SCEP Configuration

SCEP (Simple Certificate Enrollment Protocol) is a standardized protocol for certificate management, crucial for securely provisioning digital certificates to devices, including the devices managed by the Workspace ONE® SDK. These certificates are essential for device and user authentication, enabling secure access to corporate resources.

Table of Contents

Key Concepts

- Certificate: A digital certificate verifies the identity of a device or user.

- SCEP: A protocol that automates certificate requests and enrollment.

- Workspace ONE: A unified endpoint management (UEM) platform that includes tools and services to manage devices.

- Workspace ONE SDK: Provides libraries for developers to integrate Workspace ONE functionalities, including SCEP, into device applications.
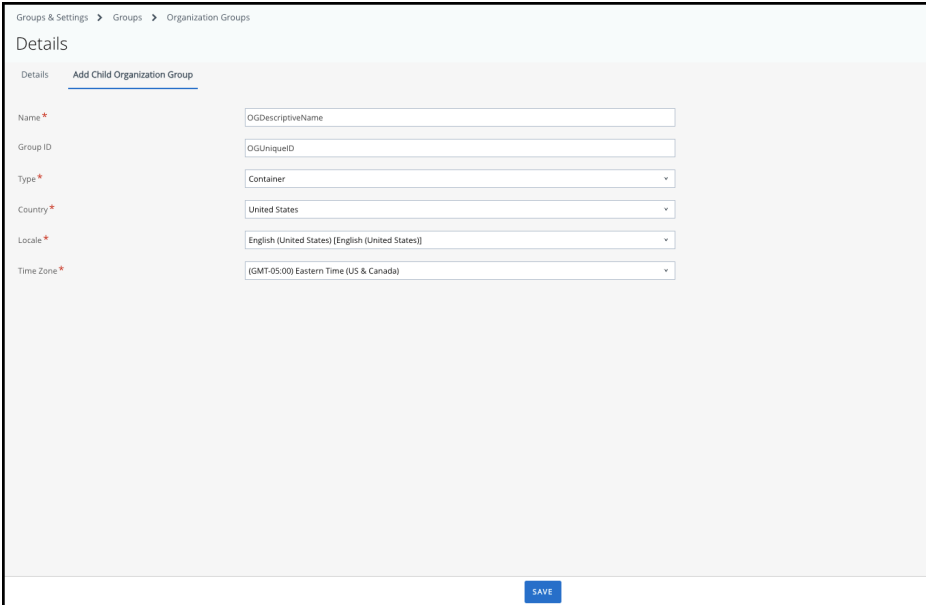
SCEP Enrollment Process With Workspace ONE

When using Workspace ONE, the SCEP enrollment process involves these steps:

Creating an Organization Group (OG) in Workspace ONE UEM

Organization Groups are used to organize devices, users, and policies within the Workspace ONE UEM.

Steps:

- Navigate to Organization Group Details:
- Go to `Groups & Settings > Groups > Organization Groups > Details`.
- Select the `Add Child Organization Group` tab.
- Provide the following information. Refer screen capture below:

Screen Capture: OG Creation

- Select **Save** and save the settings.

Once inside your created OG, all further steps must be completed there.

Workspace ONE SCEP Configuration

The administrator configures SCEP settings in the Workspace ONE UEM, including the SCEP server URL, certificate templates, and enrollment policies.

Steps:

- Navigate to Certificate Authorities Settings:
- Go to `Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities` and click **Add** to add a certificate authority.
- Enter the information from the SCEP server. Refer screen capture below:

Screen Capture: Certificate Authorities

- Choose the `Authority Type` from the dropdown menu to match your SCEP server configuration. Refer screen capture below.

Screen Capture: CA Authority Types

- After entering all details, click `Test Connection`.
- If the test is successful, a confirmation pop-up will appear; click **Save** to save the configuration.
- If the test is unsuccessful, check the server connection. Refer Screen Capture below:

Screen Capture: CA Test Connection

- The next step is to add a certificate template. Switch to the `Request Templates` tab on the current screen. Refer Screen Capture below:

Screen Capture: CA Request templates

- Click 'Add' to add a Certificate Template. Enter the required information, select the previously added certificate authority, and save. Refer Screen Capture below:

Screen Capture: Certificate Template

With this Certificate authority and Certificate template configuration is completed in Workspace One UEM.

Active Directory Group Creation in Workspace ONE UEM

Workspace ONE UEM leverages your existing Active Directory (AD) infrastructure for user authentication and group management.

Steps:

- Navigate to AD(Active Directory) settings.
- Go to `Groups & Settings > All Settings > System > Enterprise Integration > Directory Services` and enter further information. Refer Screen Captures below:

Screen Capture: AD Server

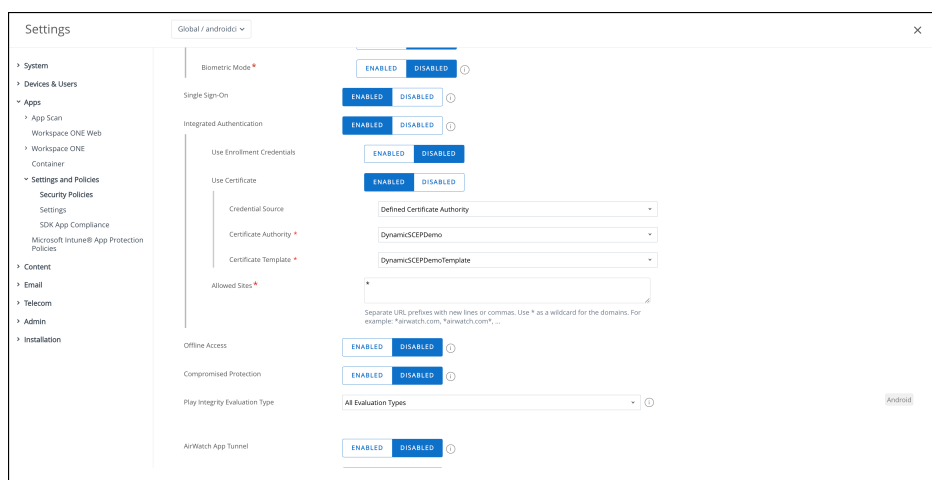**Screen Capture:** AD User

Screen Capture: AD Group

- After entering all details, click `Test Connection`. A confirmation pop-up will appear; click `Save` to save the configuration.

Configuring SCEP Details in SDK Profile in Workspace ONE UEM

This configuration allows applications that integrate the Workspace ONE SDK to obtain certificates for authentication and other security purposes. SDK profiles can be configured with either default or custom options.

Steps(DEFAULT):

- Navigate to default SDK profile settings.
- Go to `Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies`.
- Enable Integrated Authentication by selecting the previously created CA (Certificate Authority) and its template from the dropdown menus. Refer Screen Capture below:

Screen Capture: SCEP Settings in SDK Profile

- Click **Save** to save the default SDK profile.

Steps(CUSTOM):

- If you want to create a custom SDK profile, go to `Devices > Profiles & Resources > SDK Profiles` and click `Add Profile`.
- Select the `Android` platform and click `Next`.
- Enter the required information and select the previously created CA (Certificate Authority) and its template from the dropdown menus. Refer Screen Captures below:

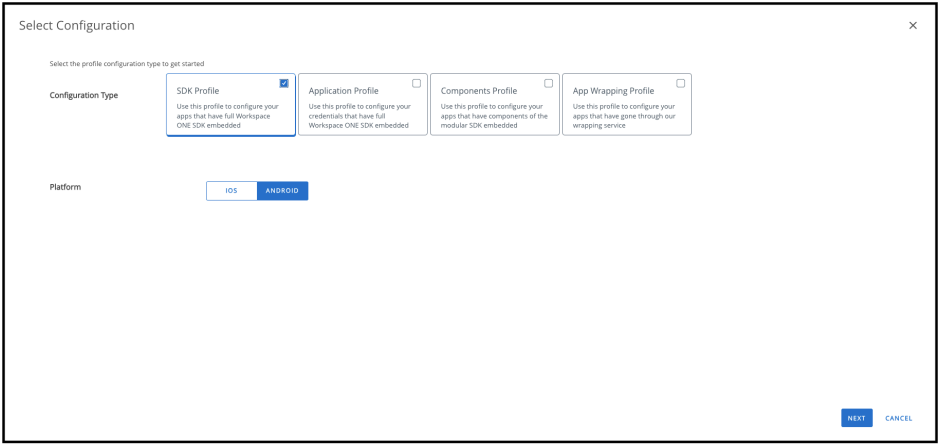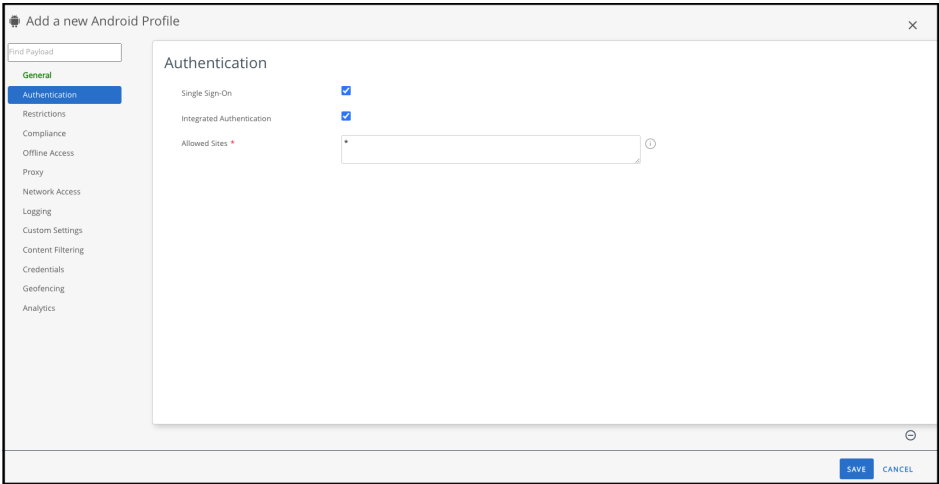Screen Capture: SCEP Settings in Custom SDK Profile

Screen Capture: SCEP Settings in Custom SDK Profile IA
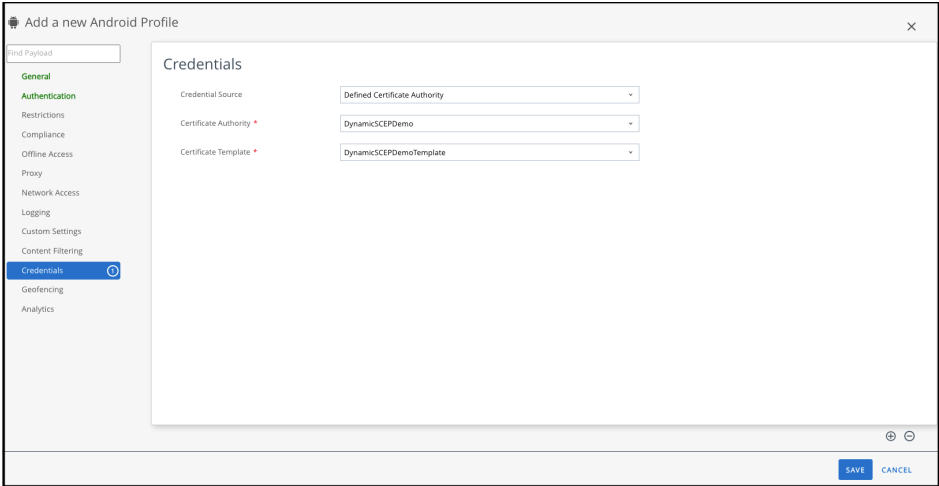
Screen Capture: SCEP Settings in Custom SDK Profile Cert

- Click **Save** to save the custom SDK profile.

After saving, navigate to your application and assign the newly created SDK profile(default or custom).

Device Application enrolment

Enrol the device application in this server and Organization Group with AD(Active Directory) user information. Workspace ONE then delivers the SDK profile with SCEP configuration to the managed device. Sample Application Code for Workspace ONE for Android SDK is available at Integration Guide For Android.

Setup Verification

When the SCEP endpoint is accessed, the URL connection should return an HTTP 200 (OK) response, confirming successful certificate issuance.
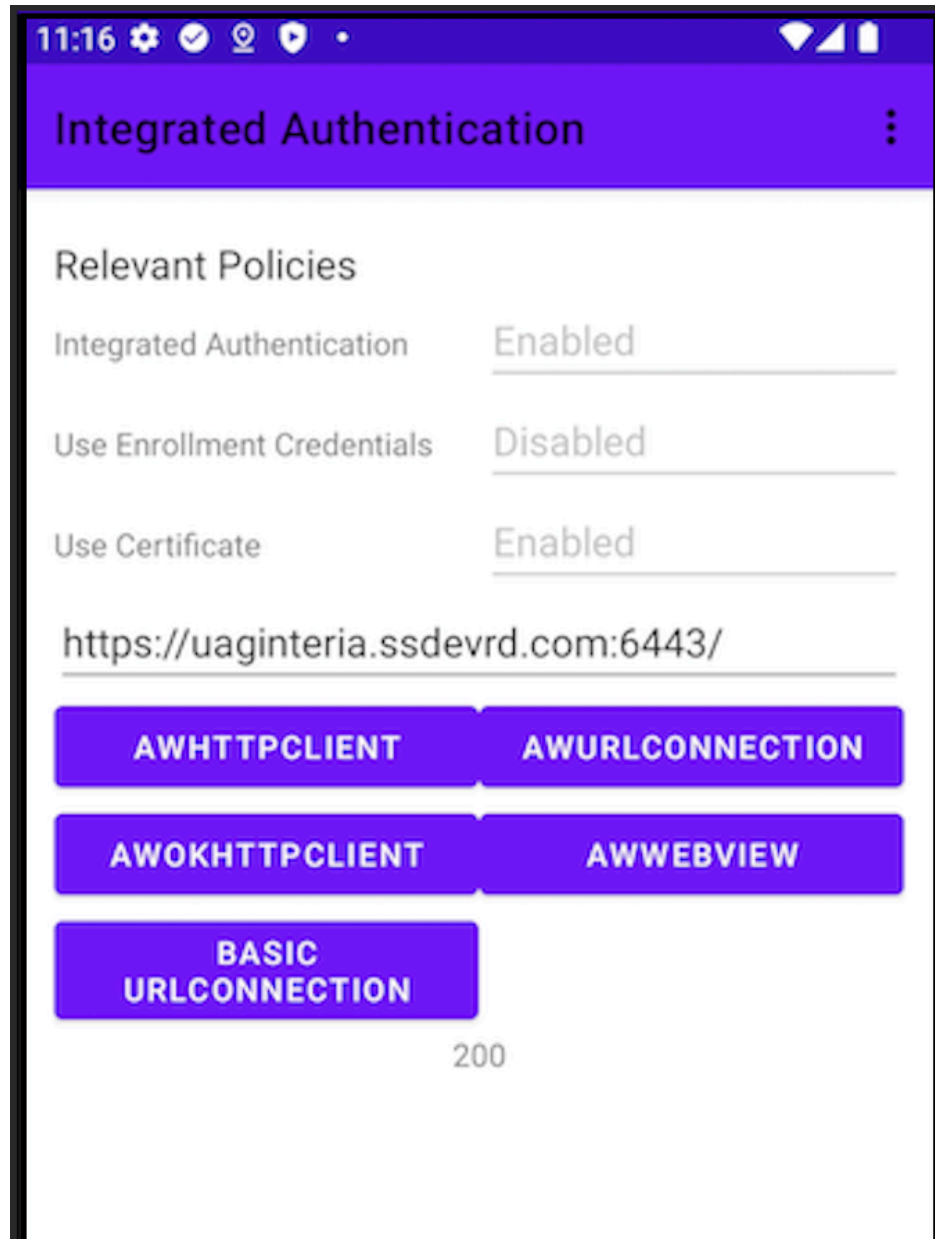
Screen Capture: SCEP Verification

Document Information

Revision History

The following table shows the revision history of this document.

Date	Revision
22 May 2025	Initial Publication.
04 Aug 2025	Updated the revision history format.

License

This software is licensed under the Omnissa Software Development Kit (SDK) License Agreement; you may not use this software except in compliance with the License.

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

This software may also utilize Third-Party Open Source Software as detailed within the Android_open_source_licenses.txt file.