in with an account that has admin permissions for both the VMware AirWatch Cloud Connector server and the domain, otherwise you may not be able to access MMC and also add a domain user to manager the private key.
 - 9 Select the Restricted Enrollment Agent.
 - 10 In MMC, right-click the Restricted Enrollment Certificate you added and select **All Tasks** and then **Manage Private Keys**.
 - 11 Add the service account and set read permissions.
 - 12 Click **OK** to save settings and close the **Properties** page.

- 13 Add the service account to both the VMware AirWatch Cloud Connector and the Secure Channel Certificates.
 - Both these certificates are issued by the **Device Services Child Certificate**.
 - They are issued to **AW Cloud Connector - VMware Enterprise Systems Connector** and **AW Cloud Connector -** .
- 14 From services.msc, manually start the **Cloud Connector** service.

What to do next

If you see one of these error messages, review some troubleshooting tips.

- The system cannot find the file specifie4. 0x80070002 (WIN32: 2) The REA signing certificate might not be present on the console/DS server's certificate stor5. You might have added it using your SSO AD user. These AD user-uploaded MMC certificates remain specific to that instance since they are not Network Admin users. Therefore, airwatchdev\svcscep (the network admin) cannot access the private key of REA certificate uploaded using awsso \shwethan.

When adding an REA signing certificate to MMC, make sure you log in as the network admin (airwatchdev\svcscep). Then add the signing certificate to the certificate store and give proper network service access to it so that other network admin users can also access it.

When you provide Service Account credentials on the CA configuration page in the Workspace ONE UEM console, the console/DS server performs a remote call to the server hostname using these service account credentials.

- Object reference not set to an instance of an object The CA server received the certificate request, but the policy module denied the request. The denial happens either because the LDAP forest referrals are not set (Step 1 of CA server), or because the user domain used is not correct or not associated with the CA server.

For Issued certificates on the CA server, only requests from the Airwatchdev domain are processe4. AWSSO domain requests are rejected (atl01devcs21 CA is synced only with Airwatchdev AD, not with AWSSO). Therefore, we changed the directory mapping on the LGs to Airwatchdev and users from this domain for enrolling devices. The profile lands on the device with the correct client certificate for REA.

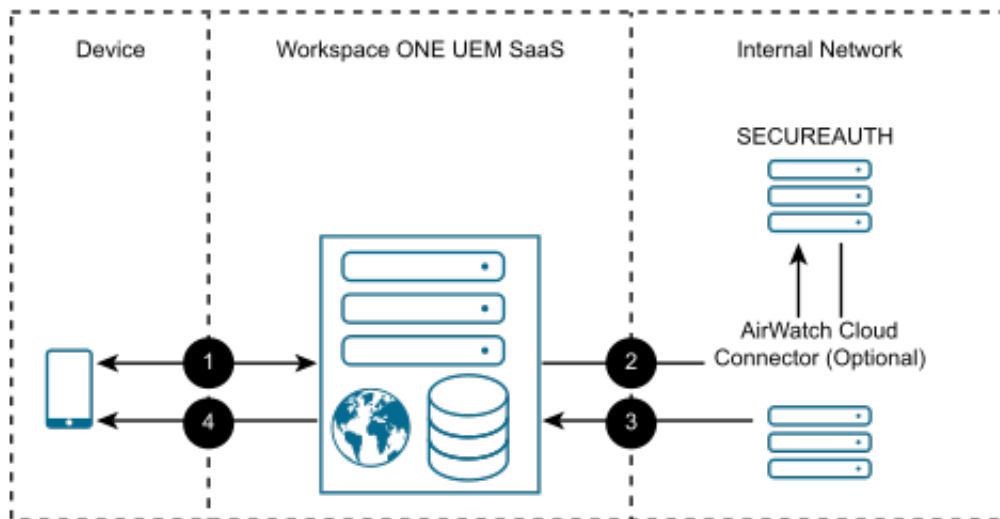
SecureAuth

6

Workspace ONE UEM is flexible with PKI integration by being able to request certificates from either internal or external certificate authorities (CA). Integrate with SecureAuth services to issue certificates for your Workspace ONE UEM MDM solution.

In order for Workspace ONE UEM to communicate with SecureAuth for certificate distribution, you must have a SecureAuth instance configured and ready to issue certificates. You can then configure Workspace ONE UEM to communicate with SecureAuth using basic authentication. Once communication is successfully established, you can define how to deploy certificates to devices. Below are some of the examples of how SecureAuth and Workspace ONE UEM can be deployed.

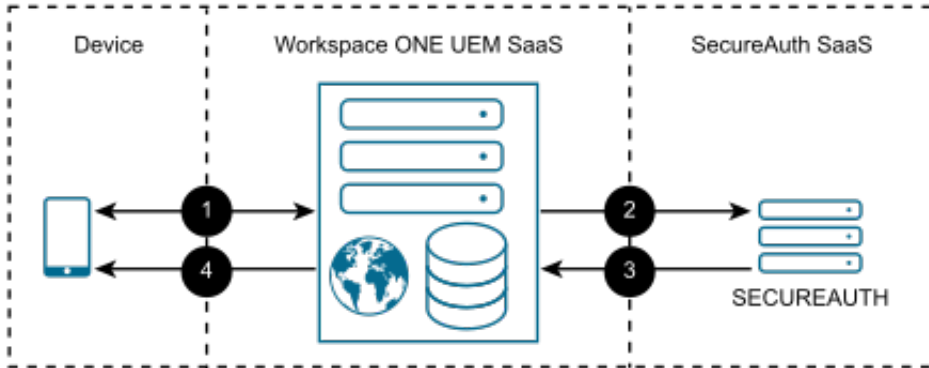
■ Workspace ONE UEM with SecureAuth Installed On-Premises



- Device enrolls with Workspace ONE UEM.
- Workspace ONE UEM requests a certificate from the SecureAuth endpoint (optionally through the AirWatch Cloud Connector).
- The SecureAuth endpoint delivers the certificate to Workspace ONE UEM (optionally through the AirWatch Cloud Connector).
- Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

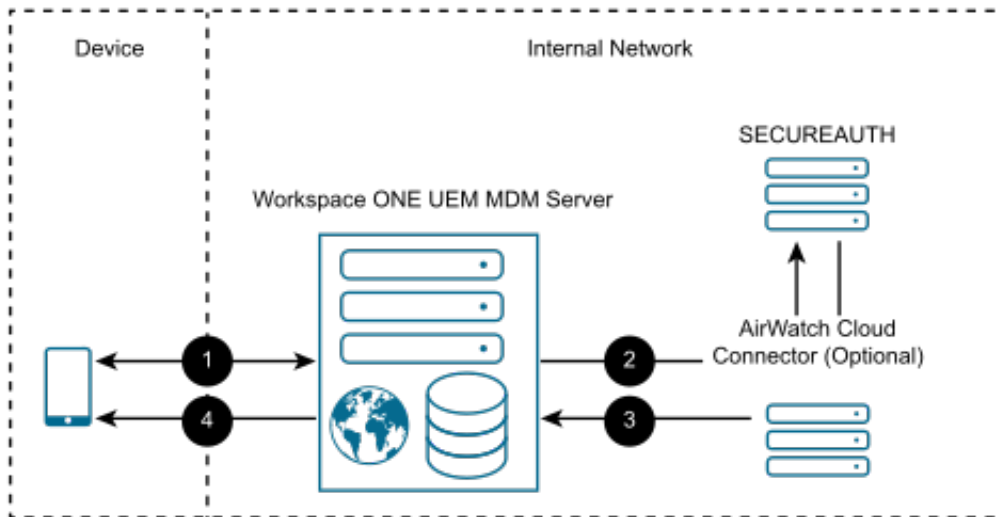
Note: If your SecureAuth endpoint is public-facing, then it must be protected by a public SSL certificate. If you are using the AirWatch Cloud Connector, configure it to trust the root certificate installed on your SecureAuth appliance.

■ Workspace ONE UEM SaaS and SecureAuth SaaS



- a Device enrolls with Workspace ONE UEM.
- b Workspace ONE UEM requests a certificate from the SecureAuth endpoint.
- c The SecureAuth endpoint delivers the certificate to Workspace ONE UEM.
- d Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

■ Workspace ONE UEM and SecureAuth Both Installed On-Premises



- a Device enrolls with Workspace ONE UEM.
- b Workspace ONE UEM requests a certificate from the SecureAuth endpoint (optionally through the AirWatch Cloud Connector).
- c The SecureAuth endpoint delivers the certificate to Workspace ONE UEM (optionally through the AirWatch Cloud Connector).

- d Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.

Note: If your SecureAuth endpoint is public-facing, then it must be protected by a public SSL certificate. If you are using the AirWatch Cloud Connector, configure it to trust the root certificate installed on your SecureAuth appliance.

This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)
- [What to do next](#)

Prerequisites

- A SecureAuth instance that is configured for certificate deployment.
- Workspace ONE UEM console version 9.6 or later.
- If your SecureAuth appliance is public-facing, it must be protected with a Public SSL Certificate. If you are using VMware AirWatch Cloud Connector for enterprise integration, then AirWatch Cloud Connector needs to be configured to trust the root certificate installed on your SecureAuth appliance.

Procedure

- 1 Generate a SecureAuth MPKI RA certificate.
- 2 Configure the CA and the request template in the Workspace ONE UEM console.
 - a Configure the CA.
 - 1 Navigate to **Devices > Certificates > Certificate Authorities > Certificate Authorities** tab.
 - 2 Click **Add** and complete the menu items.

Option	Description
Authority Type	SecureAuth
Server URL	Enter <code>https://<SecureAuth_FQDN>/SecureAuthX/webservice/certificateissuerws.svc</code> , where <code><SecureAuth_FQDN></code> is the URL of your SecureAuth instance and the "X" in "SecureAuthX" is the realm instance number that is configured for certificates. This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.
Company GUID	Enter the value that you can find in the SecureAuth portal. Look in the License Info section.

Option	Description
User name	Enter name for your SecureAuth instance. Look in the FBA WebService section of the SecureAuth portal.
Password	Enter value for your SecureAuth instance. Look in the FBA WebService section of the SecureAuth portal.

b Configure the request template.

- 1 Navigate to **Devices > Certificates > Certificate Authorities**.
- 2 Select the **Request Templates** tab.
- 3 Click **Add** and complete the menu items.

Option	Description
Certificate Authority	SecureAuth
Subject Name	The identity bound to the certificate.
Key Pair Generation Location	<p>Select either Workspace ONE UEM or SecureAuth. This is where the key pair is generated – either on the SecureAuth side or on the Workspace ONE UEM side.</p> <ul style="list-style-type: none"> ■ SecureAuth - Generates the certificate and the private key and returns it back to Workspace ONE UEM with its root certificate. The root certificate and user certificate are combined into a single certificate and sent to the device to install. ■ Workspace ONE UEM - Configure the Certificate Validity Period, which is the length of time the certificate is valid for in days. You can use the value 365. Also, configure the Private Key Length, which is how secure you want the keys. Use 2048 as the key length.
Private Key Type	Select if the certificate is used for signing and encryption operations or both.
Automatic Certificate Renewal	<p>Select the this checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by SecureAuth when it expires.</p> <p>If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests SecureAuth to reissue the certificate in the Auto Renewal Period (days) field. This requires the certificate profile on SecureAuth to have the Duplicated Certificates setting enabled.</p>
Enable Certificate Revocation	Select the this checkbox if you want Workspace ONE UEM to be able to revoke certificates.

c Configure Workspace ONE UEM profiles (payloads) for either PKI or SCEP. If in Retrieving Certificate from SecureAuth certificate authority, you chose PKI then you only need to configure a Credentials profile. Once either of these profiles are created, you can create additional payloads that the SecureAuth certificate can use, such as Exchange ActiveSync (EAS), VPN, or Wi-Fi services.

- 1 Navigate to **Devices > Profiles > List View**.
- 2 Click **Add**.

- 3 Select the applicable platform for the device type.
 - 4 Specify all **General** profile parameters.
 - 5 Select **Credentials** from the payload options and select **Configure**.
 - 6 Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.
 - 7 Select the external SecureAuth CA you created previously from the **Certificate Authority** drop-down menu.
 - 8 Select the certificate template for SecureAuth you created previously from the **Certificate Template** drop-down menu. Saving and Publishing the profile would deploy a certificate to the device. However, if you plan on using the certificate on the device for Wi-Fi, VPN, or email purposes, then you should also configure the respective payload in the same profile to leverage the certificate being deployed.
- d (Optional) If you are using AirWatch Cloud Connector and the SecureAuth appliance is not public-facing, configure AirWatch Cloud Connector to trust the SecureAuth appliance.
- 1 Open MMC by searching for it using Windows Search and launching the mmc.exe file.
 - 2 Navigate to File > Add/Remove Snap-in.
 - 3 The Add or Remove Snap-ins screen displays.
 - 4 Select the Certificates snap-in in the left pane and select Add.
 - 5 Select Computer account as Snap in source. Select Next.
 - 6 Select Local computer. Select Finish.
 - 7 Select OK.
 - 8 Expand the newly added Certificates tree.
 - 9 Expand the Trusted Root Certification Authorities folder.
 - 10 Right-click the Certificates folder here and select All Tasks > Import.
 - 11 Proceed through the Certificate Import Wizard. As prompted, browse and select the file of the root certificate used to generate the SecureAuth SSL certificate. Select Next.
 - 12 Select Place all certs in the following store. Select Next.
 - 13 Click Finish.

What to do next

Review some tips and troubleshooting steps for the integration.

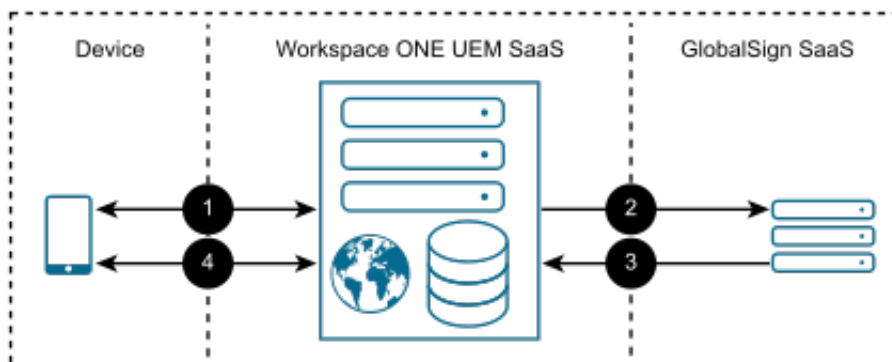
- Verify ability to perform certificate authentication without Workspace ONE UEM. Remove Workspace ONE UEM from the configuration and manually configure a device to connect to your network server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect with a certificate.

- Verify ability to perform certificate authentication with Workspace ONE UEM. You can confirm that the certificate is usable by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured EAS, VPN, or Wi-Fi access-point. If the device is not connecting and shows a message that the certificate cannot be authenticated or the account cannot connect then there is a problem in the configuration. Below are some helpful troubleshooting checks.
- If SSL TLS errors are received while creating a template.
 - This error can occur when you attempt two tasks.
 - Create a Workspace ONE UEM certificate template by selecting the Retrieve Profiles button or
 - Retrieve a certificate from the Workspace ONE UEM console from the SecureAuth certificate authority.
 - The troubleshooting technique that usually resolves this problem is adding the required server certificate chain in the console servers trusted root key store.
- If the Workspace ONE UEM Certificate Profile fails to install on the device.
 - Inform Workspace ONE UEM Professional Services of the error and request they:
 - Turn On Verbose Mode to capture additional data.
 - Retrieve web console log.
 - Workspace ONE UEM analyzes the log and works with customer to resolve the problem.
- If the certificate is not populated in the View XML option of the profile.
 - Confirm that lookup values configured on the SecureAuth certificate profile match the lookup values in the Workspace ONE UEM console's Request Template.
 - Confirm that lookup values in Workspace ONE UEM Request Template are actually populated in the user information being pulled from AD.
 - Confirm you are pointing to the right profile in SecureAuth.

Workspace ONE UEM is flexible with PKI integration by being able to request certificates from either internal or external certificate authorities (CA). Integrate with GlobalSign PKI services to issue certificates for your Workspace ONE UEM MDM solution.

In order for Workspace ONE UEM to communicate with GlobalSign for certificate distribution, you must have a GlobalSign instance configured and ready to issue certificates. You can then configure Workspace ONE UEM to communicate with GlobalSign using basic authentication. Once communication is successfully established, you can define how to deploy certificates to devices. Below is an example of how GlobalSign and Workspace ONE UEM can be deployed.

- 1 The device enrolls with Workspace ONE UEM.
- 2 Workspace ONE UEM requests a certificate from the GlobalSign endpoint.
- 3 The GlobalSign endpoint delivers the certificate to Workspace ONE UEM.
- 4 Workspace ONE UEM delivers the certificate to the device as part of an EAS, VPN, or Wi-Fi profile.



This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)
- [What to do next](#)

Prerequisites

- A GlobalSign instance that is configured for certificate deployment.
- Workspace ONE UEM console version 9.5 or later.
- A service account with authentication permissions.

Procedure

- 1 Generate the GlobalSign certificate.
- 2 Configure the GlobalSign certificate authority in Workspace ONE UEM console.
 - a Navigate to **Devices > Certificates > Certificate Authorities**.
 - b Click **Add**.
 - c Select **GlobalSign** from the **Authority Type** drop-down menu.
 - d Enter a unique name and description that identifies the GlobalSign certificate authority in the **Certificate Authority** and **Description** fields.
 - e In the **Server URL** field enter the URL of your GlobalSign instance.
 - f This is the web endpoint that Workspace ONE UEM will use to submit requests and issue certificates.
 - g Enter the **Username** and **Password** fields belonging to the service account with authentication permissions mentioned in System Requirements above.
 - h Click **Save**.
 - i Click **Test Connection** when complete to verify the test is successful. An error message appears indicating the problem if the connection fails.
 - j Click **Save**.
- 3 Set up the request template for GlobalSign in Workspace ONE UEM console.
 - a Navigate to **Devices > Certificates > Certificate Authorities**.
 - b Select the **Request Templates** tab and select **Add** to complete the menu items.

Option	Description
Certificate Authority	GlobalSign
Profile ID	Enter the GlobalSign profile identity bound to the certificate.
Product Code	Enter the code for the certificate and the license.
Validity Period	Enter how long the certificate is valid.

Option	Description
SAN Type	<p>Select Add to include one or more Subject Alternate Names with the template.</p> <p>This entry 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.</p> <p>Each field supports lookup values. Email Address, User Principal Name, and DNS Name are supported by GlobalSign templates by default.</p>
Automatic Certificate Renewal	<p>Select the checkbox if Workspace ONE UEM is going to automatically request the certificate to be renewed by GlobalSign when it expires.</p> <p>If you select this option, enter the number of days prior to expiration before Workspace ONE UEM automatically requests GlobalSign to reissue the certificate in the Auto Renewal Period (days) field. This requires the certificate profile on GlobalSign to have the Duplicated Certificates setting enabled.</p>
Enable Certificate Revocation	Select the checkbox if you want Workspace ONE UEM to be able to revoke certificates.

- c Select **Save**.
- 4 Configure a Workspace ONE UEM Credentials profile (payloads) to deploy to devices. This profile connects the GlobalSign certificate authority configured in the console to devices with this Credentials profile (payload).
 - a Navigate to **Devices > Profiles > List View**.
 - b Click **Add**.
 - c Select the applicable platform for the device type.
 - d Specify **General** profile parameters.
 - e Select **Credentials** from the payload options and select **Configure**.
 - f Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.
 - g Select the external GlobalSign CA you created from the **Certificate Authority** drop-down menu.
 - h Select the request template for GlobalSign you created from the **Certificate Template** drop-down menu. Saving and publishing the profile would deploy a certificate to the device. However, if you plan on using the certificate on the device for Wi-Fi, VPN, or email purposes, then you should also configure the respective payload in the same profile to leverage the certificate being deployed.

What to do next

Review some tips and troubleshooting steps for the integration. * Verify ability to perform certificate authentication without Workspace ONE UEM. Remove Workspace ONE UEM from the configuration and manually configure a device to connect to your network server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect with a certificate. *

Verify ability to perform certificate authentication with Workspace ONE UEM. You can confirm that the certificate is usable by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured EAS, VPN, or Wi-Fi access-point. If the device is not connecting and shows a message that the certificate cannot be authenticated or the account cannot connect then there is a problem in the configuration. Below are some helpful troubleshooting checks. * If SSL TLS errors are received while creating a template. * This error can occur when you attempt two tasks. * Create a Workspace ONE UEM certificate template by selecting the Retrieve Profiles button or * Retrieve a certificate from the Workspace ONE UEM console from the SecureAuth certificate authority. * The troubleshooting technique that usually resolves this problem is adding the required server certificate chain in the console servers trusted root key store.

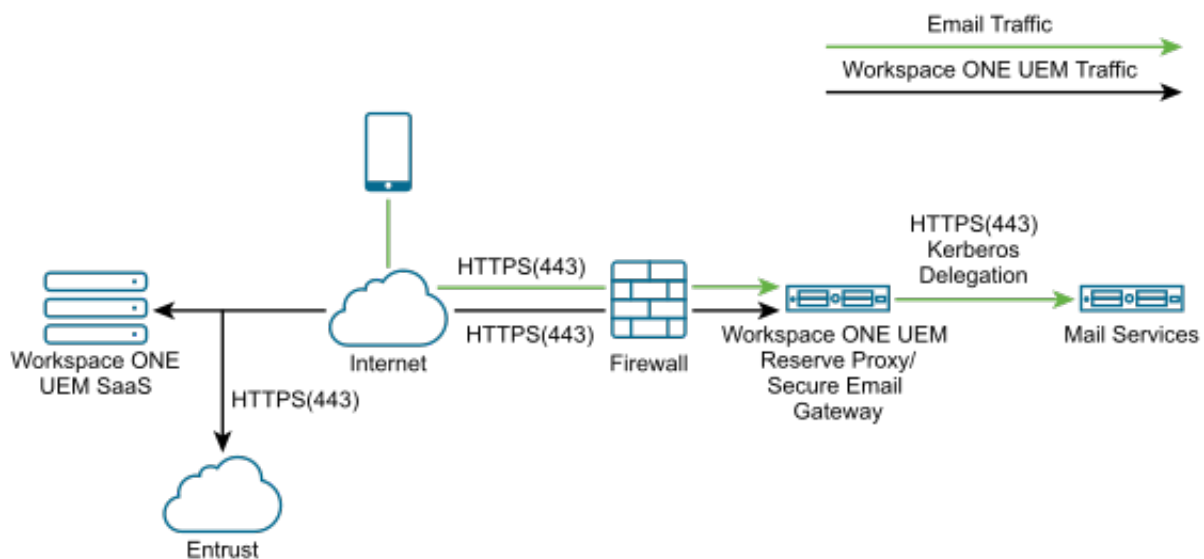
- If the Workspace ONE UEM Certificate Profile fails to install on the device.
 - Inform Workspace ONE UEM Professional Services of the error and request they:
 - Turn On Verbose Mode to capture additional data.
 - Retrieve web console log.
 - Workspace ONE UEM analyzes the log and works with customer to resolve the problem.
- If the certificate is not populated in the View XML option of the profile.
 - Confirm that lookup values configured on the GlobalSign certificate profile match the lookup values in the Workspace ONE UEM console's Request Template.
 - Confirm that lookup values in Workspace ONE UEM Request Template are actually populated in the user information being pulled from AD.
 - Confirm you are pointing to the right profile in GlobalSign.

Entrust ID Issuance

8

Workspace ONE UEM can request certificates from various certificate authorities, one is Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority. To use Entrust as a certificate authority, use the supported version of Workspace ONE UEM console, have access to an Entrust ID Enterprise instance, and set up Entrust ID Enterprise for mobile enrollment.

You can use Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority as a third-party certificate authority for Workspace ONE UEM in a SaaS environment. Communication flows between Workspace ONE UEM, Entrust, and mobile devices.



This chapter includes the following topics:

- [Prerequisites](#)
- [Procedure](#)
- [What to do next](#)

Prerequisites

- Open port 19443 from the Workspace ONE UEM console to your Entrust server.

Note: SaaS deployments can contact VMware Support Services to check that 19443 is open.

- If you use the AirWatch Cloud Connector, go to the advanced settings, and disable the Entrust PKI.
- Use supported Entrust API versions V8 and V9.
- Use Workspace ONE UEM console version 9.5 or later.
- VMware AirWatch Cloud Connector is required if the Entrust ID Enterprise instance is installed behind a firewall.
- An Entrust ID Enterprise instance needs to be available.
- Configure Entrust ID Enterprise for mobile enrollment.

Procedure

- 1 Set up Entrust ID Enterprise for mobile enrollment with Workspace ONE UEM. This task creates an Entrust Managed certificate authority (CA) and issues the instance of Entrust with a digital ID. Perform this task with help from your Entrust ID Enterprise representative. If you are using Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority, your representative gives you several values for configuring Entrust as a CA in Workspace ONE UEM console.
 - URL to enter as the **Server URL** of the CA.
 - Credentials for the **Server URL**.
 - A digital ID configuration to enter while completing the certificate template.
 - Configure an Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority CA in Entrust ID Enterprise. Adding a Managed CA allows Entrust ID Enterprise to communicate with your Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority CA.
 - Configure a Digital ID Configuration in Entrust ID Enterprise. A Digital ID Configuration is a template that Entrust ID Enterprise uses to issue digital IDs.
 - Configure the Entrust ID Enterprise digital ID policies.
 - Mirror the password rules set in Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority and Entrust ID Enterprise. If the password rules do not match, errors can occur when issuing digital IDs.
 - Add an Entrust ID Enterprise administrator that your Workspace ONE UEM MDM uses to issue digital IDs.
- 2 Configure Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority as a certificate authority (CA) in the Workspace ONE UEM console. Configuration sets communication between the systems using values from your Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority managed certificate authority.
 - Navigate to **Devices > Certificates > Certificate Authorities** and in the **System Settings** page that displays, select the **Certificate Authorities** tab.

- Select the **Add** button. The Certificate Authority – Add / Edit page displays.
- Enter in the **Name** field a unique name that identifies the Entrust certificate authority.
- Select the **Authority Type** drop-down and select **Entrust**.
- For **Protocol**, select either the **PKI** or **SCEP** radio button.
- Enter in the **Server URL** field the URL of the Administration Services MDM Web Service or the Entrust ID Enterprise Administration Service. If you are using Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority PKI, your Entrust ID Enterprise representative gave you this URL when you configured Entrust for mobile enrollment. should have been provided to you by an Entrust representative. An example of the URL is `https://mobile.example.com:19443/mdmws/services/AdminServiceV8`.
- In the **Username** and **Password** settings, enter the user name of the Administration Services or Entrust ID Enterprise administrator you created while configuring Entrust. If you are using Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority PKI, this username and corresponding password should have been provided to you by an Entrust representative.
- When complete, select the Test Connection button and verify that the test is successful. If the connection failed, an error displays. This error could be the result of a certificate not being installed on the Workspace ONE UEM server or the URL not being correct. In the example error, the Server URL was not correct.

Connection Failed: There was no endpoint listening at https://ptnr-pki-ws.bbtest.net/policyService that could accept the message. This is often caused by an incorrect address or SOAP action. See InnerException, if present, for more details.

- Select **Save**.
- 3 Define which certificate Workspace ONE UEM console deploys to devices by setting up a certificate template for Entrust ID Enterprise.
- On the **Certificate Authorities** system settings page (**Groups & Settings > Configurations > Certificate Authorities**), select the **Request Templates** tab.
 - Select the **Add** button to add a new Certificate Template. The **Certificate Template Add/Edit** window displays.
 - Select on the **Certificate Authority** drop-down and select the Entrust CA you configured earlier.
 - Enter in the **Name** and **Description** fields the name you want to give the Entrust certificate template.
 - For **Managed CA**, select the name of the Entrust CA.
 - Click on the **Profile Name** drop-down and select the name of the Digital ID Configuration that you created while configuring Entrust. If you are using Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority, this Digital ID Configuration should have been provided to you by an Entrust representative.

- Configure **Subject Alternative Name** (SAN) attributes as required. These are used for additional unique identification of the device and need to match the Digital ID configuration.
- If Workspace ONE UEM automatically requests the certificate to be reviewed by Entrust when it expires, check the **Automatic Certificate Renewal** check box and make sure the assignment type is set to Auto. Set the number of days prior to expiration before Workspace ONE UEM automatically requests Entrust to reissue the certificate in Auto Renewal Period (days) field.
- If certificates must be revoked, either manually or when they are removed from the device, select **Enable Certificate Revocation**.
- Complete the **Mandatory Fields** that are used to form the common name of the distinguished name within the certificate. These fields can change depending on which Entrust profile you choose since the information within the profile may be different. The fields you see on the left side correspond to the data source fields you declared on the Entrust side. The values on the right are the Workspace ONE UEM variables. Enter **Lookup Values** in each of the fields that complement those fields in the Entrust profile. Make sure the lookup values you use match those used in the Digital ID configuration. If you are using Entrust PKI as a Service (PKIaaS) or Entrust Certificate Authority, this information should have been provided to you by an Entrust representative.
- Click **Save**.

What to do next

To fix a (40) error that occurs in your integration of Entrust ID Enterprise and Workspace ONE UEM, delete old profiles and update the values for two parameters. If you see the error (40) `Error AirWatch.CloudConnector.CertificateService.CertificateService.TestConnection`, take the following steps to fix the error.

- Clean up stale profiles.
- Increase the size of **MaxReceivedMessageSize** to 2147483647.
- Increase the size of **MaxBufferSize** to 2147483647.