

VMware AirWatch Integration with SCEP (iOS/Mac) Guide

For VMware AirWatch

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Workspace ONE UEM Integration with SCEP	3
High-Level Design	3
System Requirements and Known Limitations	4
Chapter 2: Install, Set Up, Configure Certificate	5
Step 1: Configure the SCEP CA	5
Step 2: Configure the Request Template	6
Step 3: Create a SCEP Profile	6

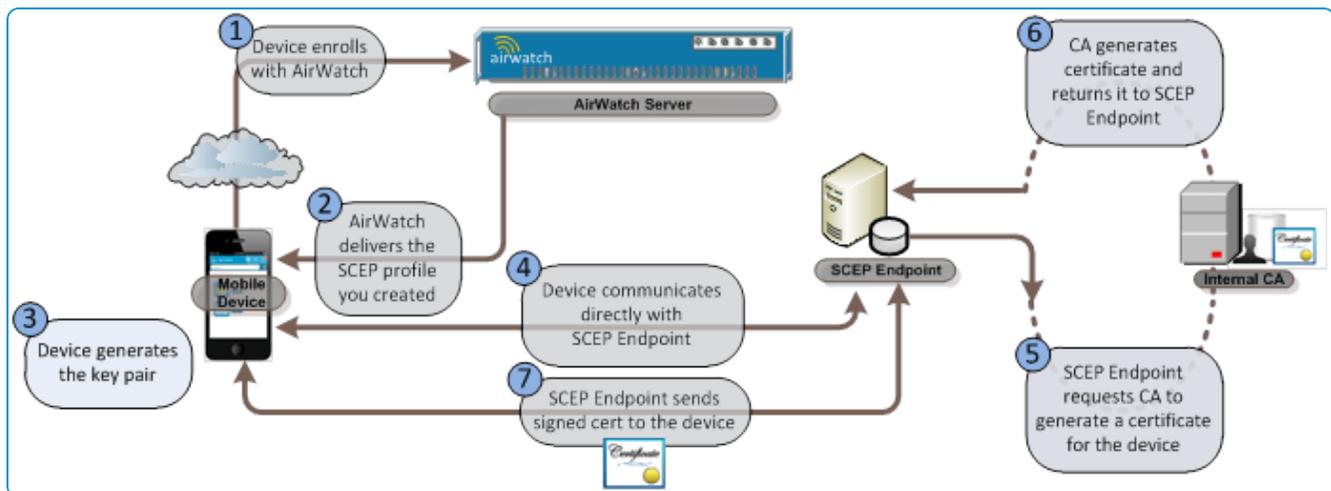
Chapter 1:

Workspace ONE UEM Integration with SCEP

Workspace ONE UEM supports SCEP (Simple Certificate Enrollment Protocol) for iOS and macOS 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.

High-Level Design

AirWatch 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.



System Requirements and Known Limitations

Workspace ONE UEM console

- AirWatch 7.0+

Supported Platforms

- iOS 5.0+
- macOS 10.7+

CA Requirements

- 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 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.

Known Limitations

- Renewal is **not supported**.
- Revoke is **not supported**.

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: Configure the SCEP CA

Perform the following steps to configure your SCEP endpoint.

1. Navigate to **Devices > Certificates > Certificate Authorities**. Select **Add**.
The Add/Edit certificate authority page displays.
2. Select **Generic SCEP** from the **Authority Type** drop-down.
3. Enter the following information pertaining to your SCEP Endpoint:

Field Name	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, its usages, etc.
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 will use 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.

4. Select **Save**.

Step 2: Configure the Request Template

Next you need to configure the request template, which is used to determine what goes in the subject field, the key length, and the private key usage.

Perform the following steps to configure the request template.

1. Navigate to **Devices > Certificates > Certificate Authorities**. Select the **Request Templates** tab. Select **Add**. The Add/Edit certificate template page displays.
2. Enter the following information pertaining to your request template.

Name	Field 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.

3. 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 SANn 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.
4. Select **Save**.

Step 3: Create a SCEP Profile

Even if you protect your corporate email, Wi-Fi and VPN with strong passcodes and other restrictions, your infrastructure still remains vulnerable to brute force and dictionary attacks, in addition to employee error. For greater security, you can implement digital certificates to protect corporate assets. To do this, you must first 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.

To push certificates down to devices, you need to configure a SCEP payload as part of the profiles you created for EAS, Wi-Fi and VPN settings. Use the following instructions to create a certificate-enabled profile.

1. Navigate to **Devices > Profiles > List View > Add** and select **iOS** from the platform list.
2. Configure General profile settings as appropriate.
3. Select either an **EAS**, **Wi-Fi** or **VPN** payload to configure. Fill out the necessary information, depending on the payload you selected.

4. 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.
5. 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.
6. Select **Save and Publish** when you are done configuring any remaining settings.