InCommon®

InCommon Certificate Manager

Device Certificates Enrollment
Simple Certificate Enrollment Protocol

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

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).

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

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

Settings

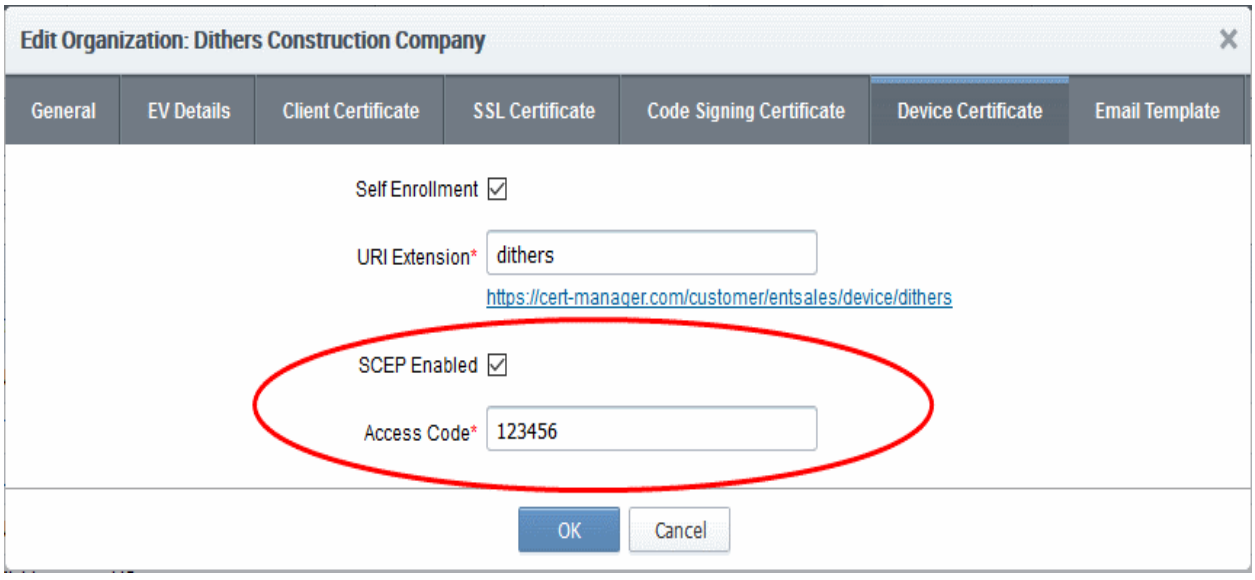
1. Enable SCEP Enrollment for Organizations/Departments

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 'Access Code' field will appear.

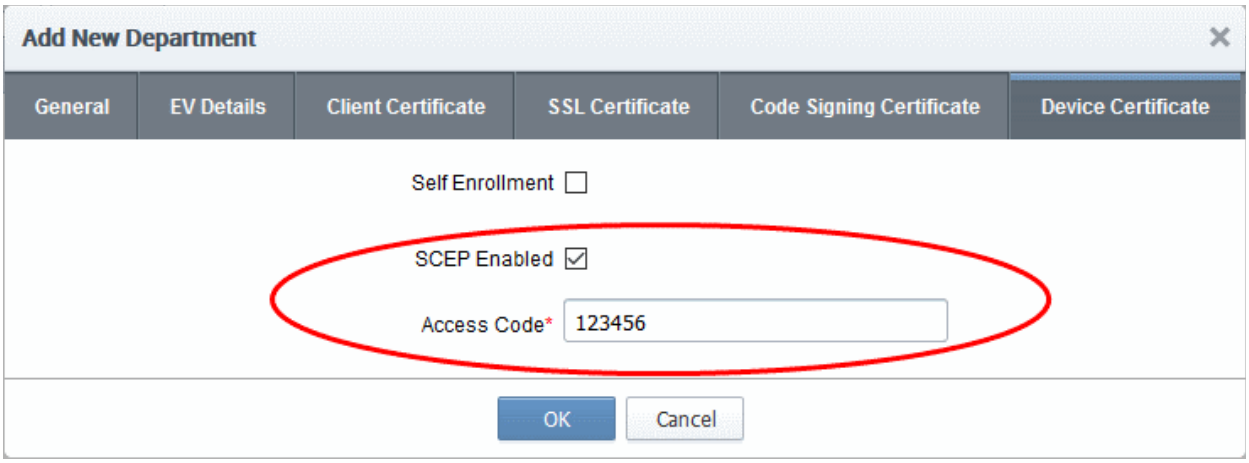
- Type an access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.

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 'Access Code' field will appear.

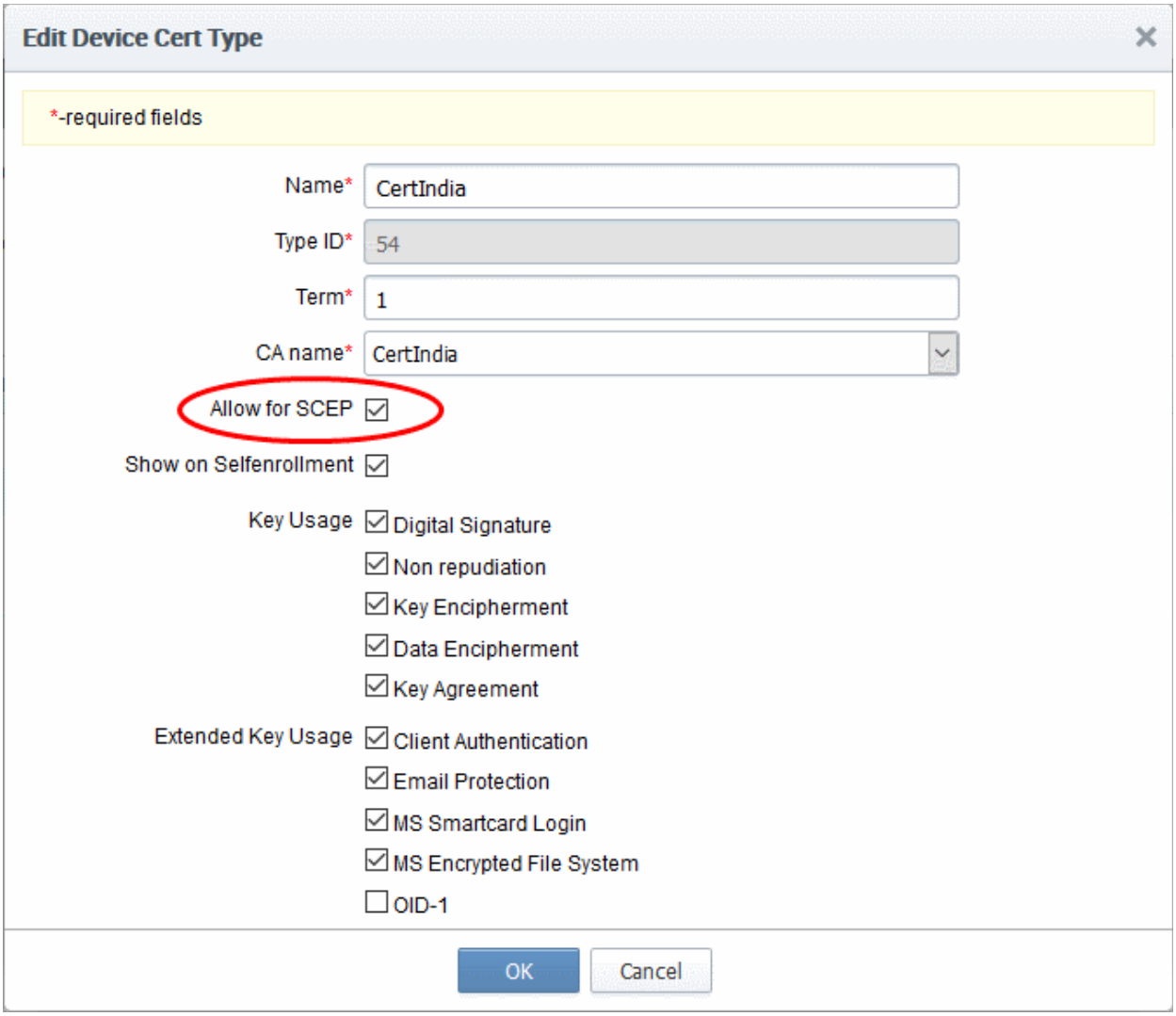
- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

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.



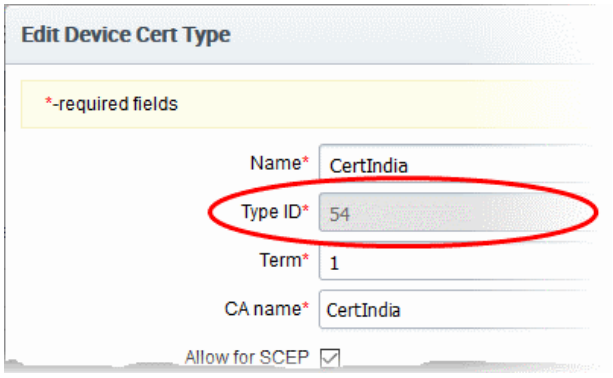
- Click 'OK'.

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://cert-manager.com/customer/InCommon/scep/device;deviceTypeId=<DeviceTypeId>/pkiclient.exe

Parameter	Description
<DeviceTypeId>	The identification number assigned to the type of device certificate to be enrolled. The Type ID can be viewed from the InCommon CM interface. • 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. 

Tip : 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/InCommon/scep/device;deviceTypeId=54/pkiclient.exe*

Tips for using SCEP in InCommon CM 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 InCommon CM 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.