Sectigo® Certificate Manager

Certificate enrollment guide

22.1

January 2022

SECTIGO

Sectigo Certificate Manager

Certificate enrollment guide, 22.1 SCMCEG

Author: Sectigo

SECTIGO

Table of Contents

Device certificates

Preface

The *Sectigo Certificate Manager Certificate enrollment guide* explains how to enroll for, collect, and install client (S/MIME), SSL, code signing, and device certificates.

Audience

This guide is intended for users invited to enroll for certificates by an SCM administrator in their organization.

This document assumes that you are familiar with concepts related to security certificates issuance and management.

This document also assumes that you are familiar with your operating system. The general operation of any operating system is described in the user documentation for that system, and is not repeated in this manual.

Related Documentation

- SCM Release Notes

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles and emphasis.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, or text that appears on the screen.
`<text>`	Italic type with chevron brackets indicates the required insertion of user or company specific text.

1

Client certificates

This chapter describes how you enroll for client certificates and the subsequent steps required to install and configure your certificate on various email clients, browsers, and devices.

This chapter describes the following topics:

1.1 Client certificate enrollment

In order to begin the certificate enrollment process, your administrator should have sent you a provisioning email or provided you with a URL for the self enrollment form. The exact procedure to follow will depend on the type of email you receive. Currently there are two methods of client certificate enrollment:

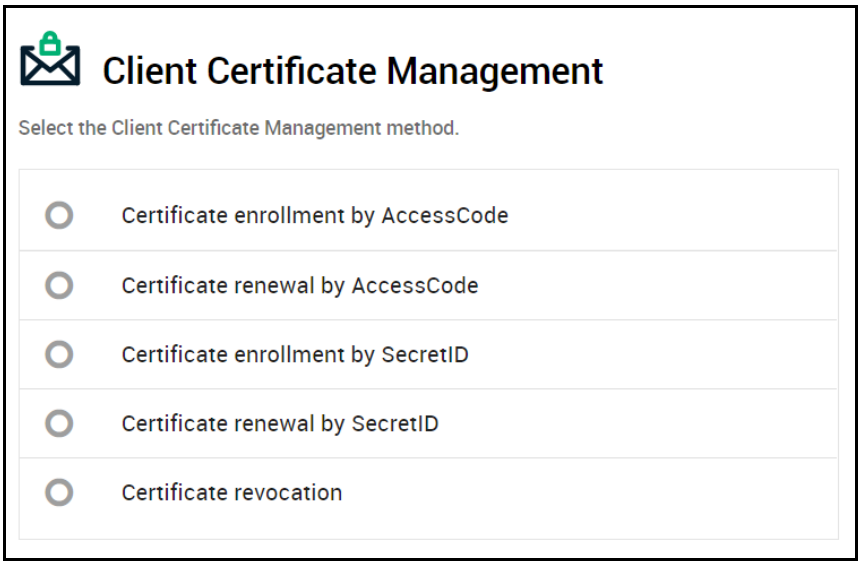
1.1.1 Client certificate self enrollment

A certificate self enrollment request requires that an administrator provides you with the URL for the self enrollment form. The administrator must also provide you with the Access Code or Secret ID needed to complete self enrollment.

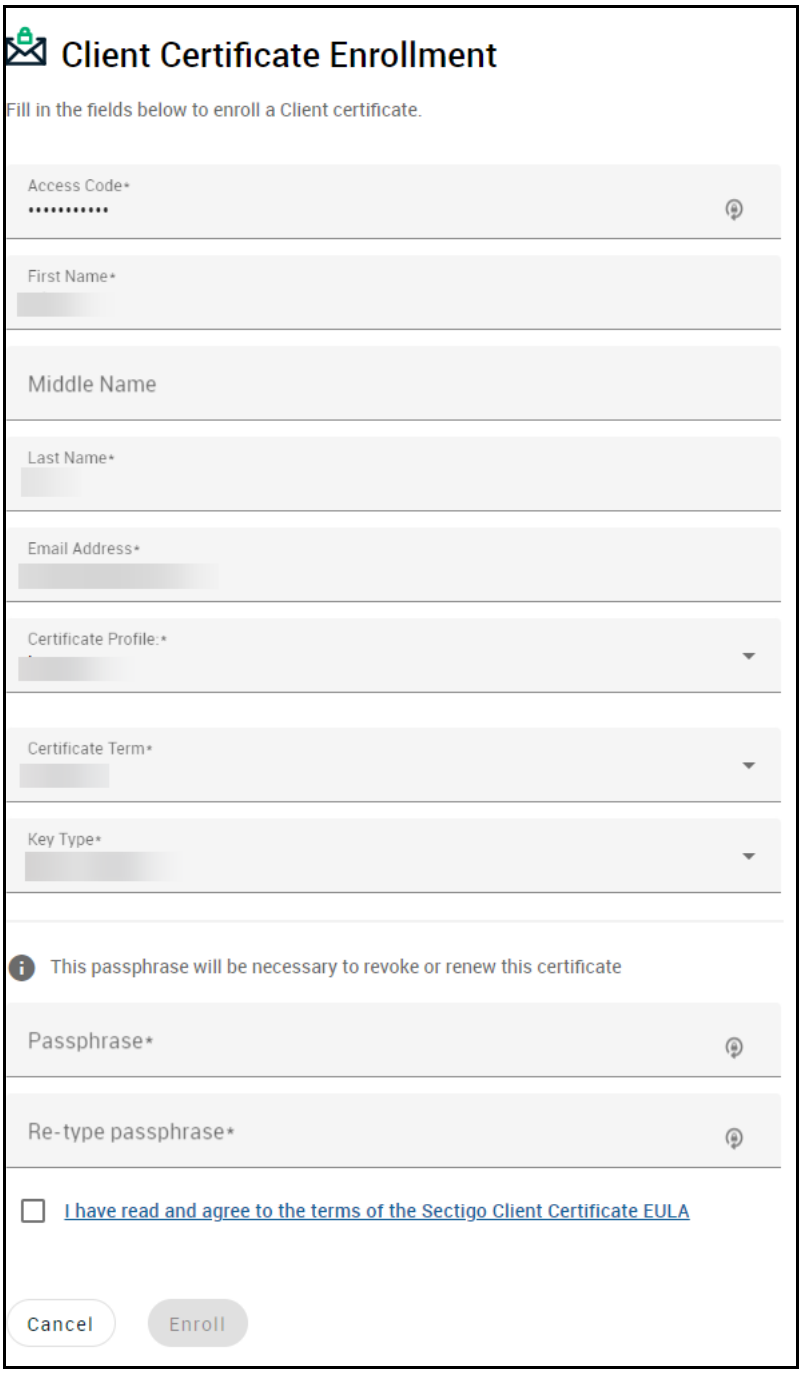
1.1.1.1 Client certificate enrollment by access code

To enroll for a certificate using an access code:

1. Navigate to the self enrollment form using the URL provided to you. The Client Certificate Management landing page is shown in the following illustration.



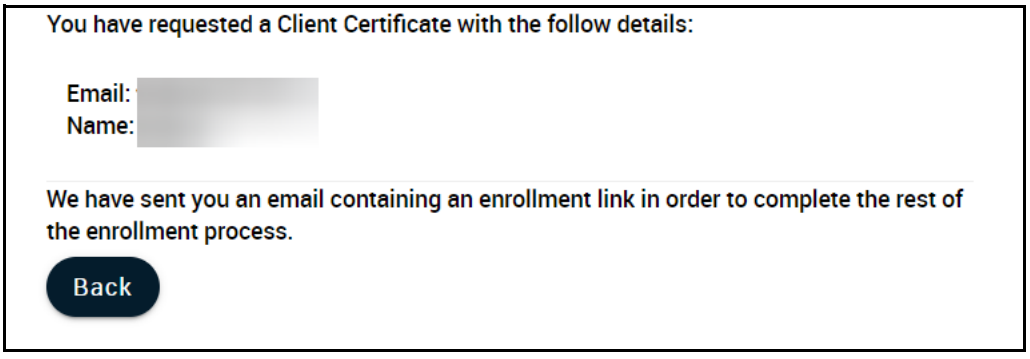
2. Select **Certificate enrollment by AccessCode**. You will be redirected to the access code self enrollment form shown in the following illustration.


Client Certificate Enrollment
Fill in the fields below to enroll a Client certificate.
Access Code*
First Name*
Middle Name
Last Name*
Email Address*
Certificate Profile:*
Certificate Term*
Key Type*
This passphrase will be necessary to revoke or renew this certificate
Passphrase*
Re-type passphrase*
I have read and agree to the terms of the Sectigo Client Certificate EULA
Cancel
Enroll

3. Complete the certificate enrollment fields using the following table.

Field	Description
Access Code	The identifier for your particular organization or department. This code is used to authenticate certificate requests that are made using the self-enrollment form. This code should have been provided to you with the self enrollment form URL.
First Name	Your first name.
Middle Name (Optional)	Your middle name.
Last Name	Your last name.
Email	Your email address for the domain belonging to your organization.
Certificate Profile	Depending on your organization's settings, you will need to enter the certificate profile for enrollment.
Certificate Term	Enter the length of the certificate term.
RSA Type	Select the appropriate key type.
Self Enrollment Passphrase	The passphrase required to revoke or renew the certificate.
Re-type Self Enrollment Passphrase	Confirmation of the passphrase.

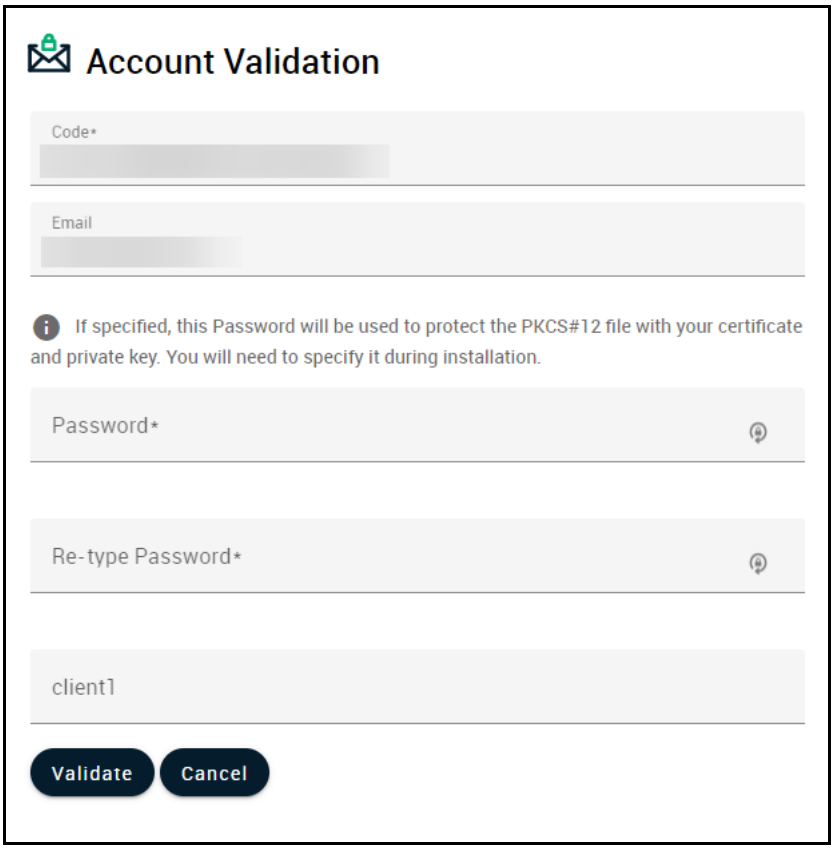
4. Read the Subscriber Agreement and accept by selecting **I accept the terms and conditions**.
5. Click **Enroll**.



Once you have enrolled you will receive a notification confirming your enrollment and an email containing a link to validate your account.

To continue with account validation:

1. Click the URL in your email to navigate to the account validation page shown in the following illustration.



2. Complete the account validation fields using the following table.

Field	Description
Code	The validation request code. This field is automatically populated.
Email	Your email address. This field is automatically populated.
Password	A password to protect your certificate. This password is used to protect access to the .p12 file.
Re-type Password	Confirmation of your Password.
Client 1	Enter the name of the client who will use the account.

3. Click **Validate**.
4. Click **Download** to download your certificate.

1.1.1.2 Renewing certificate enrollment by access code

To renew your certificate by access code, select **Certificate renewal by Access Code** in the Client Certificate Management landing page.

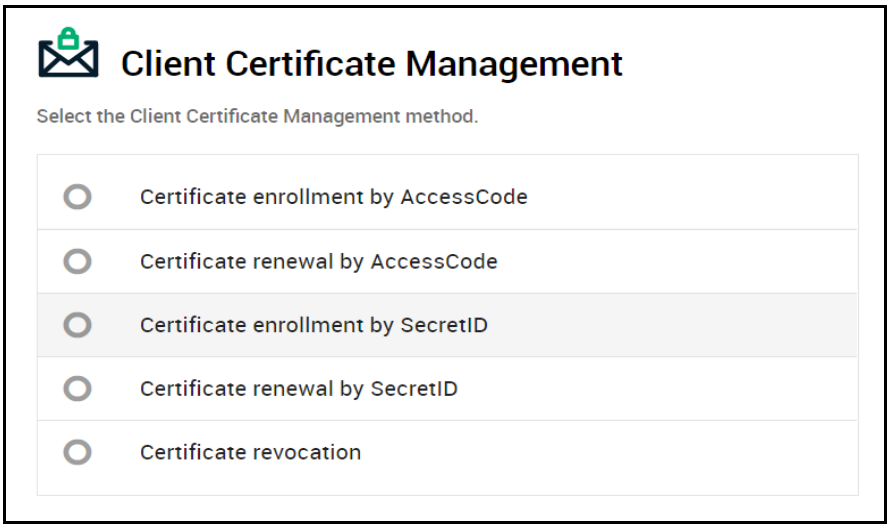
The required information is the same as for certificate enrollment.

Once you've completed all required fields, click **Renew**. You will then be able to download your renewed certificate.

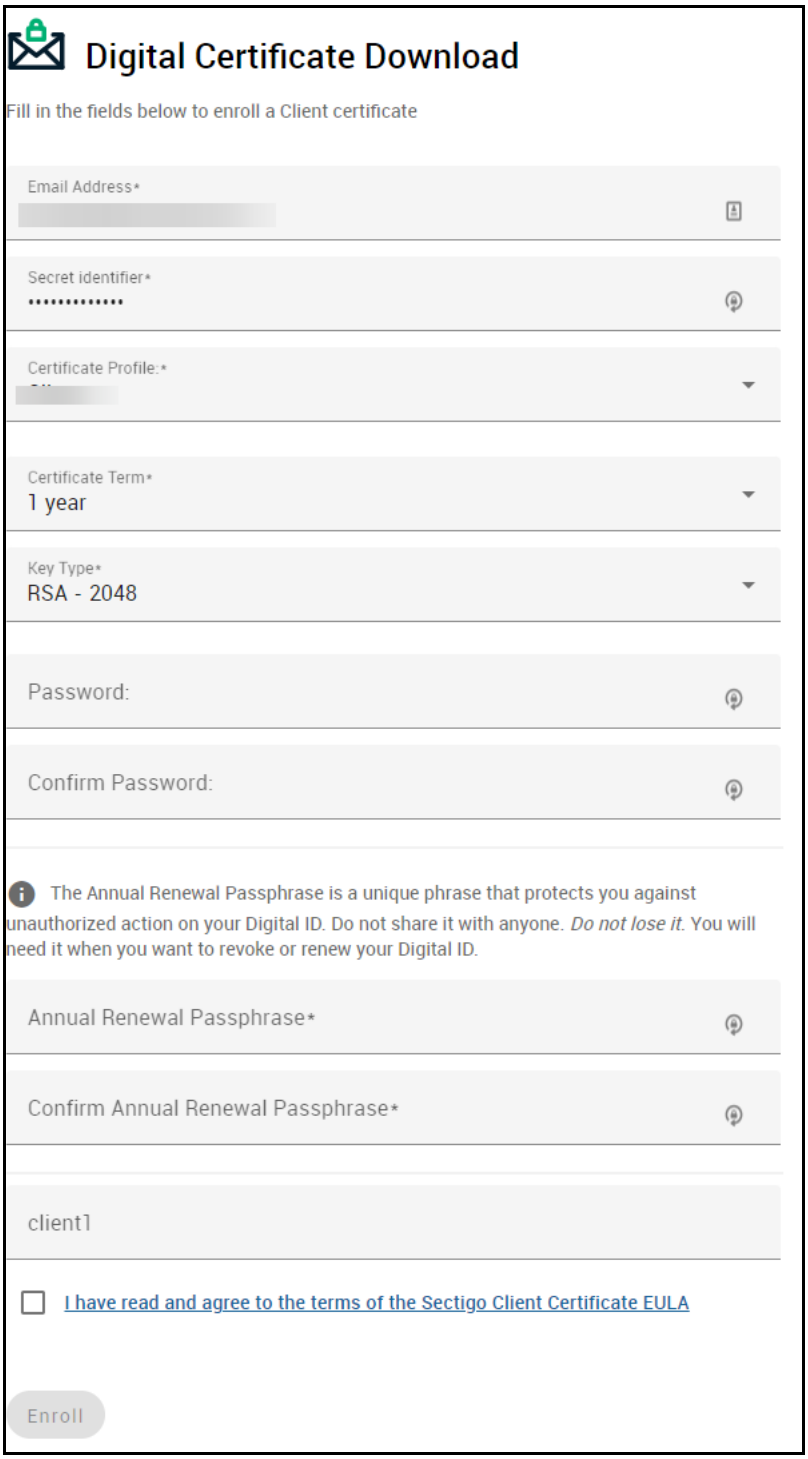
1.1.1.3 Client certificate enrollment by secret ID

To enroll for a certificate using a secret ID:

1. Navigate to the self enrollment form using the URL provided to you. The Client Certificate Management landing page is shown in the following illustration.



2. Select **Certificate enrollment by SecretID**. You will be redirected to the secret ID self enrollment form shown in the following illustration.


Digital Certificate Download
Fill in the fields below to enroll a Client certificate
Email Address*
Secret identifier*
Certificate Profile:*
Certificate Term*
1 year
Key Type*
RSA - 2048
Password:
Confirm Password:
The Annual Renewal Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID.
Annual Renewal Passphrase*
Confirm Annual Renewal Passphrase*
client1
I have read and agree to the terms of the Sectigo Client Certificate EULA
Enroll

3. Complete the certificate enrollment fields using the following table.

Field	Description
Email Address	Your email address for the domain belonging to your organization.
Secret Identifier	The identifier for your particular user account. This identifier is used to authenticate certificate requests that are made by you using the self-enrollment form. This identifier should have been provided to you with the self enrollment form URL.
Certificate Profile	Depending on your organization's settings, you will need to enter the certificate profile for enrollment.
Certificate Term	Enter the length of the certificate term.
Key Type	Select the appropriate key type.
Password	A password to protect your certificate. This password is used to protect access to the .p12 file.
Confirm Password	Re-enter your password as confirmation.
Annual Renewal Passphrase	The passphrase required to revoke or renew the certificate.
Confirm Annual Renewal Passphrase	Re-enter your passphrase as confirmation.
Client	Enter the name of your client.

4. Read the Subscriber Agreement and accept by selecting **I accept the terms and conditions**.
5. Click **Enroll**.
6. Click **Download** to download your certificate.

1.1.1.4 Renewing client enrollment by Secret ID

To renew your certificate by Secret ID, select **Certificate renewal by Secret ID** in the Client Certificate Management landing page.

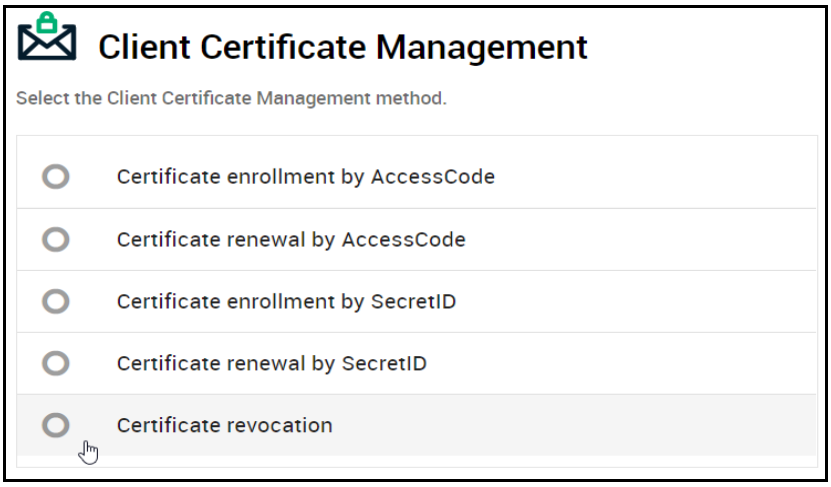
The required information is the same as for certificate enrollment.

Once you've completed all required fields, click **Renew**. You will then be able to download your renewed certificate.

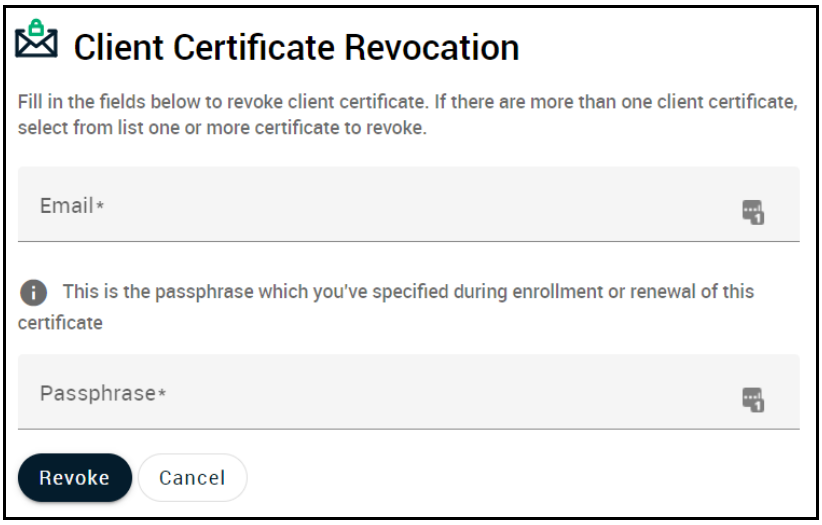
1.1.1.5 Revoking client certificates

To revoke a certificate:

1. Navigate to the self enrollment form using the URL provided to you. The self enrollment landing page is shown in the following illustration.



2. Select **Certificate revocation**. You will be redirected to the certificate revocation form shown in the following illustration.



3. Complete the certificate revocation fields using the following table.

Field	Description
Email Address	Your email address for the domain belonging to your organization.
Passphrase	The passphrase which you've specified during enrollment or renewal of this certificate.

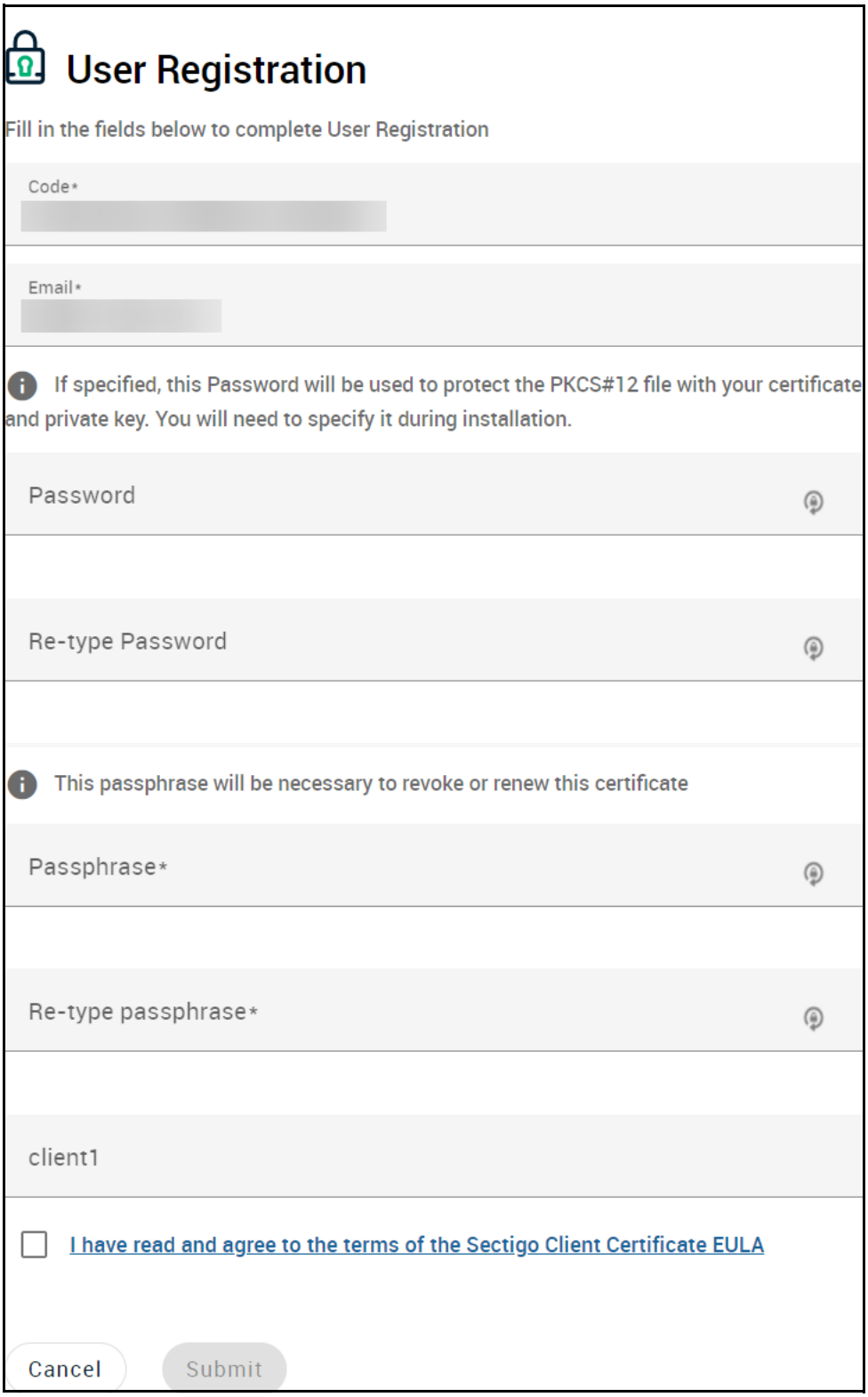
4. Select **Revoke**.

1.1.1.6 Client certificate user registration invitation

A user registration invitation email provides you with the URL for the user registration form. The email will also provide you with a request code required to complete self enrollment.

To enroll for a certificate using the user registration form:

1. Navigate to the **User Registration** form using the URL provided to you. The **User Registration** page is shown in the following illustration.



2. Complete the **User Registration** fields using the following table.

Field	Description
Code	The user registration request code. This field is automatically populated.
Email	Your email address. This field is automatically populated.
Password	A password to protect your certificate. This password is used to protect access to the .p12 file.
Re-type Password	Confirmation of your PIN.
Passphrase	The passphrase required to revoke the certificate.
Re-type passphrase	Confirmation of the passphrase.
Client	Enter the name of your client.

3. Read the Subscriber Agreement and accept by selecting **I accept the terms and conditions**.
4. Click **Enroll**.
5. Click **Download** to download your certificate.

1.2 Client certificate installation

Once you have completed the client certificate enrollment and received your certificate, you must import your certificate into your web browser and/or email client.

NOTE: Your client certificate should be automatically installed on any web browsers and email clients located on the computer from which you downloaded the certificate.

The exact process for installing your certificate is dependent on which browser and/or email client you are using. This section covers the following:

- Email clients
- Web browsers
- Mobile devices

1.2.1 Email clients

1.2.1.1 Importing your certificate into Outlook

To import your certificate into Outlook 2013-2019:

1. Open your Outlook email client.
2. Click **File > Options**.
3. Navigate to **Trust Center** and click **Trust Center Settings...**

4. Click **Email Security**.
5. Click **Import/Export...**
6. Click **Browse** and locate your client certificate.
7. Select your certificate and click **Open**.
8. Provide the password used to secure the certificate.
9. Click **OK**.
10. Click **Set Security Level...**, select **High** or **Medium**, click **Next** and then **Finish**.
11. Click **OK**.

Once you have successfully imported your certificate into Outlook, you need to configure Outlook to use the new certificate.

To apply your new certificate in Outlook:

1. Open your Outlook email client.
2. Click **File > Options**.
3. Navigate to **Trust Center** and click **Trust Center Settings...**
4. Click **Email Security**.
5. Click **Settings...**
6. From the **Change Security Settings** window, click **Choose** next to **Signing Certificate**.
7. Select your certificate.
8. Provide the password used to secure the certificate.
9. Click **OK**.

1.2.1.2 Importing your certificate into Mozilla Thunderbird

To import your certificate into Mozilla Thunderbird:

1. Open your Thunderbird email client.
2. Click on the menu to the right of the search bar.
3. In the menu, click **Options**.
4. Click **Options**.
5. Click **Advanced > Certificates > View certificates**.
6. From the **Certificate Manager** area, open the **Your Certificates** tab.
7. Click **Import**.
8. Browse to the location of your client certificate.
9. Select your certificate and click **Open**.
10. Provide the password used to secure the certificate.
11. Click **OK**.

Once you have successfully imported your certificate into Thunderbird, you need to configure Thunderbird to use the new certificate.

To apply your new certificate in Thunderbird:

1. Open your Thunderbird email client.
2. Click on the menu to the right of the search bar.
3. Click **Options > Account Settings > Security**.
4. In the **Digital Signing** area, click **Select**.
5. Select your certificate and click **OK**.
6. Select **Digitally sign messages (by default)**.
7. In the **Encryption** area, click **Select**.
8. Select your certificate and click **OK**.
9. Click **OK.**

1.2.1.3 Importing your certificate into Apple Mail

Apple Mail uses the Keychain Access Utility to manage digital certificates.

To import your certificate into the Keychain Access Utility:

1. Navigate to **Applications > Utilities > Keychain Access**.
2. Select **Login**.
3. Click **File > Import Items...**
4. Browse to the location of your client certificate.
5. Select your certificate and click **Open**.
6. Provide the password used to secure the certificate.
7. Click **OK**.

Once installed the certificate will be available for digitally signing and encrypting your emails through Apple Mail.

1.2.2 Web browsers

1.2.2.1 Internet Explorer

To import your certificate into Internet Explorer:

1. Open your Internet Explorer web browser.
2. Navigate to **Tools > Internet Options**.
3. Select the **Content** tab and click **Certificates**.
4. Select the **Personal** tab and click **Import**.
5. Click **Next.**
6. Click **Browse** and locate your client certificate.
7. Select your certificate and click **Open**.
8. Provide the password used to secure the certificate and select any applicable import options.
9. Click **Next**.
10. Specify the location that the certificate should be stored.

NOTE: Unless your administrator has specified otherwise, you should use the default option.

11. Click **Finish**.

1.2.2.2 Firefox

To import your certificate into Firefox:

1. Open your Mozilla Firefox web browser.
2. Click on the collapsed **menu icon** in the top-right of the window.
3. Click **Options**.
4. Click **Privacy & Security**.
5. In the **Certificates** area of the **Privacy & Security** tab, click **View Certificates...**
6. Select the **Your Certificates** tab and click **Import**.
7. Click **Browse** and locate your client certificate.
8. Select your certificate and click **Open**.
9. Provide the password used to secure the certificate.
10. Click **OK**.
11. Click **OK** again to close the **Certificate Manager**.

1.2.2.3 Chrome

To import your certificate into Chrome:

1. Open your Chrome web browser.
2. Click on the collapsed **menu icon** in the top-right of the window.
3. Click **Advanced** and then **Privacy and Security**.
4. Click **Manage certificates**.
5. Select the **Personal** tab and click **Import**.
6. In the **Certificate Import Wizard**, click **Next**.
7. Click **Browse** and locate your client certificate.
8. Select your certificate and click **Open**.
9. Click **Next**.
10. Provide the password used to secure the certificate and select any applicable import options.
11. Click **Next**.
12. Specify the location that the certificate should be stored.

    NOTE: Unless your administrator has specified otherwise, you should use the default option.

13. Click **Next**.
14. Click **Finish**.

1.2.2.4 Safari

Safari uses the Keychain Access Utility to manage digital certificates.

To import your certificate into the Keychain Access Utility:

1. Navigate to **Applications > Utilities > Keychain Access**.
2. Select **Login**.
3. Click **File > Import Items...**
4. Browse to the location of your client certificate.
5. Select your certificate and click **Open**.
6. Provide the password used to secure the certificate.
7. Click **OK**.

1.2.3 Mobile devices

1.2.3.1 Android Device

To import your certificate into your Android device:

1. Open the **Settings** app.
2. Tap **Security & location > Advanced > Encryption & credentials**.
3. Under the **Credential storage** area, tap **Install from storage**.

   NOTE: This path may vary depending on your device.
4. Browse to the location of your client certificate.
5. Select your certificate.
6. Provide the password used to secure the certificate.
7. Tap **OK**.

1.2.3.2 iPhone/iPad

To import your certificate into your iOS device:

1. Locate and open the .p12 file containing your certificate.

   NOTE: You may need to open the file using iOS Safari.
2. Tap **Install**.
3. Select **Install Now**.
4. Provide the password used to secure the certificate.
5. Tap **Next**.
6. Tap **Done**.

2

SSL certificates

This chapter describes how you enroll for SSL certificates and the subsequent steps required to install and configure your certificate on various email clients, browsers, and devices.

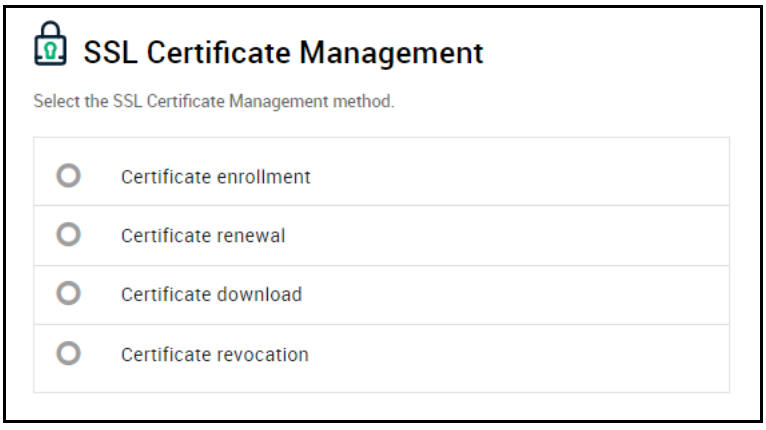
This chapter describes the following topics:

2.1 SSL certificate enrollment

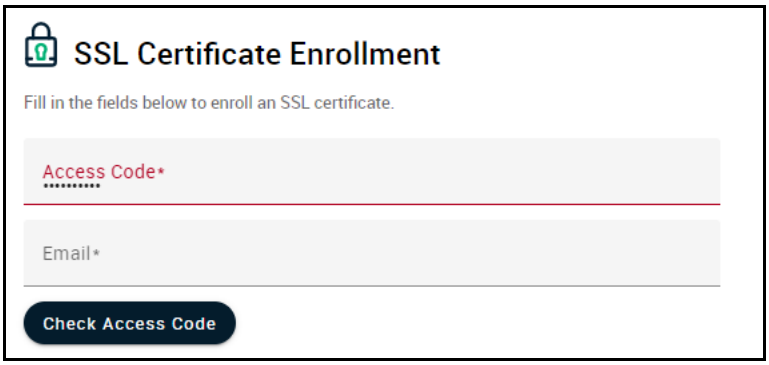
A certificate self enrollment request requires that an administrator provides you with the URL for the self enrollment form. The administrator must also provide you with the Access Code.

To enroll for a certificate:

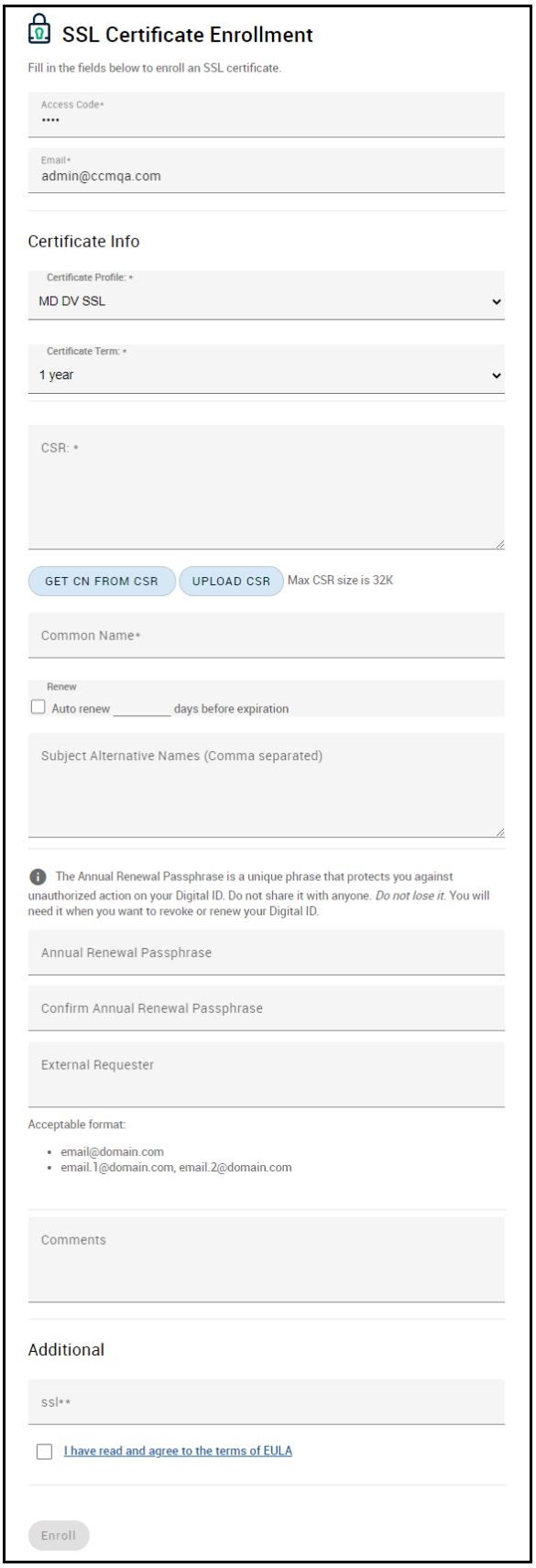
1. Navigate to the self enrollment form using the URL provided to you. The self enrollment landing page is shown in the following illustration.



2. Select **Certificate enrollment**. You will be redirected to the **SSL Certificate Enrollment** form shown in the following illustration.



3. Enter your **Access Code** and **Email**.
4. Click **Check Access Code** to continue to the self enrollment form shown in the following illustration.


SSL Certificate Enrollment
Fill in the fields below to enroll an SSL certificate.
Access Code*
••••
Email*
admin@ccmqa.com
Certificate Info
Certificate Profile: *
MD DV SSL
Certificate Term: *
1 year
CSR: *
GET CN FROM CSR
UPLOAD CSR
Max CSR size is 32K
Common Name*
Renew
Auto renew _____ days before expiration
Subject Alternative Names (Comma separated)
The Annual Renewal Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID.
Annual Renewal Passphrase
Confirm Annual Renewal Passphrase
External Requester
Acceptable format:
email@domain.com
email.1@domain.com, email.2@domain.com
Comments
Additional
ssl**
I have read and agree to the terms of EULA
Enroll

5. Complete the certificate enrollment fields using the following table.

Field[a]		Description
Access Code		The identifier for your particular organization or department. This code is used to authenticate certificate requests that are made using the self-enrollment form. This code should have been provided to you with the self enrollment form URL.
Email		Your email address for the domain belonging to your organization.
Address Details[b]		These fields are auto-populated from the details in the **General Settings** area of the organization or department on whose behalf the certificate request is being made. These fields cannot be modified. However, for OV certificates, you can choose to omit them from the certificate by selecting **Remove** beside the appropriate field. The allowed address details appear in the issued certificate and the removed details appear as omitted details. For EV certificates, these fields are mandatory.
	Address 1, Address 2, Address 3, City, State/Province, Postal Code	
Certificate Profile		The certificate profile to be issued. The certificate profiles available are configured by administrators in your organization.
Certificate Term		The life time of the certificate you select in the **Certificate Profile** list. The certificate terms are configured by administrators in your organization.
Server Software		The server software that is used to operate your web server.

Field[a]		Description
CSR		A CSR based on which Sectigo is to process your application and issue the certificate for the domain. The CSR can be entered either by pasting it directly into this field or by uploading the CSR as a .txt file using **Upload CSR**. In public key infrastructure systems, a CSR is a message sent from an applicant to a CA in order to apply for a digital identity certificate. Before creating a CSR, you first generate a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key selected by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the CA, and the CA may contact you to obtain additional information. Upon uploading or pasting the CSR, the form automatically parses the CSR. If you require assistance in generating a CSR, you should consult the Sectigo KnowledgeBase article for your web server type. In the case of applications for Multi-Domain Certificates (MDC), the CSR you generate only needs to be for a single common name (also known as the Primary Domain Name). You should type the additional domains that you require in the **Subject Alternative Name** field on this form.
	Get CN from CSR	Auto-populates the **Common Name** field upon the correct entry of the CSR, therefore ensuring the domain name in the application for matches the domain in the CSR. In the case of application for an MDC, you must list the additional domains in the SAN field of this form. If you created a CSR that already contains these SANs, clicking **Get CN from CSR** will auto-populate the **Subject Alternative Names** and the **Common Name** fields.
	Upload CSR	You can upload the CSR saved as a .txt file in the local computer instead of copying and pasting the CSR into the **CSR** field.
Common Name		The correct fully qualified domain name for the organization or department. The maximum allowed character length for this field is 64. For single domain certificates, it is the domain name in the format of example.com. For wildcard certificates, it is the domain name in the format of *.example.com. For MDC, it is the primary domain name in the format of example.com.
Renew		You can specify whether or not the certificate should be automatically renewed when it is nearing expiry. Specify the number of days in advance of expiry when the renewal process should start. On the scheduled day, SCM automatically submits the renewal application to the CA with a CSR generated using the same parameters as the existing certificate.
	Auto renew days before expiration	

Field[a]	Description
Subject Alternative Names (Mandatory for MDC)	If the **Certificate Profile** is set to Multi-Domain Certificate (MDC), then you should list the additional domains separated by commas.
Annual Renewal Passphrase	The passphrase needed to revoke the certificate when using the external revocation page.
Confirm Annual Renewal Passphrase	Confirmation of the passphrase.
External Requester	The full email address of the individual on behalf of whom you are submitting the application. The email address must be from the same domain for which the certificate is applied. The certificate collection email is sent to this email address.
Comments	Additional information that you want to provide the approving administrator.
Subscriber Agreement (EULA)	You must accept the terms and conditions before submitting the form by reading the agreement and clicking **I Agree**. The **Subscriber Agreement** differs depending on the SSL certificate selected from the **Certificate Profile** list. If Sectigo EV SSL certificate or Sectigo EV multi-domain SSL certificate is selected, **I Agree** is not shown and the agreement is accepted when the application is submitted.

a. In addition to the standard fields in the self-enrollment form, custom fields such as **Employee Code** and **Telephone** can be added an administrator.
b. The option to hide address fields is only available if configured for your organization or department.

6. Read the Subscriber Agreement and accept by selecting **I have read and agree to the terms of EULA**.
7. Click **Enroll**.

Once you have enrolled you will receive a notification confirming your enrollment and an email containing links to download your certificate in various formats.

2.2 SSL certificate installation

Once your certificate enrollment request has been approved and you have received your certificate, you will need to install it on the server for which the request generated. The steps to install your certificate are dependent on your web server. This section covers the following:

- Installing certificates on Apache HTTP server
- Installing certificates on Nginx
- Installing certificates on Microsoft IIS (8.x)

NOTE: Further instructions for installing certificates on different web servers can be found on the Sectigo KnowledgeBase.

2.2.1 Installing certificates on Apache HTTP server

The following sections provide instructions on the installation of SSL certificates on various Apache Linux distributions.

2.2.1.1 Configuring SSL certificates on Apache servers (Debian/Ubuntu)

To install certificates on your Apache (Debian/Ubuntu) server:

1. Ensure that you have the following files:
   - Private Key (generated with the CSR)
   - Server Certificate
   - Intermediate CA/Chain Certificate `.ca-bundle`.
2. Copy the files into your Linux server. It is recommended that you place these files in the following locations:
   - Server Certificate and Intermediate—`/etc/pki/tls/certs/`
   - Private Key—`/etc/pki/tls/private/`
3. Ensure that the Apache `mod_ssl` module is installed on the server. If the `mod_ssl` was not installed, install it by running the following command:

   ```
   #a2enmod ssl
   ```
4. Ensure that the default-ssl.conf file is enabled by running the following command:

   ```
   #a2ensite default-ssl
   ```
5. Edit the virtual host entry available in `/etc/apache2/sites-available/default-ssl.conf` to assign the Private Key, Certificate, and the Intermediate CA file to the configuration.

   NOTE: These instructions assume that you use the default configuration.

```
<VirtualHost *:443>
     SSLEngine On

     SSLCertificateFile /etc/pki/tls/certs/your_domain_name.crt
     SSLCertificateKeyFile /etc/pki/tls/private/private.key
     SSLCertificateChainFile /etc/pki/tls/certs/your_domain_name.ca-bundle

     ........
     ........
     ........
     ........
</VirtualHost>
```

6. To finalize the installation, restart the Apache service using the following the command:

   ```
   #service apache2 restart
   ```

2.2.1.2 Configuring SSL certificates on Apache servers (RedHat/CentOS/Fedora)

To install certificates on your Apache (RedHat/CentOS/Fedora) server:

1. Ensure that you have the following files:
   - Private Key (generated with the CSR)

- Server Certificate
- Intermediate CA/Chain Certificate `.ca-bundle`.

2. Copy the files into your Linux server. It is recommended that you place these files in the following locations:
   - Server Certificate and Intermediate—`/etc/pki/tls/certs/`
   - Private Key—`/etc/pki/tls/private/`
3. Ensure that the Apache `mod_ssl` module is installed on the server. If the `mod_ssl` was not installed, install it by running the following command:

   ```
   #yum install mod_ssl
   ```
4. Edit the virtual host entry available in `/etc/httpd/conf.d/ssl.conf` file to assign the Private Key, Certificate, and the Intermediate CA file to the configuration.

```
<VirtualHost *:443>
     SSLEngine On

     SSLCertificateFile /etc/pki/tls/certs/your_domain_name.crt
     SSLCertificateKeyFile /etc/pki/tls/private/private.key
     SSLCertificateChainFile /etc/pki/tls/certs/your_domain_name.ca-bundle

     ........
     ........
     ........
     ........
</VirtualHost>
```

5. To finalize the installation, restart the Apache service using the following the command:

   ```
   #systemctl restart httpd.service
   ```

2.2.2 Installing certificates on Nginx

To install certificates on your Nginx server:

1. Ensure that you have the following files:
   - Private Key (generated with the CSR)
   - Server Certificate
   - Intermediate CA/Chain Certificate `.ca-bundle`.
2. Copy the files into your Ngnix server. It is recommended that you place these files in the following locations:
   - Server Certificate and Intermediate—`/etc/nginx/ssl/example_com/`
   - Private Key—`/etc/nginx/ssl/example_com/`
3. Ensure that your nginx config points to the right certificate file and the to your private key:

   ```
   server {
   listen 443;
   server_name domainname.com;
   ssl on;
   ssl_certificate /etc/ssl/certs/ssl-bundle.crt;
   ssl_certificate_key /etc/ssl/private/domainname.key;
   ```

```
ssl_prefer_server_ciphers on;
}
```

NOTE: If you are using a multi-domain or wildcard certificate, it is necessary to modify the configuration files for each domain/subdomain included in the certificate. You need to secure and refer to the same certificate files in the VirtualHost record as described above.

4. (Optional) Enable OCSP Stapling. It is recommended that you enable OCSP Stapling which improves the SSL handshake speed of your website. Nginx has OCSP Stapling functionality for versions 1.3.7 or later.

   In order to use OCSP Stapling in Nginx, you must set the following configuration:

   ```
   ## OCSP Stapling
   resolver 127.0.0.1;
   ssl_stapling on;
   ssl_stapling_verify on;
   ssl_trusted_certificate <full path to the certificate bundle>;
   ```

   NOTE: For ssl_stapling_verify and ssl_stapling to work, you must ensure that all necessary intermediates and root certificates are installed. Furthermore, the resolver name may change depending on your environment.

5. After making changes to your configuration file, check for syntax errors with the following command:

   ```
   > sudo nginx -t -c /etc/nginx/nginx.conf
   ```

6. To finalize the installation, restart the Apache service using the following the command:

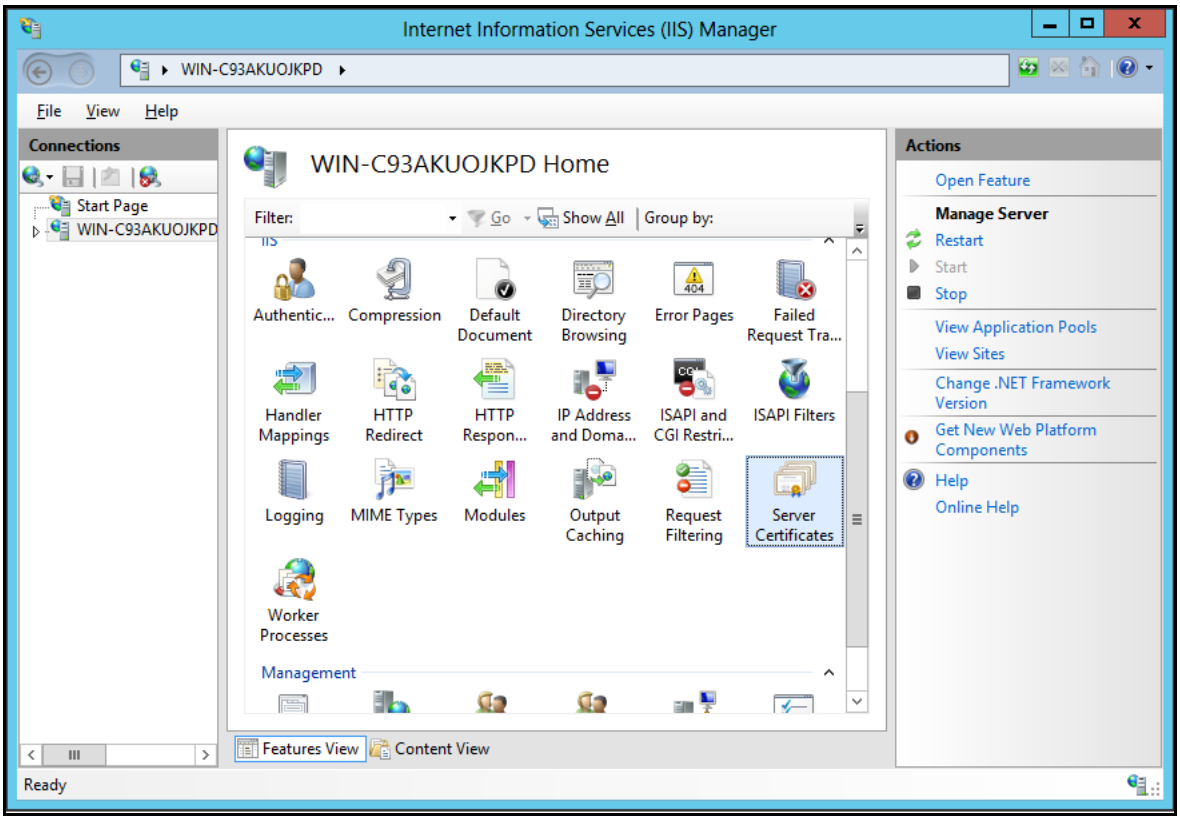
   > sudo /etc/init.x/nginx restart

7. (Optional) Verify that your certificate installation was completed correctly the test found at https://www.ssllabs.com/ssltest/.

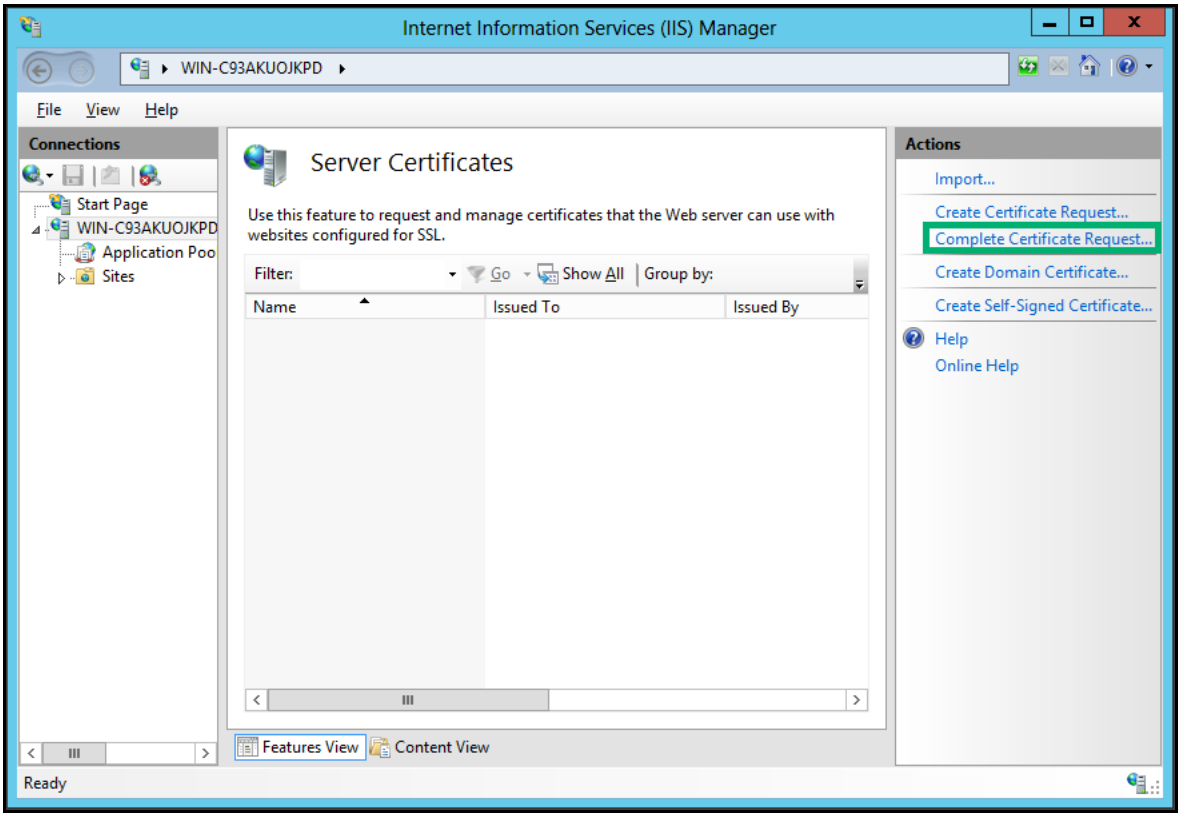
2.2.3 Installing certificates on Microsoft IIS (8.x)

To install certificates on your Microsoft IIS server:

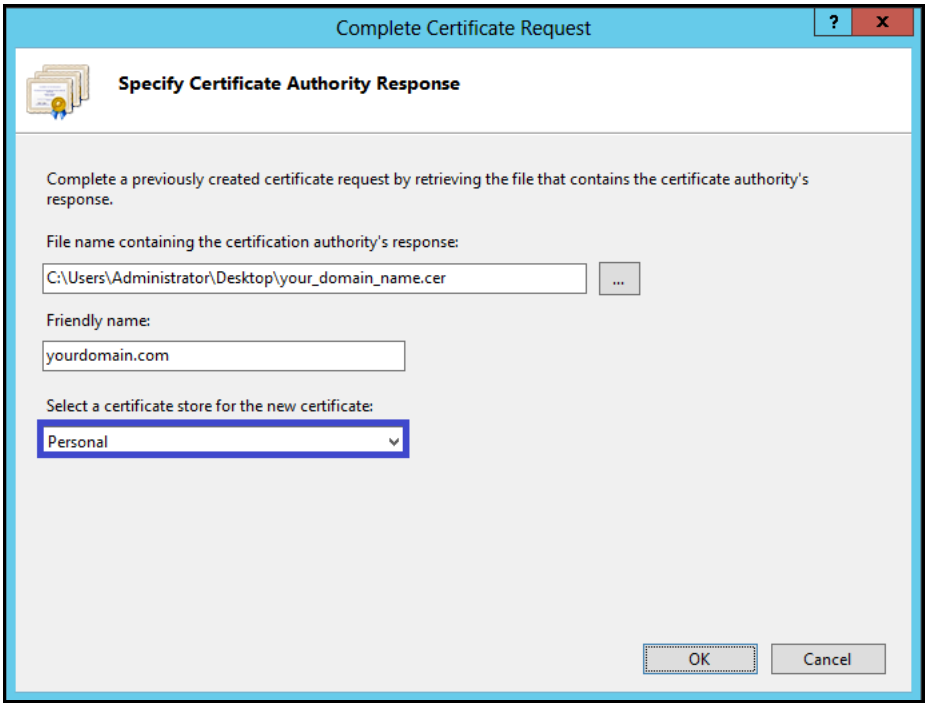
1. Open the .ZIP file containing your certificate and save the file as your_domain_name.cer to the desktop of the web servers.
2. Open the **Internet Information Services (IIS) Manager**.
3. Click on the server name.
4. Double-click **Server Certificates**.



5. In the **Actions** panel, click **Complete Certificate Request...**



6. Open the your_domain_name.cer file.
7. Enter a friendly name for the certificate. The friendly name is not part of the certificate itself and is used by server administrators to easily distinguish the certificate.
8. Select **Personal** certificate store.

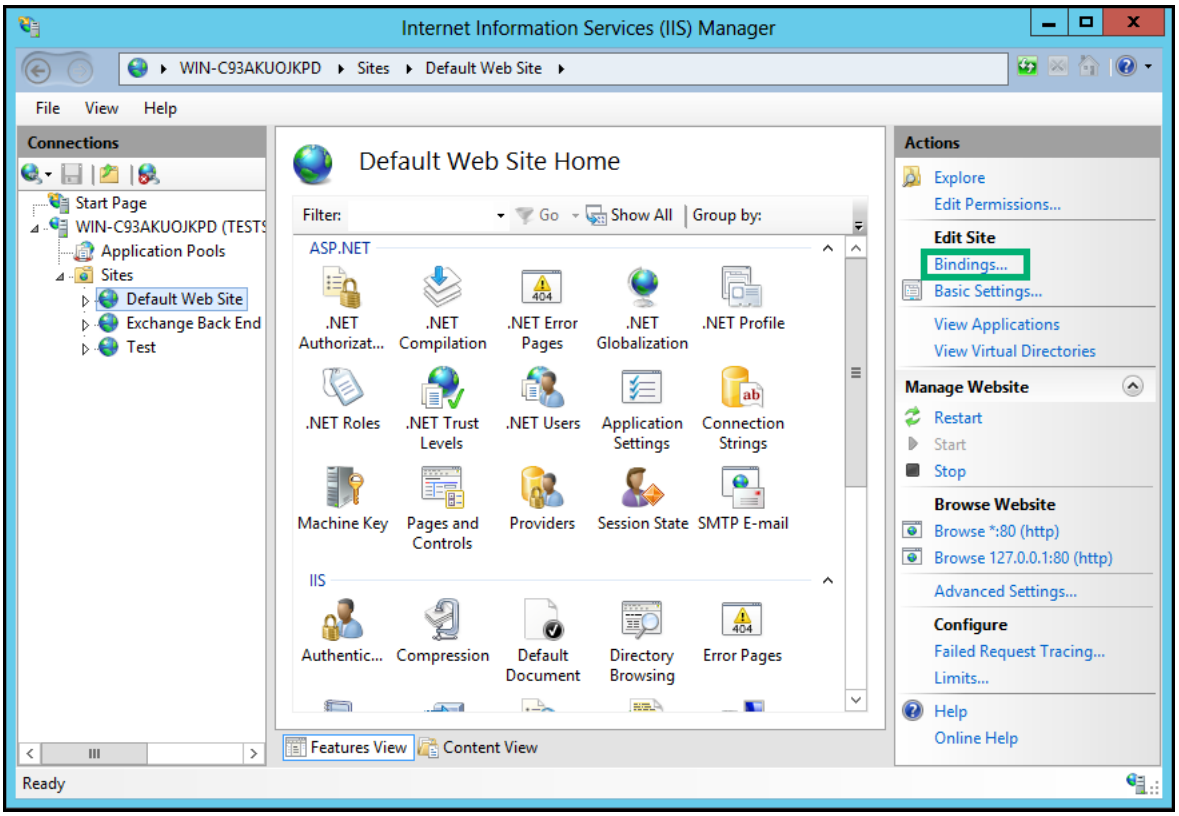


9. Click **OK**.

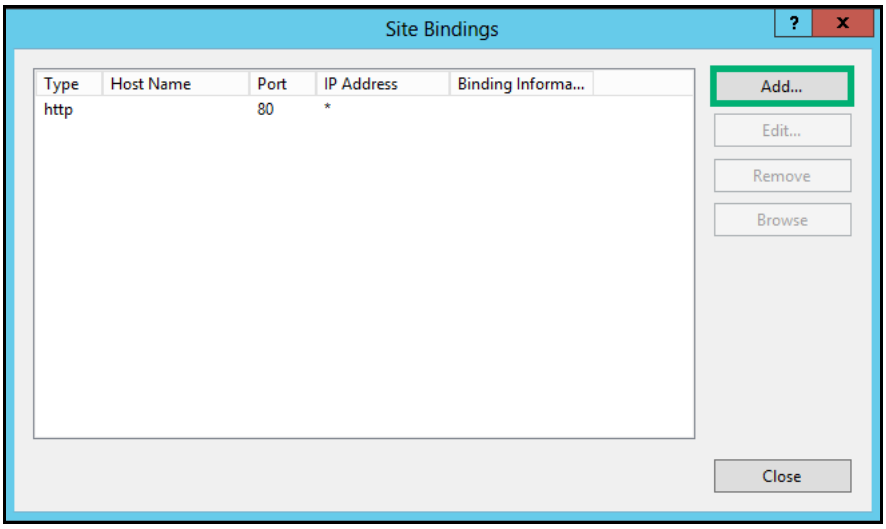
Once the certificate has been successfully installed on your sever, you must assign that certificate to the appropriate website using IIS.

To assign the certificate to a website:

1. Open the **Internet Information Services (IIS) Manager**.
2. In the **Connections** panel, select the name of the server to which the certificate was installed.
3. Under **Sites**, select the site to be secured with the certificate.
4. In the **Actions** panel, click **Bindings...**



5. Click **Add...**



6. For **Type**, select **https**.
7. For **IP address**, select **All Unassigned** or the IP address of the domain.
8. The **Port** over which traffic will be secured by SSL is usually 443.
9. For **Host name**:
    - Primary Domain: If you are assigning a certificate to your primary domain you can leave this section empty.

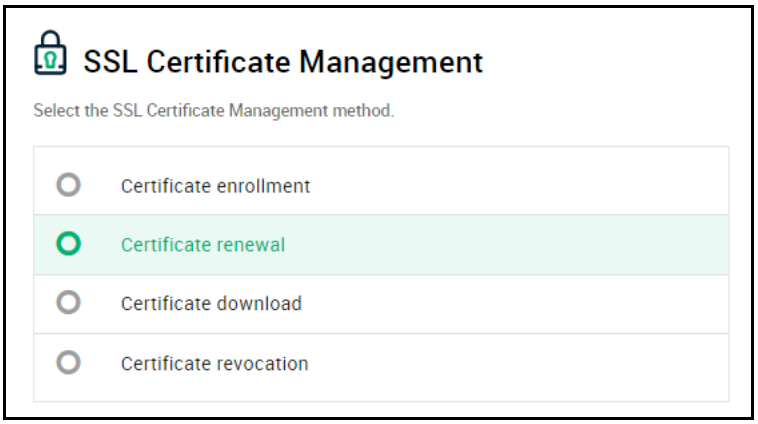
- Additional Domains: If you are assigning a certificate to any additional domains, you must enter the appropriate host name and select **Require Server Name Indication**.

10. For **SSL Certificate**, select your installed certificate.

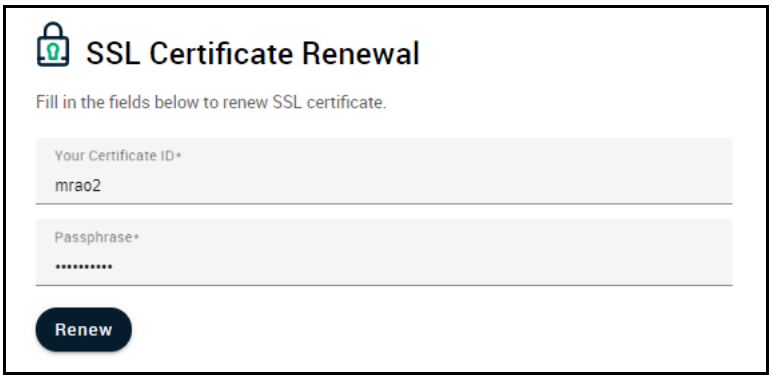
2.3 SSL certificate renewal

To manually renew a certificate:

Navigate to the self enrollment form using the URL provided to you. The self enrollment landing page is shown in the following illustration.



Select **Certificate Renewal**. You will be redirected to the **SSL Certificate Renewal** form shown in the following illustration.



11. Enter your Certificate ID and Passphrase.

    NOTE: The Certificate ID can be found in the certificate collection email you received during enrollment.

12. Click **Renew**.

3

Code Signing certificates

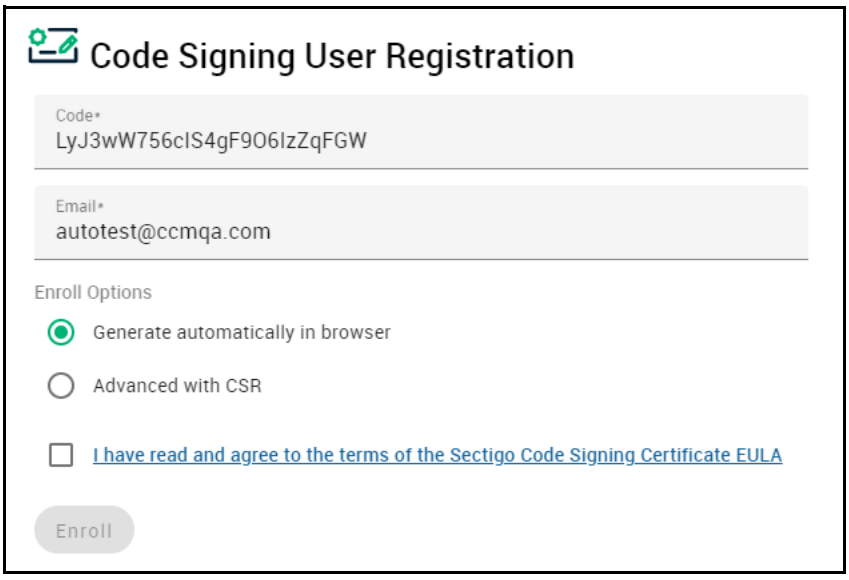
This chapter describes how you enroll for Code Signing certificates and the subsequent steps required to install your certificate.

This chapter describes the following topics:

3.1 Code Signing certificate enrollment

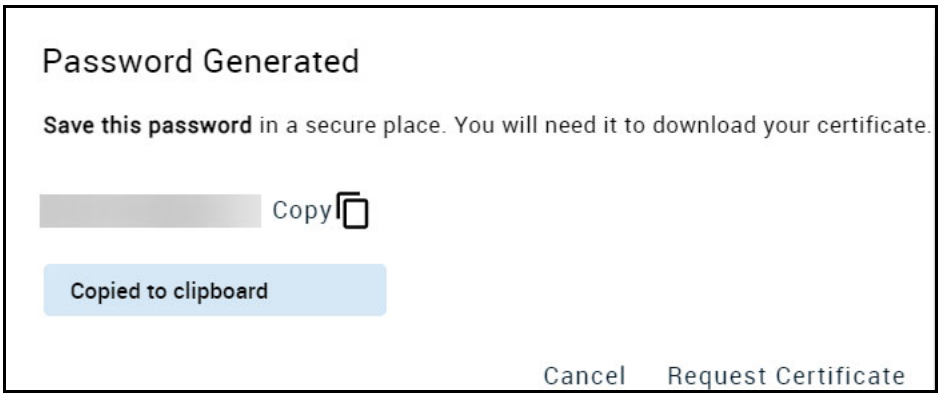
To begin the certificate enrollment process, your administrator should have sent you an invitation email, or provided you with a URL for accessing the self enrollment form.

1. Navigate to the self enrollment form using the URL provided to you in the email. You will be redirected to the **Code Signing User Registration** form shown in the following illustration.



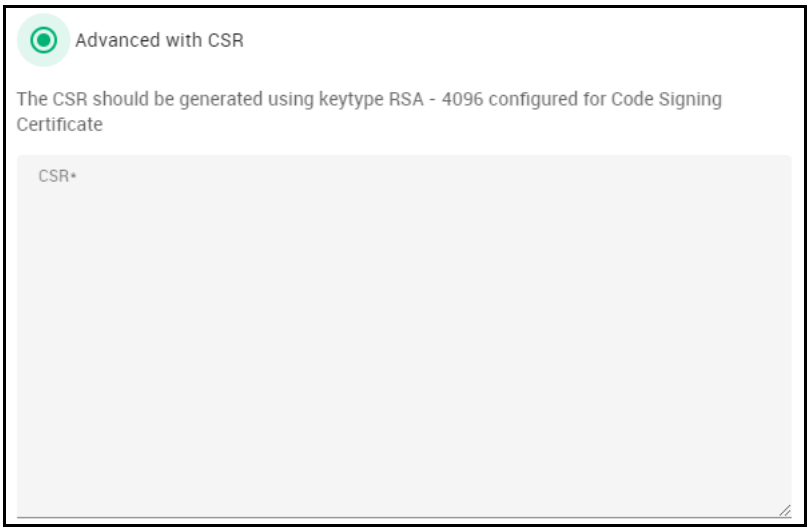
2. Your code and email address will be automatically completed into the appropriate fields.
3. Select the appropriate enroll option.
4. Read and agree with the EULA.
5. Click **Enroll**.

   If you selected **Generate automatically in browser**, the following form will open:



NOTE: Be sure to save the generated password. You will need to enter this password when downloading your certificate.

If you selected Advanced with CSR, you will be prompted to enter the CSR that was generated using RSA keytype.

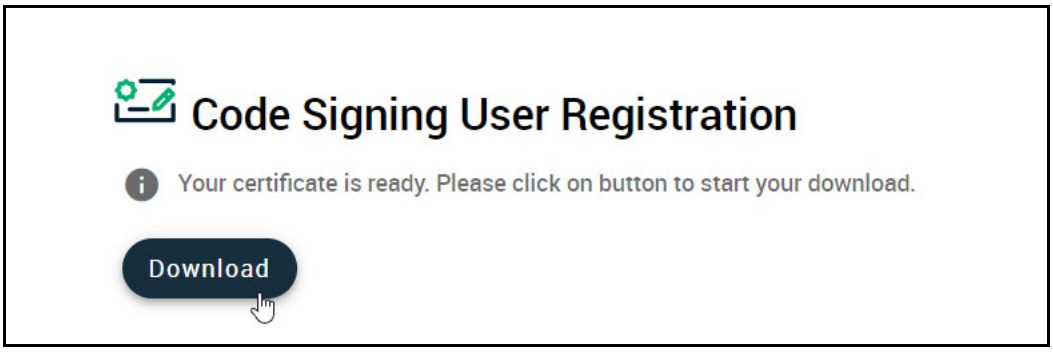


6. Click **Request Certificate**.

The message that your application was accepted will appear. You will be notified by email when your certificate is ready for collection.

To collect your certificate:

1. Click on the link provided in the email. You will be prompted to enter the password that was generated from the **User Registration** page.
2. Click **Download** and install your certificate.



3.2 Code Signing certificate collection and installation

Once your certificate enrollment request has been approved and you have downloaded your certificate, you will need to install it to your browser. If you require help with the installation of your code signing certificate, contact Sectigo Support. Once installed, the certificate will be available for digitally signing and encrypting your software and applications.

4

Device certificates

This chapter describes how you enroll for Device certificates and the subsequent steps required to install and configure your certificate on various devices.

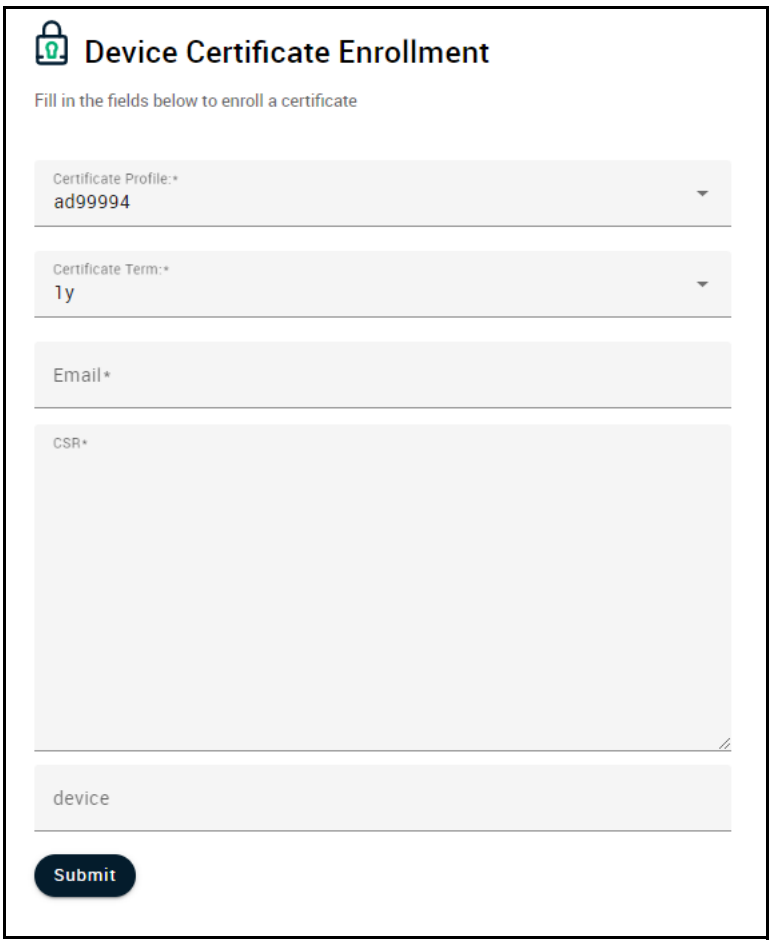
This chapter describes the following topics:

4.1 Device certificate enrollment

A certificate self enrollment request requires that an administrator provides you with the URL for the self enrollment form.

To enroll for a certificate:

1. Click the URL provided to you. You will be redirected to the device certificate enrollment form shown in the following illustration.



2. Complete the certificate enrollment fields using the following table.

Field	Description
Certificate Profile	The certificate profile to be issued. The certificate profile available are configured by administrators in your organization.
Certificate Term	The lifetime of the certificate you select in the **Certificate Profile** list. The certificate terms are configured by administrators in your organization.
Email	Your email address for the domain belonging to your organization. The certificate collection email will be sent to this email.

Field	Description
CSR	A CSR based on which Sectigo is to process your application and issue the certificate for the domain. The CSR can be entered by pasting it directly into this field. In public key infrastructure systems, a CSR is a message sent from an applicant to a CA in order to apply for a digital identity certificate. Before creating a CSR, you first generate a key pair, keeping the private key secret. The CSR contains information identifying the applicant (such as a directory name in the case of an X.509 certificate), and the public key selected by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request. The CSR may be accompanied by other credentials or proofs of identity required by the CA, and the CA may contact you to obtain additional information. Upon pasting the CSR, the form automatically parses the CSR. If you require assistance in generating a CSR, you should consult the Sectigo KnowledgeBase article for your web server type.

3. Click **Submit**.

Once you have enrolled, you will receive a notification confirming your enrollment and an email containing links to download your certificate in various formats.

4.2 Device certificate collection and installation

Once your certificate enrollment request has been approved and you have downloaded your certificate, you will need to install it. The steps to install your certificate depend on your device. Refer to your device vendor's documentation on how to install the **Device Certificate** on your device.