



Comodo Certificate Manager

Device Certificates Enrollment
Simple Certificate Enrollment Protocol

Device Certificates Enrollment - Simple Certificate Enrollment Protocol

Introduction

The Simple Certificate Enrollment Protocol (SCEP) is a mechanism for automating the requests of digital certificates. Using SCEP, an administrator can automatically re-enroll and retrieve new digital certificates to replace expired/expiring certificates. It was developed originally by Cisco Systems for use in network devices such as routers, but its use has expanded to other hardware and software devices. A recent example of a SCEP - capable system would be Apple's iOS platform and the devices that run it (iPhone, iPad, iPod Touch).

CCM supports SCEP and is integrated with a fully-compliant SCEP server. This document describes the settings required to access and use CCM as a SCEP server to enroll device certificates.

Note: To enable this feature, contact your account manager at Comodo.

Settings

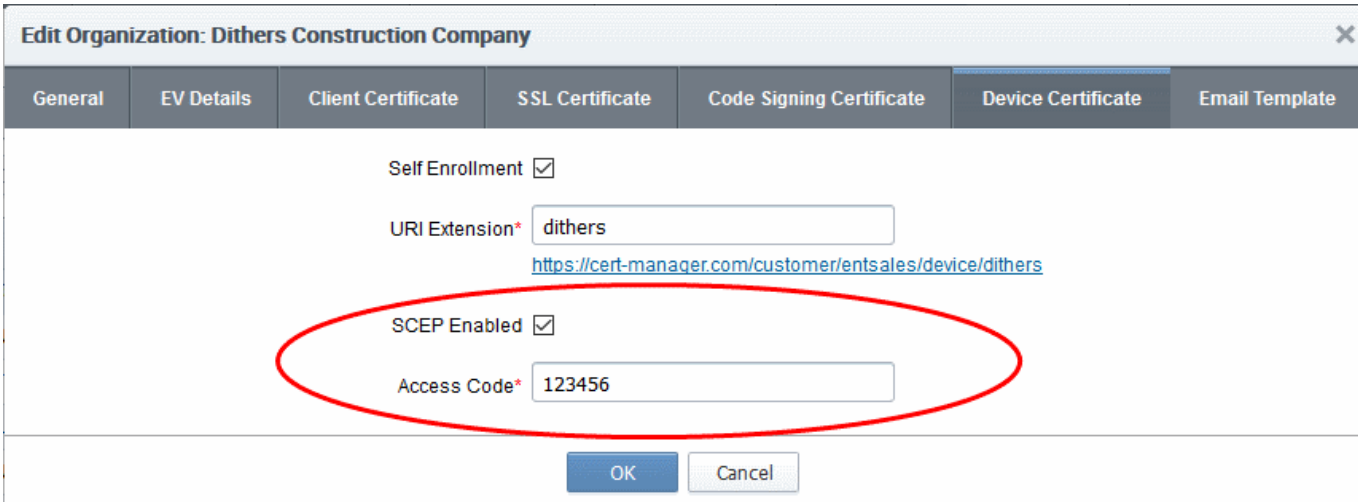
1. Enable SCEP Enrollment for Organizations/Departments

Device certificates can be enrolled for devices belonging to an Organization/Department, by rolling out a configuration profile for OTA enrollment to them.

SCEP enrollment needs to be enabled for the Organization/Department and an access code is to be specified. This can be done while adding a new Organization/Department or by editing an Organization/Department.

To enable SCEP enrollment for an Organization:

- Click the 'Settings' tab and choose 'Organizations'
- In the 'Organizations' screen, click the 'Add' button or select an organization and click the 'Edit' button
- In the 'Add New Organization' or 'Edit Organization' dialog, click the 'Device Certificate' tab.
- Check the 'SCEP Enabled' checkbox:



The screenshot shows a dialog box titled "Edit Organization: Dithers Construction Company" with a close button (X) in the top right corner. The dialog has several tabs: "General", "EV Details", "Client Certificate", "SSL Certificate", "Code Signing Certificate", "Device Certificate", and "Email Template". The "Device Certificate" tab is selected. In this tab, there are several settings:

- "Self Enrollment" is checked with a checkbox.
- "URI Extension*" is set to "dithers" in a text field, with a blue link below it: <https://cert-manager.com/customer/entsales/device/dithers>
- "SCEP Enabled" is checked with a checkbox, and this entire section is circled in red.
- "Access Code*" is set to "123456" in a text field.

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

The 'Access Code' field will appear.

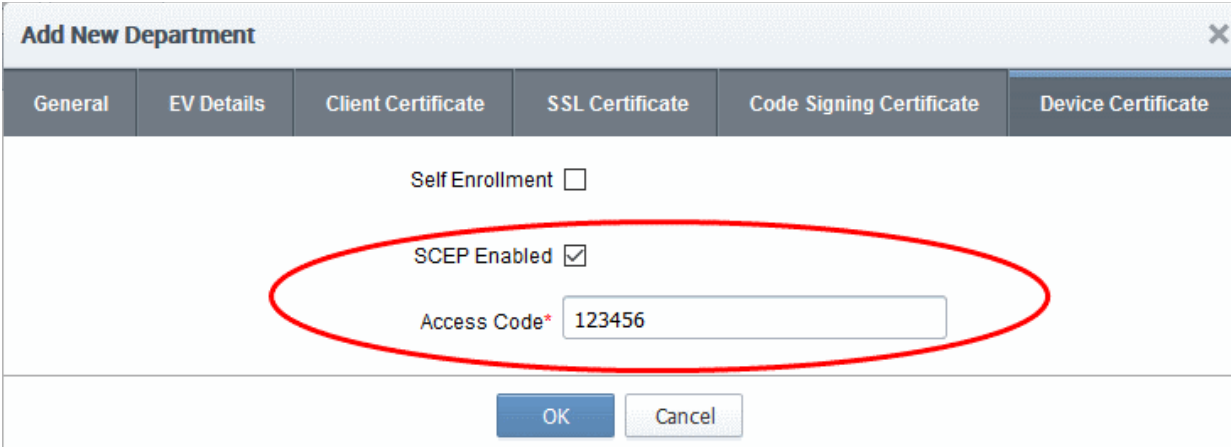
- Type an access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.

Note: The access code for the organization should be entered as the 'challengePassword' parameter in the profile applied to devices which belong to that organization.

- Click 'OK'.

To enable SCEP enrollment for Departments:

- Click the 'Settings' tab and choose 'Organizations'
- In the 'Organizations' screen, select an organization and click the 'Departments' tab to view its departments
- In the 'Departments' dialog, click the 'Add' button, or select an existing department and click 'Edit'
- In the Add/Edit department dialog, click the 'Device Certificate' tab.
- Check the 'SCEP Enabled' checkbox.



The screenshot shows a dialog box titled "Add New Department" with a close button (X) in the top right corner. The dialog has six tabs: "General", "EV Details", "Client Certificate", "SSL Certificate", "Code Signing Certificate", and "Device Certificate". The "Device Certificate" tab is selected. Inside the dialog, there are three checkboxes: "Self Enrollment" (unchecked), "SCEP Enabled" (checked), and "Access Code*" (checked). Below the "SCEP Enabled" checkbox is a text input field containing the value "123456". A red oval highlights the "SCEP Enabled" checkbox and the "Access Code*" field. At the bottom of the dialog are two buttons: "OK" and "Cancel".

The 'Access Code' field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

2. Set Device Certificate Types for SCEP Enrollment

Each device certificate type needs to be configured for SCEP enrollment. This will allow enrollment and provisioning of those types of certificates to devices belonging to suitably enabled Organizations and Departments.

- Click the 'Settings' tab and choose 'Certificates'
- Click the 'Device Cert Types' tab in the 'Certificates' interface
- In the 'Device Cert Types' screen, click the 'Add' button or select an existing Device Certificate type and click the 'Edit' button.
- In the 'Add New Device Cert Type' or 'Edit Device Cert Type' dialog, select the 'Allow for SCEP' check box.

*-required fields

Name*

Type ID*

Term*

CA name*

Allow for SCEP

Show on Selfenrollment

Key Usage Digital Signature
 Non repudiation
 Key Encipherment
 Data Encipherment
 Key Agreement

Extended Key Usage Client Authentication
 Email Protection
 MS Smartcard Login
 MS Encrypted File System
 OID-1

- Click 'OK'.

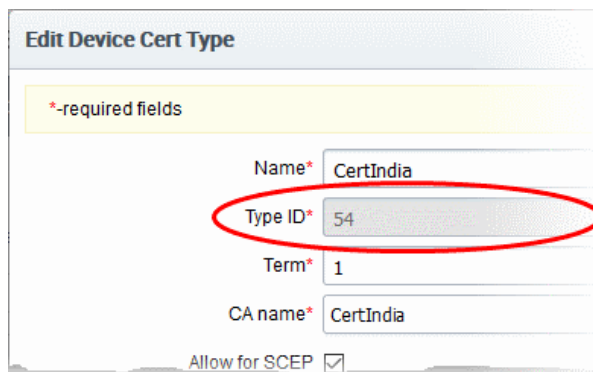
3. URL of the SCEP server

You need to include the URL of the SCEP server in the configuration profile for OTA enrollment. The URL should be in this format:

`http://<CCM Server>/customer/<customer name>/scep/device;deviceTypeld=<Device Typeld>/pkiclient.exe`

Partner	Description
<CCM Server>	The address of the CCM server you use
<customer name>	Your CCM company name
<DeviceTypeld>	The identification number assigned to the type of device certificate to be enrolled. The Type ID can be viewed from the CCM interface. <ul style="list-style-type: none"> • Click 'Settings' > 'Certificates' > 'Device Cert Types'

- Select the device certificate type and click 'Edit'
- The 'Type ID' is displayed in the Edit Device Cert Type dialog.



The screenshot shows a dialog box titled "Edit Device Cert Type". It contains several input fields: "Name*" with the value "CertIndia", "Type ID*" with the value "54", "Term*" with the value "1", and "CA name*" with the value "CertIndia". There is also a checkbox labeled "Allow for SCEP" which is checked. A yellow banner at the top of the form area indicates "*-required fields". The "Type ID*" field is circled in red.

Note 1: The URI protocol should be 'http' and not 'https' since the SCEP protocol relies on signed messages during a transaction.

For example: `http://cert-manager.com/customer/AcmeCorporation/scep/device;deviceTypeId=54/pkiclient.exe`

Tips for using SCEP in CCM for iOS devices:

On some older versions of iOS (4.x), setting the RSA Key Size in the mobileconfig file at 4096 may be required, as it appears iOS will sometimes generate 2047 bit keys (when 2048 bit is chosen), which will not be accepted by CCM or the CA.

In the nested-arrays for the Subject information in the mobileconfig, it may be necessary to use the OID for the 'emailAddress' field - 1.2.840.113549.1.9.1.

The 'challengePassword' should be set with the Access Code set for the Organization/Department.

About Comodo CA

Comodo Certificate Authority is one of the world's largest providers of SSL certificates by volume having issued over 91 million certificates and serving over 200,000 customers across 150 countries. The company provides a full suite of certificate products spanning all validation levels for website certificates, certificates for code-signing and email-signing, and the Comodo Certificate Manager (CCM) platform. Comodo CA has its US headquarters in New Jersey and international offices in the United Kingdom, Ukraine and India.

Comodo CA Limited

3rd floor, Office Village Exchange Quay

Trafford Road, Manchester, M5 3EQ

United Kingdom

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767