

COMODO
Creating Trust Online®



Comodo Certificate Manager

Software Version 5.7

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.

The screenshot shows the 'Add New Organization' dialog box with the 'Client Certificate' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with five tabs: 'General', 'EV Details', 'Client Certificate', 'SSL Certificate', and 'Code Signing Certificate'. The 'Client Certificate' tab is active. The settings are as follows:

- Self Enrollment:
- Access Code*:
- Web API:
- Allow Key Recovery by Master Administrators:
- Allow Key Recovery by Organization Administrators:
- Allow Principal Name:
- Allow Principal Name Customization:
- Client Cert Types:

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

- 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.

The screenshot shows the 'Add New Department' dialog box with the 'Client Certificate' tab selected. The dialog has a title bar with a close button (X) and a tabbed interface with five tabs: 'General', 'EV Details', 'Client Certificate', 'SSL Certificate', and 'Code Signing Certificate'. The 'Client Certificate' tab is active and contains the following settings:

- Self Enrollment
- Access Code*
- Web API
- Allow Key Recovery by Master Administrators
- Allow Key Recovery by Organization Administrators
- Allow Key Recovery by Department Administrators
- Allow Principal Name
- Allow Principal Name Customization
- Client Cert Types

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- 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/pkclient.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

The Comodo organization is a global innovator of cybersecurity solutions, protecting critical information across the digital landscape. Building on its unique position as the world's largest certificate authority, Comodo authenticates, validates and secures networks and infrastructures from individuals to mid-sized companies to the world's largest enterprises. Comodo provides complete end-to-end security solutions across the boundary, internal network and endpoint with innovative technologies solving the most advanced malware threats, both known and unknown. With global headquarters in Clifton, New Jersey, and branch offices in Silicon Valley, Comodo has international offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom. For more information, visit comodo.com.

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,

Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

Email: EnterpriseSolutions@Comodo.com

Comodo Security Solutions, Inc.

1255 Broad Street

Clifton,

NJ 07013

United States

Tel: +1.877.712.1309

Tel: +1.888.256.2608

For additional information on Comodo - visit <http://www.comodo.com>.