



Comodo Certificate Manager

Version 5.6

SSL Certificates Enrollment, Collection, Installation and Renewal

Guide Version 5.6.012317

Enrolling For Your Certificate

This step-by-step guide will explain how to enroll for then collect and install an SSL certificate on your web server.

Step 1: The provisioning email and authentication

Firstly, your SSL administrator should have sent you a certificate provisioning email. This email will contain two important items:

- A link to the certificate enrollment/renewal pages. The URL will be similar to https://cert-manager.com/customer/<company_name>/ssl
- An access code which will be used to authenticate you before you can proceed to the enrollment form.
- Click the enrollment link in your mail to open the authentication screen:



The screenshot shows the 'COMODO Certificate Manager' interface. Under the heading 'SSL Enrollment', there are two input fields. The first is labeled 'Access Code: *' and contains six black dots. The second is labeled 'Email: *' and contains the text 'johnsmith@ditherscons.com'. Below these fields is a blue button labeled 'CHECK ACCESS CODE'.

- Copy and paste the code from your email into the 'Access Code' field.
- Enter your email address in the space provided. This email address must be on the same domain as the certificate for which you are applying. For example, if you are applying for a certificate for www.company.com, then the email address entered here must be something like yourname@company.com. You must also be able to receive mail at this address.
- Click 'Check access code' to verify your application. Please contact your SSL administrator if authentication fails.
- If authentication is successful, you will proceed to Step 2: The self-enrollment form:

Step 2: The Self-Enrollment Form

You need to fill out all fields in order to submit the form. After submitting, your application will be sent to your SSL administrator for approval and issuance. Advice on all fields on this form is available directly below the screenshot.

COMODO
Certificate Manager

SSL Enrollment

Access Code: *

Email: * johnsmith@ditherscons.com

[Click here to edit address details](#)

Certificate Type: * Instant SSL

Certificate Term: * 1 year

Server Software: * AOL

CSR: *
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAbOCADCBjTELMAkGA1UEBhMCVVMxEjAQBgNVBAMTCWNj
bXFhLnNvbTES
MBAGA1UEBxMjUml12ZXJkYXZlbnN0cnVjdGlv
biBDb21wYW55MRAwDgYDVQQIEwdBbGF1YW1hMR0wGwYDVQQLExRQ

[GET CN FROM CSR](#) [UPLOAD CSR](#) Max CSR size is 32K

Common Name: * ditherscons.com

Please provide a Self Enrollment Passphrase. A passphrase is necessary for certificate revocation and renewal.

Self Enrollment Passphrase: *

Re-type Self Enrollment Passphrase: *

Comments:

Subscriber Agreement

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE
READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND
CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS
CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE
MANAGER ACCOUNT OR THE
CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR,
ACCESSING, OR
PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR
ACCESSING CERTIFICATE
MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON 'I
ACCEPT' BELOW, YOU
ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND
THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS

[PRINT](#)

☒ I Agree.*

Scroll to bottom of the agreement to activate check box.

[ENROLL](#) [RESET](#)

The external applicant need not be an existing user in the CM, but the person's email address must be from the same domain as the common name, else the application cannot proceed.

Clicking 'Get Common Name from CSR' will automatically populate the 'Common Name' field and if relevant, the 'SAN' field with the domain name(s) in the CSR - Helping to avoid errors. This feature is especially useful while applying for MDCs where the application could contain upto 100 domains in the SAN field.

The applicant can directly upload the CSR saved as .txt file by clicking 'Upload CSR'. The CSR field will be auto-populated with the CSR from the text file.

The Passphrase entered here is required for the purposes of certificate revocation.

The applicant must accept the 'Terms and Conditions' before submitting the form. The 'I Agree' checkbox becomes active only on scrolling down the page till the end.

Application form for an OV certificate

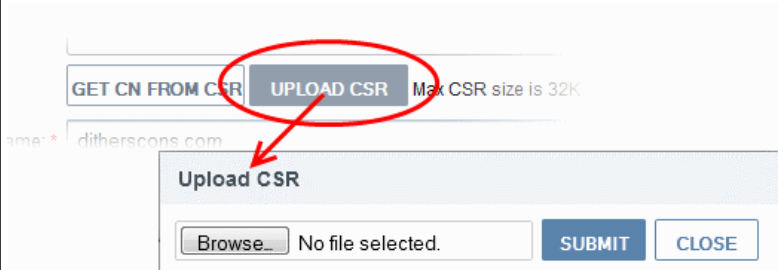
Form notes and advice

- The 'Access Code' and 'E-mail' address fields will be pre-populated as you entered them previously.

- The EV application form contains additional fields related to Incorporating Agency and certificate requester, approver and signer. The MDC form contains an additional SAN field so you can add multiple domain names.
- In addition to the standard fields in the enrollment form, additional custom fields such as 'Telephone No.' 'Employee Code' may also be displayed depending on how the administrator has configured it.
- Comodo provides a range of CSR generation documents designed to assist with the CSR creation process at https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,96,1
- After you have successfully submitted the form, your application will go for approval by your SSL administrator. Once approved, your certificate request will be forwarded to Comodo CA for issuance and you will be notified by email when it is ready for collection. Help on certificate collection and installation are in the section that comes after this table:

Form Element	Type	Description
Access Code (required)	Text Field	<p>An Access Code identifies a particular Organization or Department and is used to authenticate certificate requests that are made using the Self-Enrollment form.</p> <p>Organizations and Departments are uniquely identified by combination of the Organization's 'Access Code' and the 'Common Name' (domain) specified in 'General' properties. Multiple Organizations or Departments can have the same Access Code OR the same Common Name - but no single entity can share both.</p> <p>Administrators should choose a complex Access Code containing a mixture of alpha and numeric characters that cannot easily be guessed. This code should be conveyed to the applicant(s) along with the URL of the sign up form.</p> <p>Applicants that request a certificate using the Self Enrollment Form will need to enter this code.</p>
Email (required)	Text Field	Applicant should enter their full email address. The email address must be for a domain that has been assigned to the Organization or Department.
Address Details Displayed on clicking the Click here to edit address details link. Address 1: Address 2: Address 3: City: State or Province: Postal Code: (all auto-populated)	Text Fields	<p>Clicking the link Click here to edit address details displays the address fields.</p> <p>The address fields are auto-populated from the details in the 'General Settings' tab of the Organization or Department on whose behalf this certificate request is being made.</p> <p>These fields cannot be modified but, in the case of OV level certificates, the applicant can choose to omit them from the certificate by selecting the 'Remove' checkbox next to the fields.</p> <p>The allowed address details will appear in the issued certificate and the removed details will appear as "Details Omitted".</p> <p>For EV level certificates, it is mandatory to include and display address details of the Organization, Incorporation or Registration Agency, Certificate Requester and the Contract Signer. Therefore text fields for entering the these address details will be displayed and the option to remove certain fields is not available on the EV self-enrollment form on selecting Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate from the 'Certificate Type' drop-down.</p>

Form Element	Type	Description
Certificate Type (<i>required</i>)	Drop-down list	<p>Applicant should select certificate type. For a list of Comodo SSL certificate types, see the section Comodo SSL Certificates.</p> <p>The specific certificate types displayed in the drop-down list (and therefore available to the applicant) can be customized according to the needs of the Organization. Please refer to sections Creating a new Organization, Customize an Organization's SSL Certificate Types and SSL Types for more details.</p>
Certificate Term (<i>required</i>)	Drop-down list	Applicant should select the life time of the certificate chosen from the 'Certificate Type' drop-down.
Server Software (<i>required</i>)	Drop-down list	<p>Applicant should select the server software that is used to operate their web server (for example, Apache, IIS etc). Installation support documentation is available from the Comodo's support portal here:</p> <p>https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav=0</p>
CSR (<i>required</i>)	Text Field	<p>A Certificate Signing Request (CSR) is required to be entered into this field in order for Comodo CA to process your application and issue the certificate for the domain.</p> <p>The CSR can be entered in two ways:</p> <ul style="list-style-type: none"> Pasting the CSR directly into this field Uploading the CSR saved as a .txt file by clicking the 'Upload CSR' button <p>Background:</p> <p>In public key infrastructure systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. Before creating a CSR, the applicant first generates 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 chosen 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 certificate authority, and the certificate authority may contact the applicant for further information. Upon uploading or pasting the CSR, the form will automatically parse the CSR.</p> <p>Administrators that require assistance to generate a CSR should consult the Comodo knowledge article for their web server type here:</p> <p>https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=33&pcid=1&nav=0,1</p> <p>Special Note regarding MDC applications: The CSR you generate only needs to be for the single 'Common Name' (aka the 'Primary Domain Name'). You should type the additional domains that you require in the 'Subject Alternative Name' field' on this form.</p>

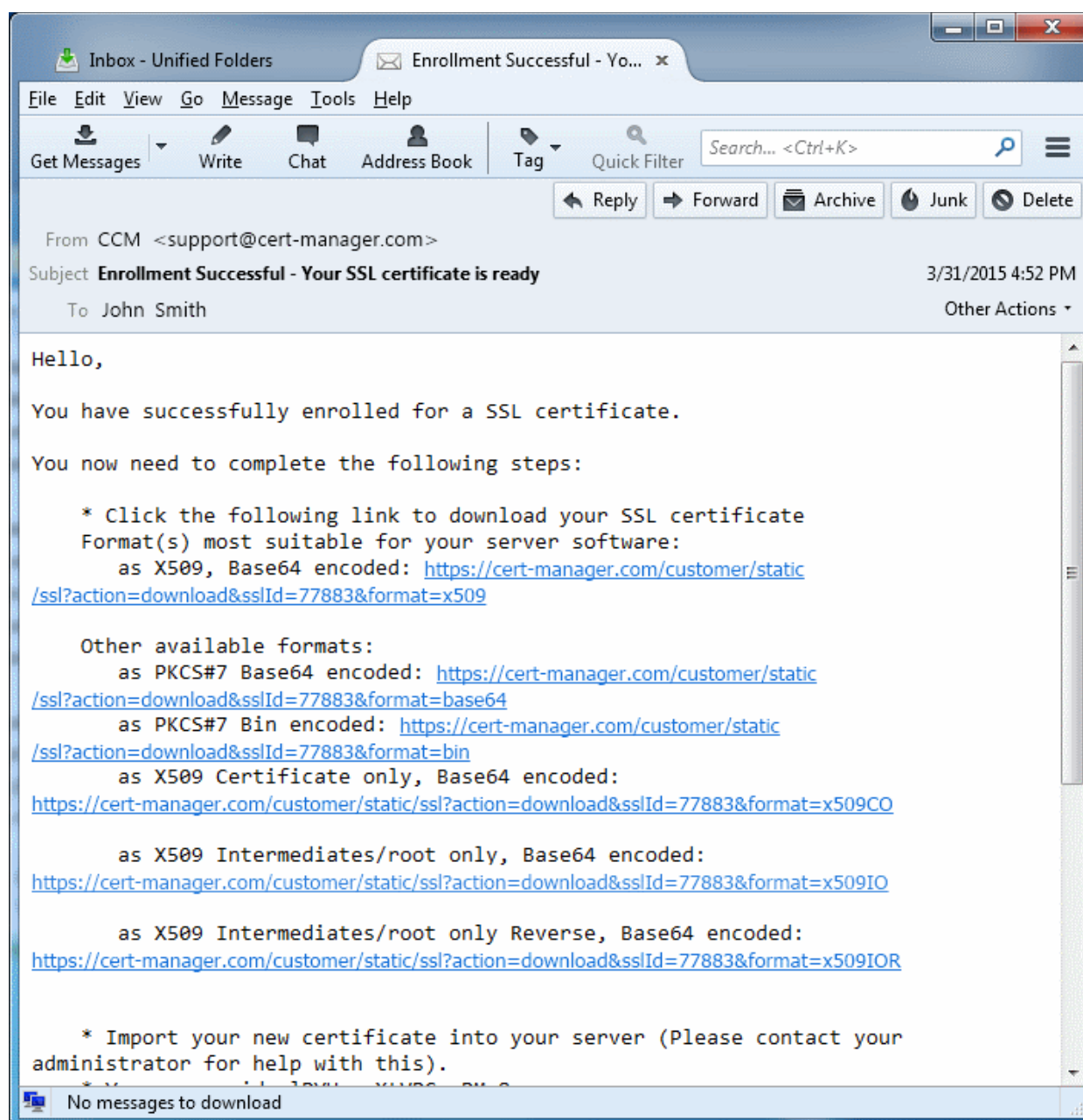
Form Element	Type	Description
Get CN from CSR (<i>optional</i>)	Control	<p>Once the CSR has been entered correctly, clicking this button will auto-populate the Common Name (CN) field. Using this method helps to avoid human error by ensuring the domain name mentioned in the application form exactly match that in the CSR. If the domain name mentioned in this application form do not match that in the CSR, then Comodo CA will not be able to issue the certificate.</p> <p>Special Note regarding MDC applications: In order to successfully order a Multi-Domain Certificate, the applicant need only list the additional domains in the SAN field on this form. In certain circumstances, however, the applicant may have created a CSR that already contains these Subject Alternative Names. In this case, clicking the 'Get CN from CSR' button will also auto-populate the 'Subject Alternative Names' form fields as well as the 'Common Name' field.</p>
Upload CSR (<i>optional</i>)	Control	<p>The applicant can upload the CSR saved as a .txt file in the local computer, instead of copying and pasting the CSR into the CSR field - helping to avoid errors.</p> 
Common Name (<i>required</i>)	Text Field	<p>Applicants should enter the correct fully qualified domain name for the Organization or Department</p> <p>Single Domain certificates - enter domain name using the form: domain.com.</p> <p>Wildcard Certificates - enter domain name using the form: *.domain.com.</p> <p>Multi-Domain Certificates - enter the primary domain name using the form: domain.com.</p>
Subject Alternative Names (<i>required for Multi-Domain certificates</i>)	Text Field	<p>If the certificate 'Type' is a Multi-Domain Certificate (MDC) then the applicant should list the 'Subj Alt Name' additional domains here. Each domain listed in this field should be separated by a comma.</p>
Self Enrollment Pass Phrase (<i>optional</i>)	Text Field	<p>This phrase is needed to revoke the certificate when using the external revocation page at: https://cert-manager.com/customer/real_customer_uri/ssl?action=revoke</p>
Re-type Self Enrollment Pass Phrase (<i>required if specified in the field above</i>)	Text Field	<p>Confirmation of the above.</p>
Comments (<i>optional</i>)	Text Field	<p>Applicant can enter information for the administrator.</p>

Form Element	Type	Description
Subscriber Agreement	Checkbox	Applicant must accept the terms and conditions before submitting the form by reading the agreement and clicking the 'I Agree' checkbox. Note: The Subscriber Agreement will differ depending on the type of SSL certificate selected from the 'Certificate Type' drop-down. If Comodo EV SSL Certificate or Comodo EV Multi-Domain SSL Certificate is selected, The 'I Agree' checkbox will not be shown and the agreement will be taken as accepted, when the user submits the application.
Enroll	Control	Submits the application and enrolls the new certificate request.
Reset	Control	Clears all data entered on the form.

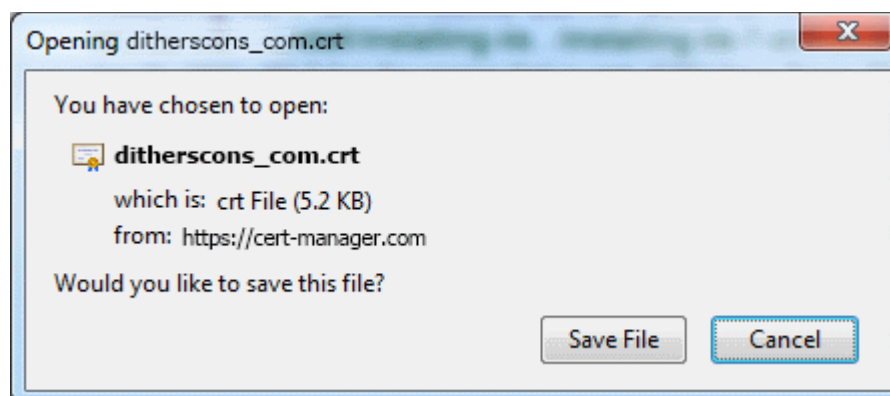
Certificate Collection and Installation

The next stage of the process is to download your certificate then install it on your web-server.

Once your certificate has been validated and issued you will receive a certificate collection email. The email will contain a summary of certificate details and a link to the certificate download page. This link also contains a unique ID that will be used to verify the download.



- Having clicked the link in the collection email, you will be able to download the certificate file.



Next, you need to install the certificate. The precise installation process will depend on which type of web server you use to host your site. The following page contains a list of tutorials covering certificate installation on a wide range of web servers:

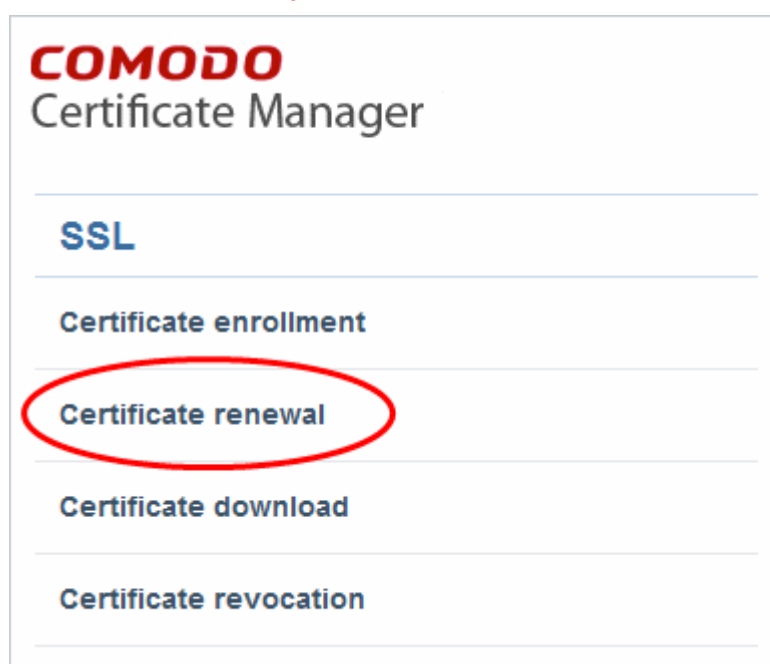
https://support.comodo.com/index.php?_m=knowledgebase&_a=view&parentcategoryid=1&pcid=0&nav

Renewing Your Certificate

You can renew certificates which are about to expire by entering the Self Enrollment Certificate ID and the renewal pass-phrase of the certificate in the Self-Renewal form. The Self Enrollment Certificate ID can be found in the certificate collection email you received during enrollment. The renewal pass-phrase is the one you entered in the self-enrollment form, while enrolling for the certificate. Please contact your administrator if you do not have access to either of these pieces of information.

Accessing the Self Renewal Form

The Self Renewal form is available at the same URL of the Self Enrollment form. The URL will be *similar* to https://cert-manager.com/customer/<company_name>/ssl



The screenshot shows the 'COMODO Certificate Manager' interface. Under the 'SSL' section, there are five links: 'Certificate enrollment', 'Certificate renewal' (which is circled in red), 'Certificate download', and 'Certificate revocation'.

- Clicking the 'Certificate renewal' link will open the self renewal form



The screenshot shows the 'COMODO Certificate Manager' interface for the 'SSL Renew' form. It contains two input fields: 'Your Certificate ID: *' with the value '77881' and 'Pass-phrase: *' with masked characters. A 'RENEW' button is located at the bottom right of the form.

Form Element	Description
Your Certificate ID (required)	Please enter the correct self enrollment certificate ID. The certificate ID is available from certificate collection email received during enrollment.

Form Element	Description
	Tip: If you do not have the certificate collection email or the self enrollment ID, you can request your SSL administrator for the same, by providing your certificate details. The administrator can refer to the Comodo Certificate Manager interface and can communicate the ID to you.
Pass-phrase <i>(required)</i>	Please enter renewal/revocation passphrase you entered in the self-enrollment form, while enrolling for the certificate.

- Filling up the 'SSL Renew' form and clicking 'Renew' will automatically renew the certificate with the same details as in the existing certificate.
- Once issued, the renewal certificate can be collected and installed. Refer to the section **Certificate Collection and Installation** for more details.

Appendix - Certificate Types

If you do not know which type of certificate to choose then we recommend that you first contact your SSL admin who should be able to advise you. This appendix is provided only to give applicants an understanding of the different types of certificate that are available but does not cover pricing or warranty levels. The appendix opens with a definition of terms that should provide an insight into SSL terminology and concludes with a table listing all certificates offered by Comodo CA. Note – this is a *complete* list of Comodo certificates. You might not see all of these certificate types if your administrator hasn't made them available.

Validation Levels

OV: **Organization Validated** certificates include full business and company validation from a certificate authority using currently established and accepted manual vetting processes.

EV: **Extended Validation** certificates provide the highest levels of trust and reassure web site visitors that it is safe to trade by turning the address bar green during https sessions. EV's are generally more expensive than OV level certificates and require a more in-depth validation process prior to issuance. However, because the green bar has become a hallmark of security seen on the Internet's largest and most prestigious websites, placing an EV on your website can often lead to increased customer conversion.

Certificate Types

SDC: **Single Domain Certificates** - will secure a single fully qualified domain name such as www.company.com

WC: **Wildcard Certificates** - will secure the domain and unlimited sub-domains of that domain

MDC: **Multi-Domain Certificates** - will secure up to 100 different domain names on a single certificate

Additional Technologies

SGC: **Server Gated Cryptography**. SGC technology upgrades the encryption capabilities of older browsers to modern day standards

Certificate Name	Type	Validation Level	Description	Maximum Term Length
Comodo Trial SSL Certificate	SDC	OV	Secures a single domain	30 days
Comodo Intranet SSL Certificate	SDC	OV	Secures a single internal host	1 year - 3 years
Comodo InstantSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo InstantSSL Pro Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo PremiumSSL Legacy Certificate	SDC	OV	Secures a single domain	1 year - 3 years
Comodo PremiumSSL Legacy Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo SGC SSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years

Certificate Name	Type	Validation Level	Description	Maximum Term Length
Comodo SGC SSL Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
EliteSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
GoldSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
PlatinumSSL Certificate	SDC	OV	Secures a single domain	1 year - 3 years
PlatinumSSL Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
PlatinumSSL Legacy Certificate	SDC	OV	Secures a single domain	1 year - 3 years
PlatinumSSL Legacy Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
PlatinumSSL SGC Certificate	SDC	OV	Secures a single domain	1 year - 3 years
PlatinumSSL SGC Wildcard Certificate	WC	OV	Secures domain and unlimited sub-domains of that domain	1 year - 3 years
Comodo Multi-Domain SSL Certificate	MDC	OV	Secure multiple Fully Qualified domains on a single certificate	1 year – 3 years
Comodo EV SSL Certificate	SDC	EV	Secures a single domain	1 year - 2 years
Comodo EV SGC SSL Certificate	SDC	EV	Secures a single domain	1 year - 2 years

About Comodo

The Comodo organization is a global innovator and developer of cyber security solutions, founded on the belief that every single digital transaction deserves and requires a unique layer of trust and security. Building on its deep history in SSL certificates, antivirus and endpoint security leadership, and true containment technology, individuals and enterprises rely on Comodo's proven solutions to authenticate, validate and secure their most critical information.

With data protection covering endpoint, network and mobile security, plus identity and access management, Comodo's proprietary technologies help solve the malware and cyber-attack challenges of today. Securing online transactions for thousands of businesses, and with more than 85 million desktop security software installations, Comodo is Creating Trust Online®. With United States headquarters in Clifton, New Jersey, the Comodo organization has offices in China, India, the Philippines, Romania, Turkey, Ukraine and the United Kingdom.

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: +1.888.266.6361

Tel: +1.703.581.6361