COMODO
Creating Trust Online®

Comodo Certificate Manager

Simple Certificate Enrollment Protocol

Comodo CA Limited
3rd Floor, 26 Office Village, Exchange Quay,
Trafford Road, Salford,
Greater Manchester M5 3EQ,
United Kingdom.

Simple Certificate Enrollment Protocol

Introduction

The Simple Certificate Enrollment Protocol (SCEP) is a mechanism for automating the requests of digital certificates. An administrator, by using SCEP, can automatically re-enroll and retrieve new digital certificates for the ones that are due to expire or expired. 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 certificates.

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

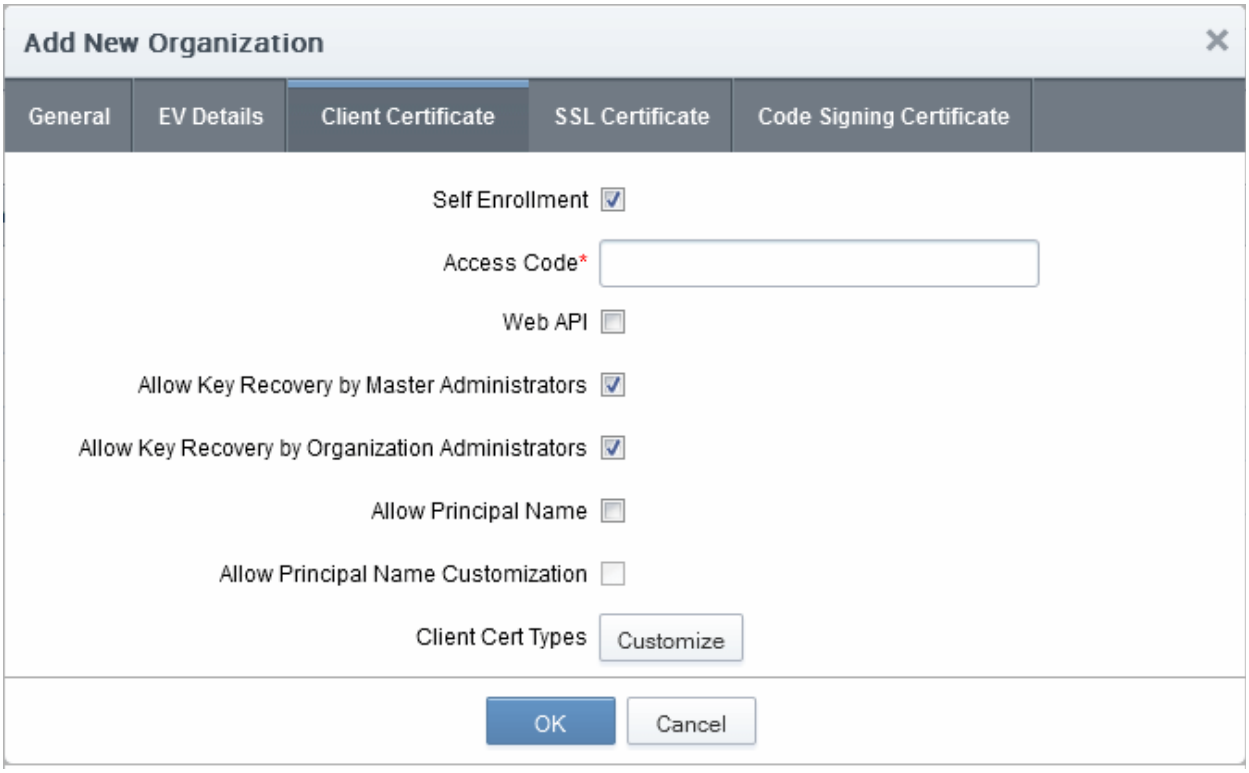
Settings

1. Enabling Self-Enrollment and Setting Access Code

Users can download certificates through SCEP only if Self-Enrollment is enabled and access code set in CCM. This can be done while adding a new Organization/Department or editing Organization/Department by the MRAO or the RAO Administrator.

To enable self-enrollment and set access code for Organizations:

- In the 'Organizations' screen, click the 'Add' button or the 'Edit' button beside an existing Organization.
- In the 'Add New Organization' or 'Edit Organization' dialog, click the 'Client cert' tab.



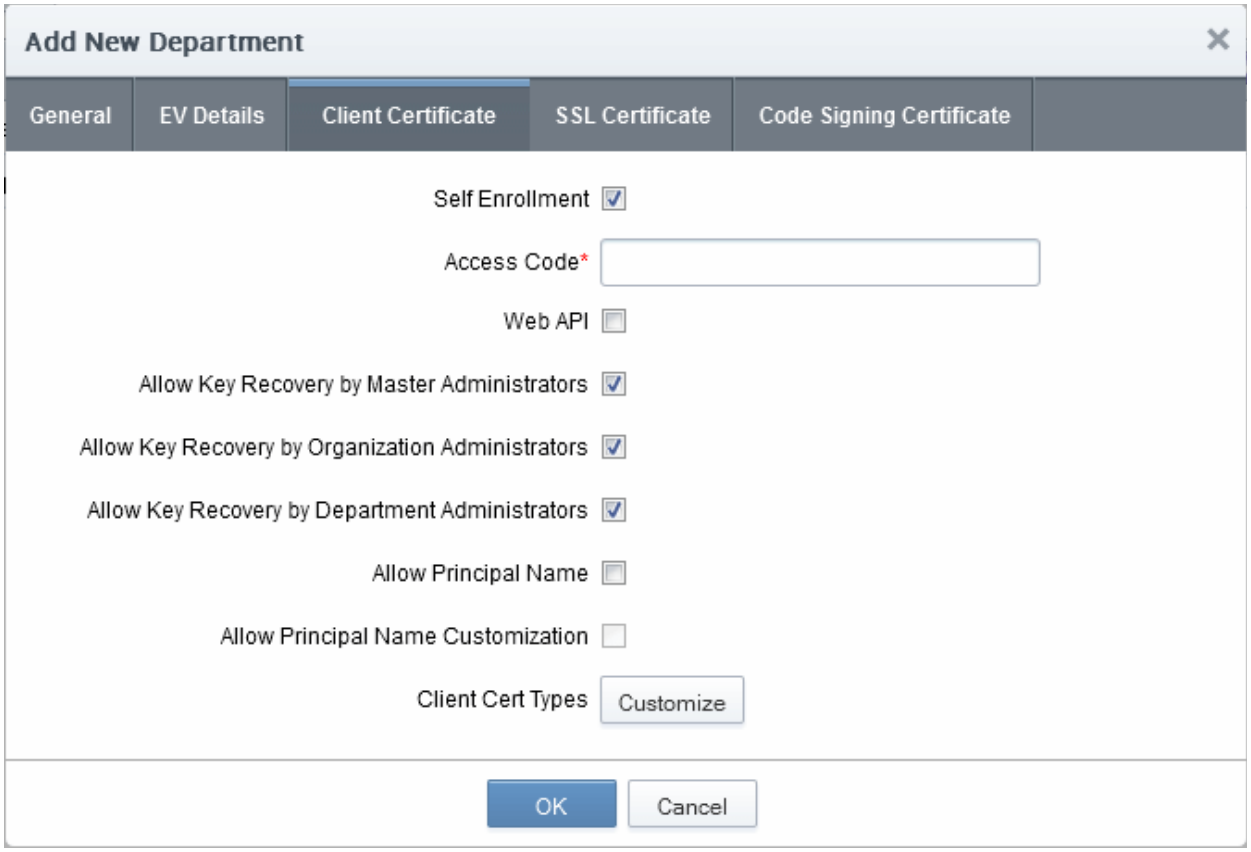
- Select the Self Enrollment checkbox.

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'.

To enable self-enrollment and set access code for Departments:

- In the 'Organizations' screen, click the respective 'Department' button beside an Organization for which you want to enable self-enrollment and set access code.
- In the 'Departments' dialog, click the 'Add' button or the 'Edit' button beside an existing Department.
- In the 'Add New Department' or 'Edit Department' dialog, click the 'Client cert' tab.



- Select the 'Self Enrollment' 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'.

To view the access code that is already set for Organizations/Departments, click the 'Edit' button beside the respective Organization/Department. You can view the access code under the 'Client cert' tab. DRAO administrator cannot set and view access codes and must consult MRAO or RAO administrator to find access code.

Note: The same access code should be entered in the 'challengePassword' field during the process of creating Certificate Signing Request. See section **Certificate Signing Request** for more details.

2. URL of the SCEP server

http://<*CCM Server*>/customer/<*customer name*>/scep/<*certificate type*>/pkiclient.exe

Partner	Description
<CCM Server>	The address of the CCM server you use
<customer name>	Your customer name
<certificate type>	'smime' for client and S/MIME certificates

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

For example: http://cert -manager.com/customer/AcmeCorporation/scep/smime/pkiclient.exe

Note 2: Private keys for certificates obtained using SCEP cannot be escrowed as the private key is never sent to CCM.

3. Certificate Signing Request

The Certificate Signing Request (CSR) requires the following:

- Key size - A minimum of 2048 bit.
- Subject information - Client certs need a minimum of CN and emailAddress.
- The subject CN must be an allowed domain, or the emailAddress (client certificates) must lie in an allowed domain for that Organization or Department.
- The CSR requires a 'challengePassword' to be set. This should be set to the 'Access Code' from within CCM for the

  Organization or Department the certificate is being enrolled into. See section **Enabling Self-Enrollment and Setting Access Code** for more details on setting access code.

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' can be set using the 'Challenge' key/value pair in the mobileconfig.

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