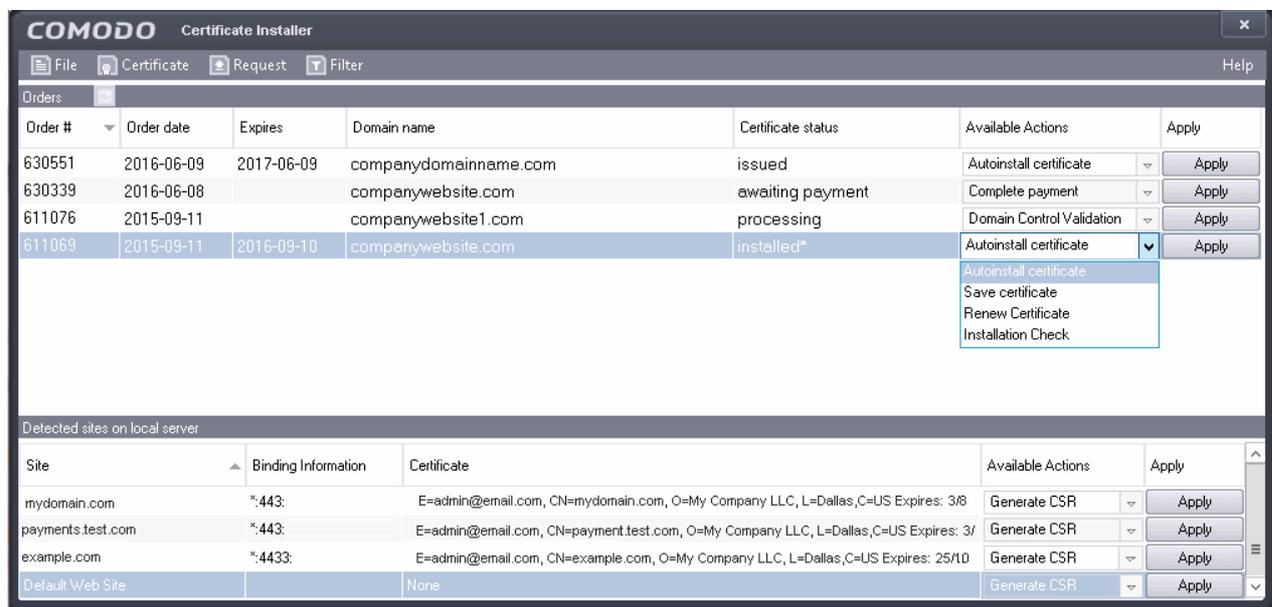


Overview and Tutorial

Comodo Certificate Auto-installer is an easy-to-use utility which simplifies the often complex process of obtaining and installing an SSL certificate on IIS/Apache web-servers. The utility allows you to:

- Create a certificate signing request and automatically submit it to Comodo
- Use one of three methods to complete Domain Control Validation
- Automatically install the certificate on your website
- Bind the certificate to an IIS domain (if this has not been done already)
- Purchase new certificates using in-app ordering
- Renew or replace certificates that are close to expiry
- Obtain a free, 90-day, Comodo certificate



Prerequisites:

Apache

- Your sites are hosted on an Apache web server on Linux (CentOS, Fedora, Ubuntu or Debian)
- You install the utility on a Windows 7/8/10 or Windows Server 2008-2012 R2 machine. Ensure .NET framework 4.0 is enabled on the Windows machine.
- Once installed, you can remotely login to your web server from the utility.
- The user that logs in should have SSH access with sudo privileges. If the SSH user does not have sudo privileges, then all keys and certificates will be placed in the home directory.

IIS

- You are running either Microsoft IIS 7.x or 8.x (Server 2008 - 2012R2). IIS 6.x (Server 2003) and below is not supported
- You must run this utility on the web-server on which you wish to install the certificate
- Your host has .NET framework version 3.5.1 or above

This document contains the following sections:

- **Download, install and run the utility**
 - **Connect to an Apache Server**
- **The main interface / actions and statuses**
- **Tutorial**
 - **Step 1 - Generate and submit a CSR**
 - **Step 2 - Complete Domain Control Validation (DCV)**
 - **Step 3**
 - **Install and bind a certificate - IIS**
 - **Install and bind a certificate - Apache**
- **Renew a certificate**
- **Buy a certificate**
- **Complete your order**
- **Generate a CSR**
- **Get a free certificate**
- **Order a certificate by redeeming a Comodo voucher**

Download, install and run the utility

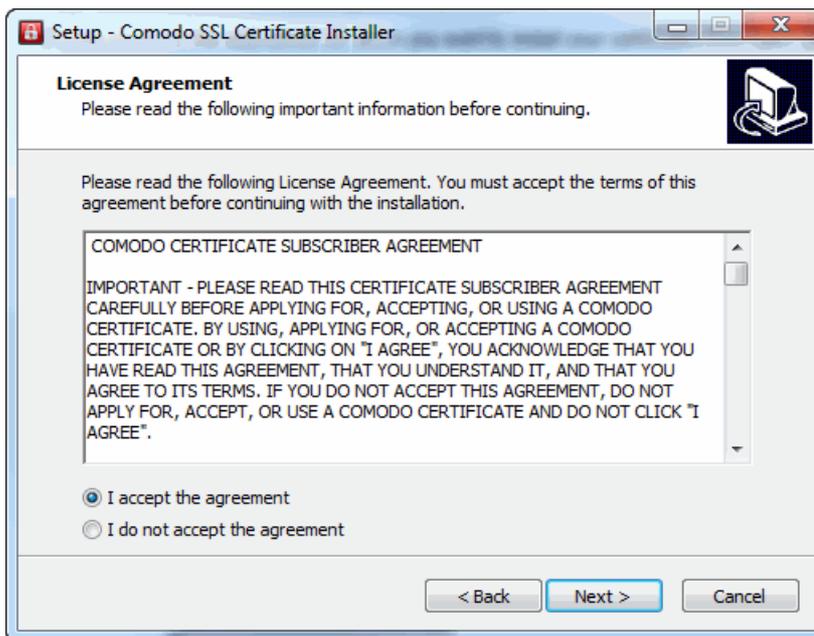
The certificate auto-installer can be downloaded from:

http://download.comodo.com/ssl_autoinstaller/ComodoSSLCertificateInstallerSetup.exe

- **Apache** – Install the utility on a Windows 7/8/10 or Server 2008/2012 R2 machine. You will remotely connect to your web server from within the utility. The next section offers advice on connecting.
- **IIS** - Install the utility directly on the web server on which you want to install your certificates.



Click 'Next' to continue.



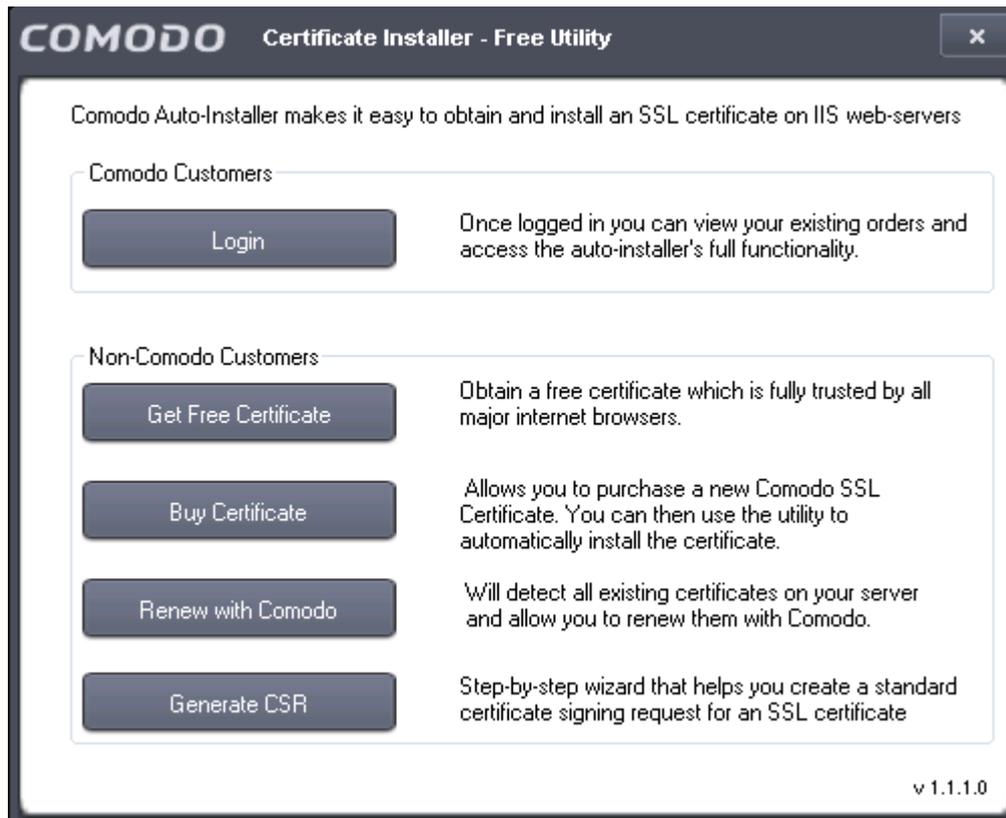
After agreeing to the user license, you will be asked to choose where to install the utility and to confirm start menu options before continuing to the setup review screen:



Click 'Install' to continue to begin installation.

- IIS users, the utility requires .NET Framework versions 3.5.1 or above. To enable this on IIS, select Start > All Programs > Administrative Tools > Server Manager > Features > Add Features and select your .NET framework.

Once installation is complete, start Comodo Auto-Installer from the start menu, the quick-launch icon or by double clicking the desktop shortcut. This will open the launch menu:



Comodo Customers - Please choose one of the following options:

- **Login** - Log in with your Comodo account user-name and password and a certificate order number to view the status of your orders, generate a CSR and install / buy / renew certificates:

- **Login with voucher** – (Comodo partners only). Allows you to redeem a Comodo voucher for a pre-paid SSL certificate. After clicking this button you will be asked to enter your voucher and verification codes before moving onto the certificate ordering

Non-customers – Please choose one of the following options:

- **Get Free Certificate** - Starts a wizard that helps you order a free Comodo SSL certificate. Free certificates are valid for 90 days and are limited to one per domain. Once your order has been created it will appear in the 'Orders' section of the utility. See [Sign up for your Free Trial Certificate](#) for more details.

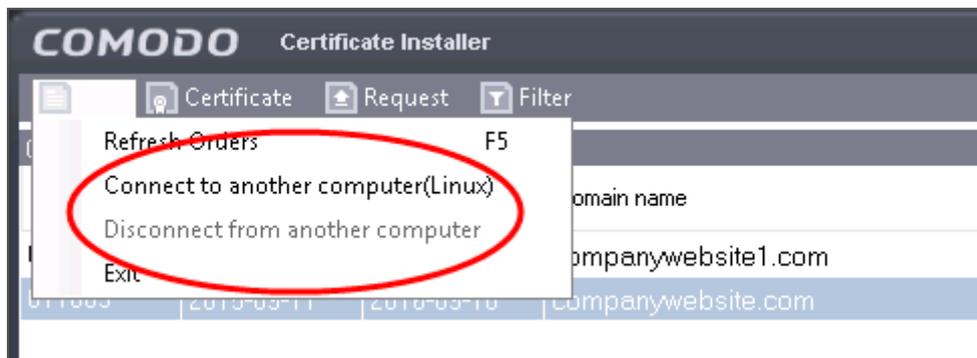
- **Generate CSR** – Starts a wizard that will help you create an industry standard certificate signing request. You can then use the CSR to apply for a certificate at any time. See [Generate a CSR](#) for more details.
- **Buy Certificate** – Starts a wizard that allows you to select and purchase a Comodo certificate. Once your order has been created it will appear in the 'Orders' section of the utility. See [Buying a Certificate](#) for more details.
- **Renew with Comodo** – The utility will scan your web-server and display a list of all installed certificates (including self-signed). Non-Comodo certificates are highlighted in red. Click 'Renew' to apply for a Comodo certificate for the same domain. See [Renewing a Certificate](#) for more details

Connect to an Apache Server

After **installation**, Apache users should login to their Comodo account at the utility start screen, then connect to the Linux server that hosts their Apache web server.

Once connected you will be able to generate a CSR, automatically install your certificate and access the full functionality of the utility.

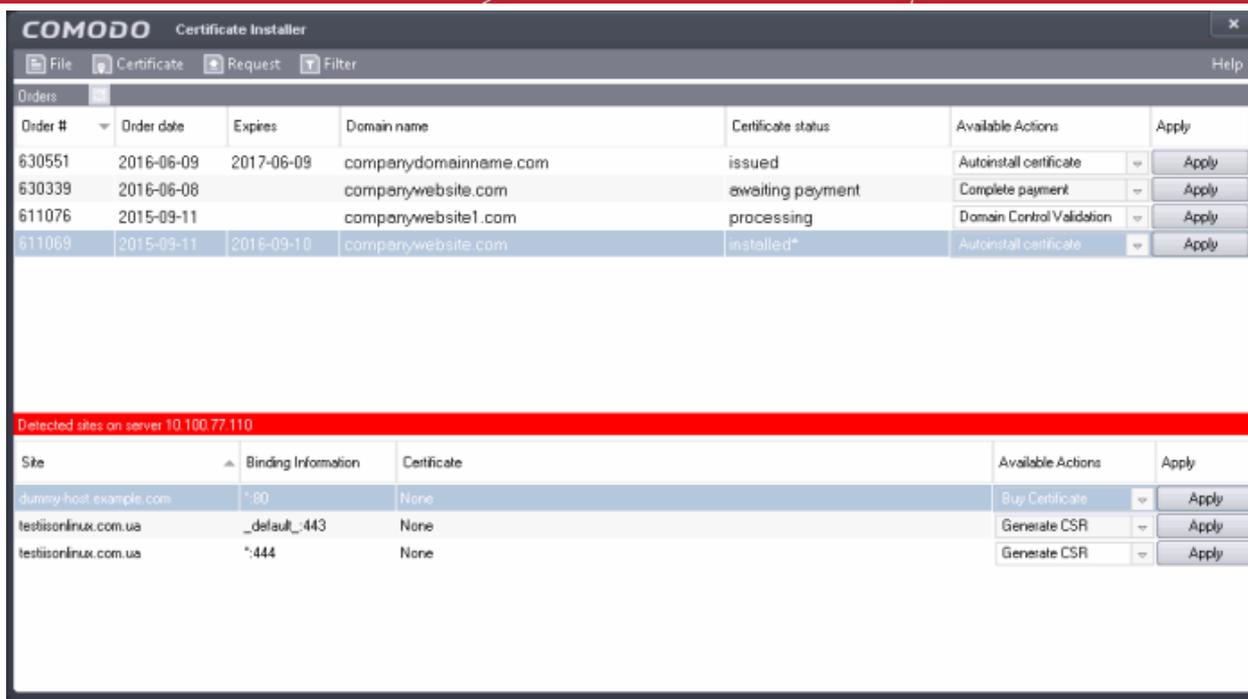
To get started, go to 'File' and select 'Connect to another computer (Linux)'.



At the host login box, enter the address and port number of your host, and the credentials of a user that has SSH access with sudo privileges. If the SSH user does not have sudo privileges, then all keys and certificates will be placed in the home directory.



- Click 'Connect'. Once connected, all web sites detected on your server will be listed in the lower pane (under the red line):



The screenshot shows the Comodo Certificate Installer application window. The top pane displays a table of orders with columns for Order #, Order date, Expires, Domain name, Certificate status, Available Actions, and Apply. The bottom pane, titled 'Detected sites on server 10.100.77.110', displays a table with columns for Site, Binding Information, Certificate, Available Actions, and Apply.

Order #	Order date	Expires	Domain name	Certificate status	Available Actions	Apply
630551	2016-06-09	2017-06-09	companydomainname.com	issued	Autoinstall certificate	Apply
630339	2016-06-08		companywebsite.com	awaiting payment	Complete payment	Apply
611076	2015-09-11		companywebsite1.com	processing	Domain Control Validation	Apply
611069	2015-09-11	2016-09-10	companywebsite.com	installed*	Autoinstall certificate	Apply

Site	Binding Information	Certificate	Available Actions	Apply
dummy-host.example.com	*:80	None	Buy Certificate	Apply
testisonlinux.com.ua	:_default_:443	None	Generate CSR	Apply
testisonlinux.com.ua	*:444	None	Generate CSR	Apply

From this point onward you can use the utility to order, install and manage all certificates on your Apache web server.

- See [The Main Interface / Actions and Statuses](#) for a basic understanding of the utility
- See the [tutorial](#) for a step-by-step guide to completing your order and installing your certificate
- See [Completing Domain Control Validation \(DCV\)](#) if you need help with DCV
- See [Install and bind a certificate](#) for an overview of the certificate installation process

The Main Interface / Actions and Statuses

After logging into your Comodo account, the upper pane of the utility will display a list of all certificates associated with your account. The lower pane displays a list of all sites and certificates detected on your server.

- Apache users should next click 'File' > 'Connect to another computer', then enter the address and login credentials of their host. [Click here](#) if you need help with this.
- IIS users do not need to connect because the utility is already installed on the host. All detected certificates and sites will automatically be shown in the lower pane.

The screenshot shows the Comodo Certificate Installer window. It is divided into two main panes. The upper pane displays a table of certificate orders with columns for Order #, Order date, Expires, Domain name, Certificate status, and Available Actions. The lower pane displays a table of detected sites on the local server with columns for Site, Binding Information, Certificate, and Available Actions. Callout boxes provide the following information:

- Upper Pane:**
 - All your Comodo certificate orders appear in the upper pane.
 - 'Status' tells you where your certificate is in the ordering and installation processes.
 - The actions you can take depend on the certificate status.
- Lower Pane:**
 - The lower pane shows all web-sites discovered on your server.
 - Lists existing certificates which are installed and bound to discovered sites. 'Red' certificates are non-Comodo.
 - Allows you to view and renew existing certificates.

The **tutorial** will take you from the 'most incomplete' status of 'Awaiting Request' through to a final status of 'Bound'. Before that, however, it is worth first explaining the 'Certificate Statuses' and 'Available Actions' you will see in the interface:

Certificate Status	Available Actions
<p>Waiting for CSR</p> <p>A certificate order has been created but a corresponding CSR has not been imported to the auto-installer nor submitted to Comodo CA. You must submit a CSR for your domain to start the certificate application and issuance processes.</p>	<p>Generate Request</p>
<p>Processing</p> <p>CSR has been submitted and received. Comodo CA is now processing the order and validating the application. Note – you must next complete Domain Control Validation (DCV) before your certificate can be issued.</p> <p>Note - If your status is 'Processing' but you have completed the CSR and domain validation (DCV) processes, it is usually because Comodo are still completing organization validation. Please check the interface regularly to see if your certificate has been issued. Please allow up to 1 week for EV certs and 2 days for OV certs.</p>	<p>Domain Control Validation Replace CSR</p>

<p>Issued</p> <p>Certificate has been issued by Comodo CA and is awaiting further actions. Certificate status will change to 'Issued' if your CSR has been accepted AND the DCV check is successful.</p>	<p>Auto-install certificate Complete request (IIS only) Save Certificate Renew Certificate Installation Check</p>
<p>Installed</p> <p>Apache – Certificate has been successfully installed. IIS - Certificate has been installed but has not been bound.</p>	<p>Auto-install certificate Bind to site (IIS only) Save Certificate Renew Certificate Installation Check</p>
<p>Bound (IIS Only)</p> <p>Certificate has been installed and assigned to the domain in IIS 'Bound' certificates should also appear in the 'Detected Sites' area.</p>	<p>Auto-install certificate Save Certificate Renew Certificate Installation Check</p>
<p>Awaiting Payment</p> <p>Your order has been placed with Comodo, but payment has not yet been received. Please complete payment for order processing to continue.</p>	<p>Complete Payment</p>

Available Actions

Generate Request

- Starts a wizard that will help you create and submit a CSR using IIS / Apache for the domain listed in the 'Domain Name' column

Replace CSR

- This option is available only while the certificate has a status of 'Processing' (after 'CSR' has been submitted but before the certificate has been issued). Use this option to replace your CSR if, for example, there were errors with the original CSR.

Domain Control Validation

- Starts the Domain Control Validation (DCV) wizard. It is mandatory to complete DCV before Comodo can issue your certificate. You can choose any of the following methods to complete the process:
 - Email – You must respond to a challenge-response email sent to an email address at your domain
 - HTTP/S CSR Hash - Comodo systems check for the presence of a .txt file uploaded to your domain
 - CNAME CSR Hash – You add a DNS CNAME record containing the SHA-1 and MD5 hashes of your CSR
 - None of the above – Select this only if you have arranged an alternative method of completing DCV with Comodo

Auto-install Certificate

- 1) Installs the certificate to the domain listed in the 'Domain Name' column (Apache and IIS)
- 2) Creates a site in IIS for the domain listed in the 'Domain Name' column if one doesn't already exist (IIS only)
- 3) Binds the certificate to the domain in IIS (IIS Only)

Note – For IIS, if the certificate has status 'Installed' then 'Auto-install' will only perform 2) and/or 3) as required

Complete Request (IIS only)

- Installs the certificate to the domain listed in the 'Domain Name' column
- Does not bind it to the domain in IIS nor create the site in IIS if it doesn't exist

Bind to Site (IIS only)

- Creates a site in IIS for the domain listed in the 'Domain Name' column (if one doesn't already exist)
- Binds the certificate to the domain in IIS

Renew Certificate

- Opens the auto-installer's 'Renew Certificate' wizard

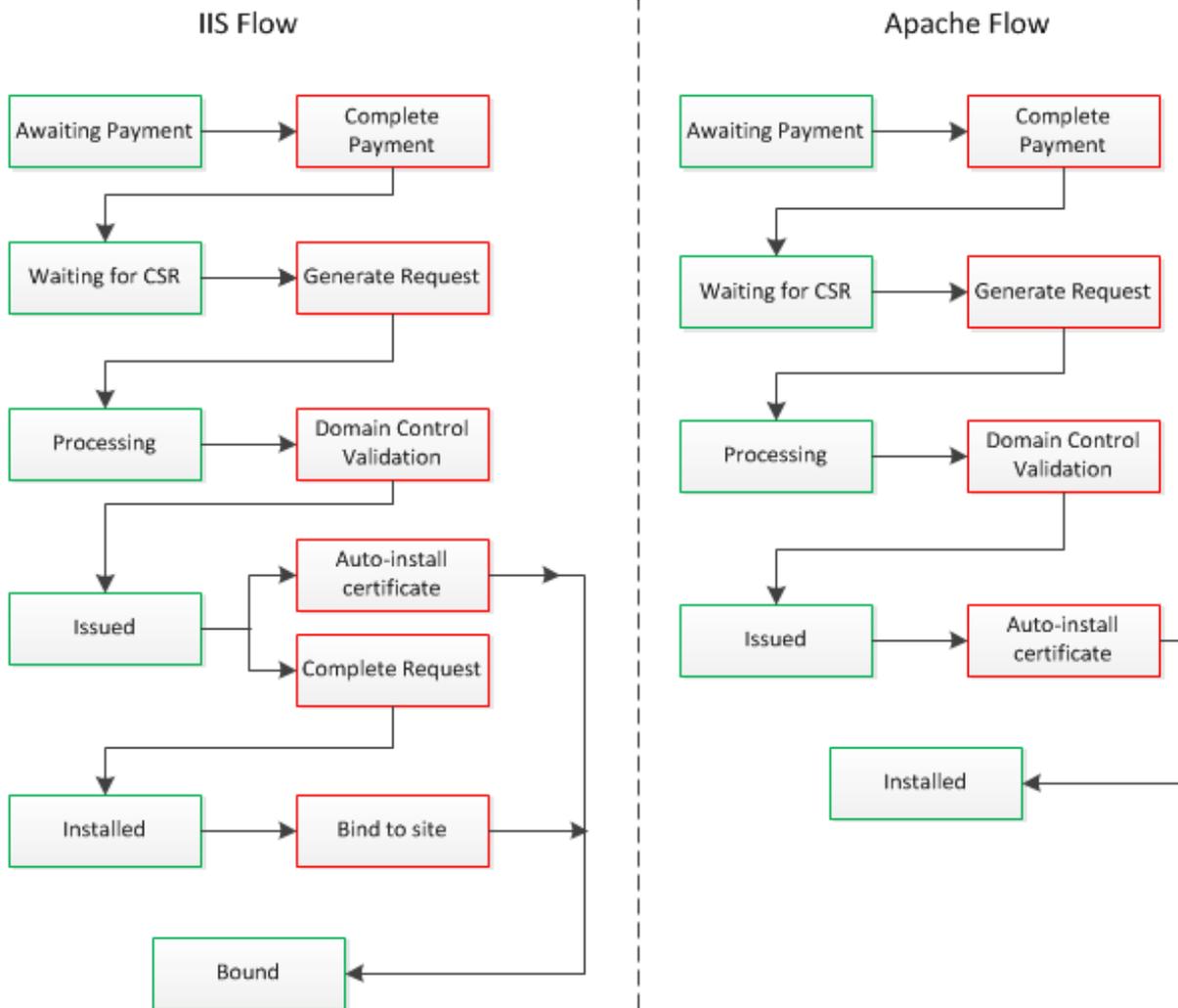
Installation Check

- Verifies whether your certificate is correctly installed on the domain named in the certificate. You can use this option to test new certificate installations, and the installation status of existing/discovered certificates.

Complete Payment

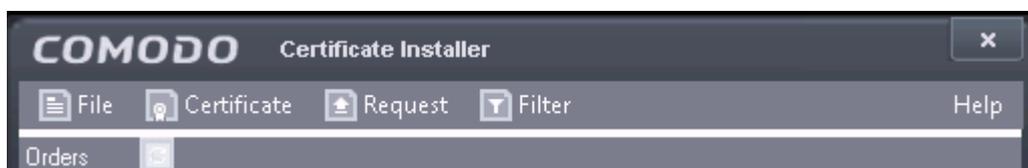
- Opens the Comodo order forms where you can enter payment details. Payment must be received before further processing can take place on your order.
- Allows you to save a zip file containing your certificate to a location of your choice

These diagrams illustrate the relationship between statuses and available actions for IIS and Apache servers:



For clarification, the 'Auto-install certificate' option is always available after issuance so you can, for example, re-use the utility to install the same certificate on a different host. The 'Renew Certificate' option will appear when certificates with a status of 'Issued', 'Installed' and 'Bound' are approaching expiry.

The top menu contains some additional functionality:



File:

- Allows you to close the application or refresh the list of orders shown in the upper pane.
- 'Connect to another computer (Linux)' / 'Disconnect from another computer' (Apache users only) – Allows you to connect to a Linux host running CentOS, Fedora, Ubuntu or Debian. You will need to enter the address of the host and the username/password of a user who has SSH access with sudo privileges.

Certificate:

- List of Installed Certificates – Comodo Certificate Installer scans your server and presents every installed certificate. This list differs from the certificates shown in the 'Detected Sites' area, which only shows certificates that have been both installed and bound.
- 'Autoinstall', 'Complete Request', 'Bind to site', 'Save to file', and 'Renew' - once a certificate is selected in the main pane, these items fulfill the same functionality as described in the **Available Actions** section.
- 'Buy Certificate' will allow you to start the purchase process for a new Comodo certificate. This is covered in **Buying a Certificate**

Request: Contains two items related to CSR generation:

- 'Create for current order' – Allows you to generate a CSR for a selected order then submit it to Comodo or save it. This is similar to the 'Generate Request' action but gives you the flexibility to create a CSR for an order at any time in its life-cycle.
- 'Create new' – Allows you to generate and save a CSR for a certificate, independent of a Comodo order. This is useful if you just want to generate a CSR to use in other applications.

Filter: Allows you to filter which certificates are displayed by status. Current filters are 'Awaiting Payment', 'Issued' and 'Processing'

Help: Displays software version information and allows you to view the online user guide.

Tutorial

Step 1 - Generate and submit a Certificate Signing Request (CSR)

Step 1 deals with orders that have the status 'Waiting for CSR'. If your order has a status of 'Processing', then **skip to step 2**. If your order has a status of 'Issued', then **skip to step 3**. If your order has a status of 'Awaiting Payment' then please select 'Complete Payment' to continue (**click here** if you'd like some more information on this).

- Locate an order with a 'Certificate Status' of 'Waiting for CSR', select 'Generate request' and click 'Apply'



- The 'Generate CSR' form will open:

COMODO Certificate Installer - Generate CSR

File Environment: Local server

Generate Paste

Common name:
 multidomain

Domains list:

Organization: Organizational unit:
City/locality: State/province:
Country/region:
E-mail:

Make private key exportable

- If you already have a CSR you wish to use, simply select the 'Paste' radio button and paste it into the text area in the lower half of the dialog. Click 'Send' to submit the CSR to Comodo CA.
- If you do not already have a CSR, you need to complete all fields. Most are self-explanatory, but for those with little experience of certificates:

Common Name = Fully Qualified Domain Name (for example, www.domain.com). This should be auto-populated.

Multi-domain = Check this box if you purchased a multi-domain certificate. You should enter all domains covered by the certificate in the 'Domains List' box

Domain list = Enter all domains covered by the certificate. Each domain should be on a separate line.

Organization = Your company Name (for example, 'My Company LLC')

Organization Unit = Department (this can be the same as 'Organization' if your company doesn't require this field)

E-mail = Your contact email address

- The 'File' menu has the following options:
 - 'Save CSR to file' - Save your CSR in .txt format
 - 'Save as template' - Save the CSR, and all data/settings in this dialog to a template file for re-use later.
 - 'Load template' – Load a previously saved template
- **'Make Private Key Exportable' IIS Only.** This checkbox is only relevant to IIS users. If the private key is exportable then it will possible to export your certificate to another web-server. This is useful, for example, if

you want to secure a load-balancing web-server or because you have switched to another hosting provider. We recommend you leave this box enabled unless you have specific reasons for making the private key non-exportable.

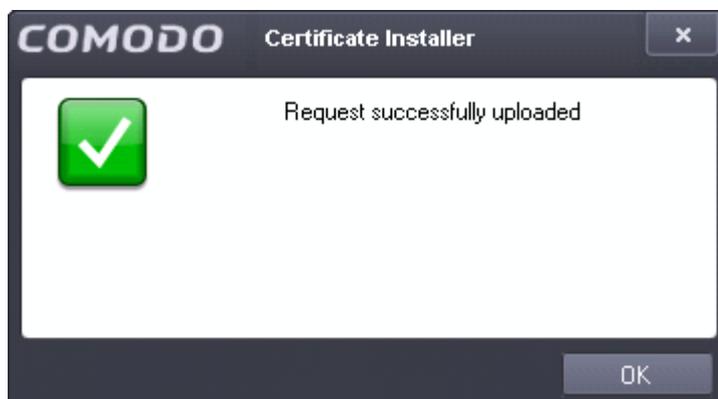
For Apache users. Your key is 'exportable' by default - your newly created CSR and key will be placed in `/home/username/Comodo_AI/sitename/key/*.*`

The screenshot shows the 'COMODO Certificate Installer - Generate CSR' window. It has a 'File' menu and 'Environment: Local server'. There are two radio buttons: 'Generate' (selected) and 'Paste'. The form includes the following fields:

- Common name: (with a 'multidomain' checkbox below it)
- Domains list:
- Organization: and Organizational unit:
- City/locality: and State/province:
- Country/region: (dropdown menu)
- E-mail:

A 'Generate' button is located to the right of the E-mail field. Below the form is a checked checkbox labeled 'Make private key exportable'. At the bottom of the window, there is a text area containing the generated CSR text, followed by 'Send', 'Copy to clipboard', and 'Cancel' buttons.

Click 'Generate' to automatically create a CSR from the details you entered. Click the 'Send' button to submit the CSR to Comodo. A confirmation window regarding your successful request will appear:



The certificate status will change to 'Processing' and 'Available Actions' for this certificate will now contain two options – 'Replace CSR' and 'Domain Control Validation'.

Comodo will check the CSR details and conduct any required validation checks on your company. Organization Validated certificates (like Instant SSL) and Extended Validation certificates require manual validation, so it might be a

day or two before the certificate is issued. Comodo staff will contact you should they need any more information. While this is in progress, you should complete Domain Control Validation (DCV).

Step 2 – Complete Domain Control Validation (DCV)

Before Comodo can issue your certificate, you must demonstrate ownership of the domain by completing DCV. Comodo offers various methods for you to achieve this. To begin, first select 'Domain Control Validation' from the 'Available Actions' drop-down and click 'Apply':



This will open the DCV configuration interface:



In the 'Method' box on the left, choose *one* of the following options:

- **Validation by email address** – You confirm domain ownership by responding to a mail sent to an email address registered for this domain. You are presented with a choice of email addresses drawn from the WHOIS database that are registered to the domain, along with some 'typically used' addresses (such as webmaster@domain.com). After choosing one, you must click the validation link in the mail to confirm your control of the domain. Alternatively, the email also contains a unique code which you can copy and paste into the auto-installer interface.

OR

- **Validation by alternative methods of DCV** – There are currently 3 alternative methods you can pick from. The first two involve uploading a .txt file containing hashes of your CSR to your web server. The third involves adding the hash of your CSR as a DNS CNAME for you domain. In all cases, Comodo will run an automated test to ensure that you have completed the task.

OR

- **None of the above** – Choose this if you have already arranged an alternative way of completing DCV with Comodo. If you choose this option, please remember to click 'Submit' to register this choice with Comodo issuance systems and to cancel any DCV method you may have selected previously.

Validation by email address

After selecting 'Email Addresses' as the DCV method, the interface will present a list of WHOIS registered and commonly used addresses.

Domain	Status
companywebsite.com	No Domain Control Validation method selected

Method of Domain Control Validation

Email Addresses

Alternative methods of DCV

None of the above

Registered Email Addresses (from WHOIS)

Level 3 Email Addresses

admin@companywebsite.com

administrator@companywebsite.com

hostmaster@companywebsite.com

postmaster@companywebsite.com

webmaster@companywebsite.com

Level 4 Email Addresses

Please enter a validation code that was received via email: _____

Submit

Send

Please select an address at which you can receive mail and click 'Submit'. Comodo will send a mail to this address which contains a validation link and a unique validation code. You can confirm domain control by clicking the link and following the instructions on the page that this link opens. Alternatively, you can copy the validation code and paste it into the field at the bottom of the interface (see screenshot below):

Domain	Status
companywebsite.com	Verification email sent to admin@companywebsite.com

Method of Domain Control Validation

Email Addresses

Alternative methods of DCV

None of the above

Registered Email Addresses (from WHOIS)

Level 3 Email Addresses

admin@companywebsite.com

administrator@companywebsite.com

hostmaster@companywebsite.com

postmaster@companywebsite.com

webmaster@companywebsite.com

Level 4 Email Addresses

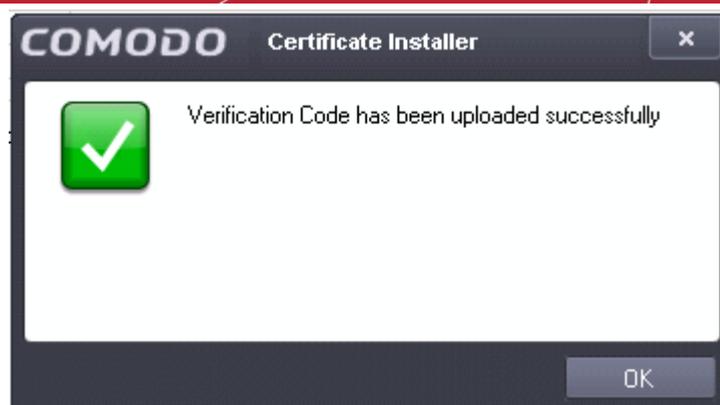
Please enter a validation code that was received via email: _____

sg364swEGes1

Submit

Send

Click 'Send' to submit the code for verification:



Validation by alternative methods of DCV

HTTP(S) CSR Hash

Both the HTTP and HTTPS CSR options involve Comodo's automated systems checking for the presence of a simple text file in the root directory of your domain. The file will contain the MD5 and SHA1 hashes of your CSR and should be publicly accessible at the following location:

`http://yourdomain.com/<Value of MD5 hash of CSR>.txt`

To complete DCV using this method:

1. Select the HTTP or HTTPS CSR Hash radio button
2. Click 'Submit' to register this choice with Comodo
3. Click 'Create File'. This button will:
 - i. Generate the required DCV file
 - ii. Ask you to provide the location of your root directory
 - iii. Place the file in your root directory
 - iv. Automatically run the DCV check

'Check file' will just run the DCV check ('iv' in the list above). This is useful if, for example, you want to create and upload the file manually. If you want to handle this process manually then there are more instructions at:

<https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/791/16/>

In short, you need to create a .txt file according to the following specifications:

File name	<code>http://yourdomain.com/[Upper case value of MD5 hash of CSR].txt</code>
Content	<code>[Value of SHA1 hash of CSR] comodoca.com</code>

You can copy the MD5 and SHA1 hashes from the interface above. You then need to save it to the root directory of your web server.

Once DCV is passed, the certificate status will change to 'Issued' if you have already successfully submitted a CSR.

Note 1: DCV will fail if any redirection is in place.

Note 2: yourdomain.com in the example above means the Fully Qualified Domain Name (FQDN) contained in the certificate. If you are ordering a MDC or UCC, each FQDN in the certificate MUST have the txt file in placed in its root folder.

Examples:

yourdomain.com/<Value of MD5 hash of CSR>.txt

subdomain1.yourdomain.com/<Value of MD5 hash of CSR>.txt

yourdomain2.com/<Value of MD5 hash of CSR>.txt

CNAME CSR Hash

The MD5 and SHA1 hash values of the CSR you submitted to Comodo are provided to you in the interface. To complete DCV using this method, you must add a DNS CNAME to your domain which use these hashes.

The CNAME record should be added as follows:

<Value of MD5 hash of CSR>.yourdomain.com. CNAME <value of SHA1 hash of CSR>.comodoca.com.

Example - 123456789ABCDEF.yourdomain.com. CNAME ABCDEF123456789.comodoca.com.

Make sure to include the trailing periods as the check will fail without them.

The procedure for adding a CNAME record varies depending on your registrar or web host. If you are not experienced in modifying DNS records, then please request the assistance of your domain registrar or web host before making this change.

Once the CNAME change has been implemented, click 'Submit' to run the DCV check. The certificate status will change to 'Issued' if the DCV check is successful AND you have successfully submitted a CSR.

Step 3

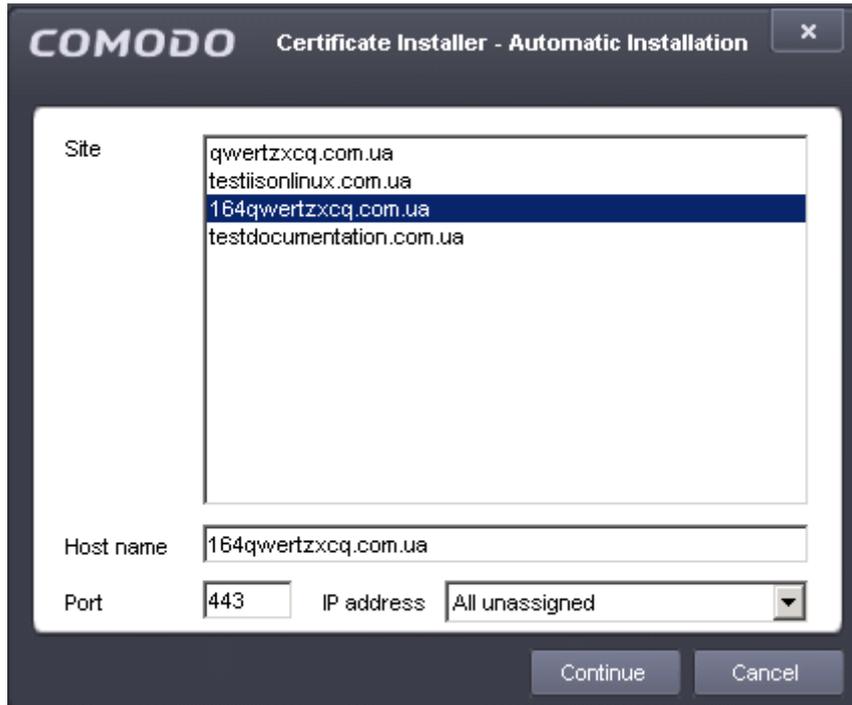
Install and bind a certificate - IIS

If your certificate has a status of 'Issued', there are two installation options available to you - 'Auto-install Certificate' and 'Complete Request'.

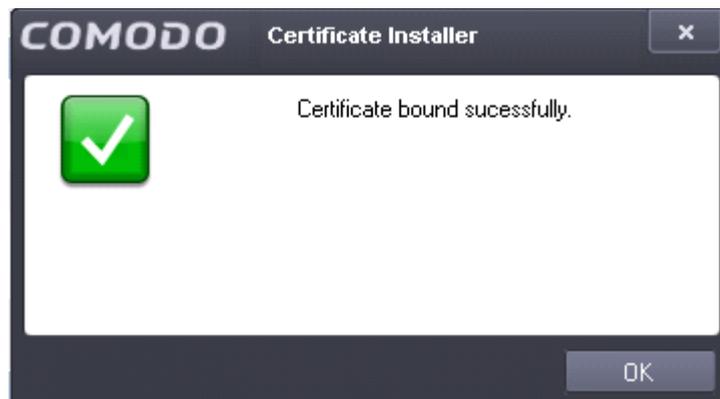
- 'Auto-Install' will install and bind your certificate in IIS and lead to a certificate status of 'Bound'
- 'Complete Request' will install the certificate but will not bind it. This option leads to a certificate status of 'Installed'.
- If you choose the 'Complete Request' action, you will be presented with the option to 'Bind to Site' afterwards.
- The 'Auto-Install' action is present at all times for 'Issued' certificates so you can re-install on different hosts as per your requirements.
- For a more complete explanation of these options, see [The Main Interface / Actions and Statuses](#)

To automatically install and bind a certificate:

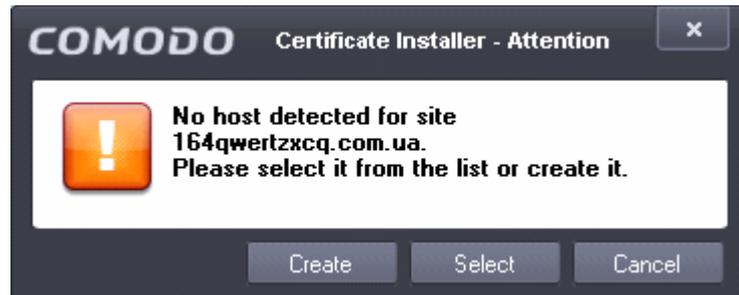
- In the main interface, select 'Autoinstall certificate' from 'Available Actions' and click 'Apply'. Choose the site you wish to install to from the 'Site' list box and click 'Continue'. Doing so will instruct the auto-installer to install and bind the certificate to the website and host specified by you.



- If the site exists and is configured correctly, then you will see a confirmation message as follows



- If the website doesn't exist on the server, you be offered the opportunity to create one:

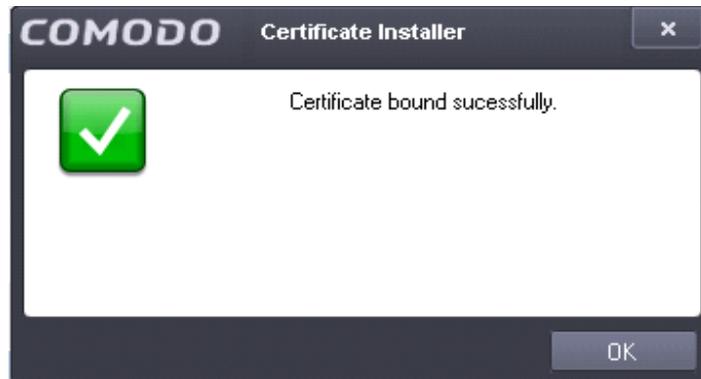


- Click 'Select' to go back and choose a different site. Click 'Create' to open the 'Add Website' interface:



- Type your website domain in the 'Site Name' text box.
 - **Application Pool (advanced users).** If you have a particular application pool on your web server to which this site should belong, then click 'Select' and choose it from the list. Otherwise, leave this at the default 'DefaultAppPool'.
 - **Content Directory.** Type the path or browse to the directory on your web-server that contains your website content.
 - **HTTPS (binding).** By default, the IP address value for the web site is 'All Unassigned' (in DNS). This means the server will respond to requests for any IP address on the port and host name that you specify for this site *except* IP addresses that have been assigned to another site. IP Address and port must be different for different web sites hosted on the same web server. This setting can be left at 'All unassigned' / 443 unless you know you have specific binding requirements.

- **HTTP** (binding). Allows you to create a HTTP binding for the site. Please also complete the 'Host name' field if you enable this option.
- Click 'OK' to save your settings then click 'Continue' on the 'Automatic Installation' screen. You will see a confirmation message if your certificate was installed correctly.

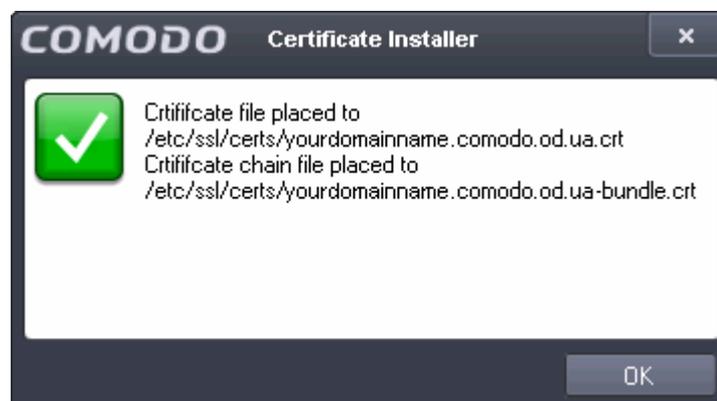


Install and bind a certificate - Apache

If your certificate has a status of 'Issued' then the next action you should choose is 'Auto-Install Certificate'.

- 'Auto-Install' will install and bind your certificate in Apache and lead to a certificate status of 'Installed'
- The 'Auto-Install' action will remain available even after installation so you can re-install on different hosts as required.

After selecting a certificate, choose 'Auto-install certificate' and click 'Apply'. The utility will copy the certificate and key to the path in the Apache configuration.



Restart Apache web server to complete the installation.

Renew a certificate

There are three ways you can renew a certificate:

- To renew one of your Comodo certificate orders, use the 'Renew Certificate' option in the 'Available Actions' drop-down.



The option above will appear when a Comodo certificate with a status of 'issued', 'installed' or 'bound' approaches its expiry date.

- To renew discovered certificates that are bound to 'Detected Sites', select the 'Renew with Comodo' option:

Site	Binding Information	Certificate	Available Actions	Apply
mydomain.com	*.443:	E=admin@email.com, CN=mydomain.co...	Renew with Comodo	Apply
payments.test.com	*.443:	E=admin@email.com, CN=payments.tes...	Generate CSR	Apply

You can also use the option above to buy a new certificate for a domain that does not have one.

- Alternatively, you can renew a certificate by using the 'List of installed certificates' feature to find ALL installed certificates on your web server (the 'Detected Sites' area only shows certificates that are installed AND bound to a domain)

Detected Certificates	Valid From	Valid To	Subject	View	Renew
...	6/25/2015	6/19/2016	...	View	Renew
...	2/25/2016	2/19/2017	...	View	Renew
...	4/30/2015	4/24/2016	...	View	Renew
...	6/7/2005	5/30/2020	...	View	Renew
...	5/30/2000	5/30/2020	...	View	Renew
...	4/22/2015	4/16/2016	...	View	Renew
...	8/11/2014	8/6/2015	...	View	Renew
...	2/24/2016	2/18/2017	...	View	Renew
...	4/27/2015	4/21/2016	...	View	Renew
...	8/17/2015	8/16/2016	...	View	Renew
...	4/4/2016	3/30/2017	...	View	Renew
...	5/29/2015	5/23/2016	...	View	Renew
...	7/7/2015	7/1/2016	...	View	Renew
...	4/4/2016	3/30/2017	...	View	Renew
...	4/27/2015	4/21/2016	...	View	Renew

The 'Filter' check box at bottom-right allows you narrow results by:

- Domain Name
- Validity (Valid from/to)
- Subject

- Existing Comodo customers can access this list by logging in then choosing 'List of installed certificates' from the 'Certificates' menu.

- Non-customers can access the same interface from the start-up dialog:

Non-Comodo Customers

<p>Get Free Certificate</p>	Obtain a free certificate which is fully trusted by all major internet browsers.
<p>Buy Certificate</p>	Allows you to purchase a new Comodo SSL Certificate. You can then use the utility to automatically install the certificate.
<p>Renew with Comodo</p>	Will detect all existing certificates on your server and allow you to renew them with Comodo.
<p>Generate CSR</p>	Step-by-step wizard that helps you create a standard certificate signing request for an SSL certificate

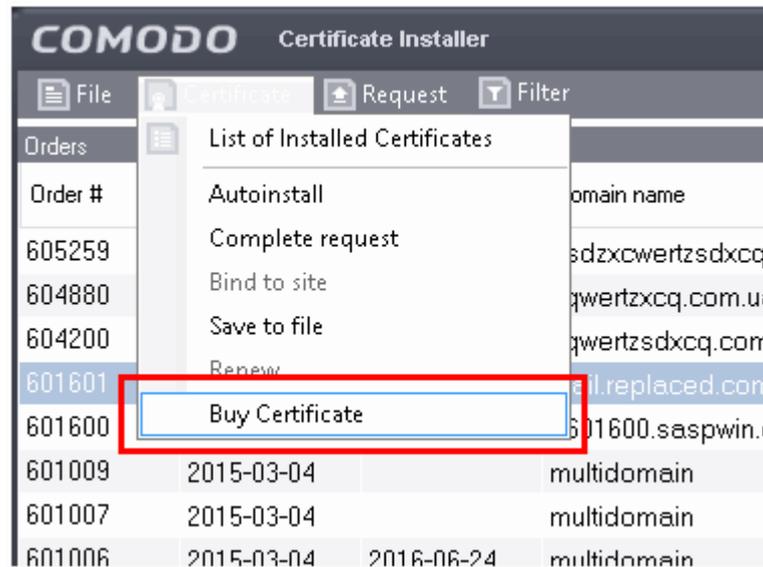
v 1.1.1.0

After choosing a certificate to renew using any of these methods, you will move onto the next step, **Completing Your Order**.

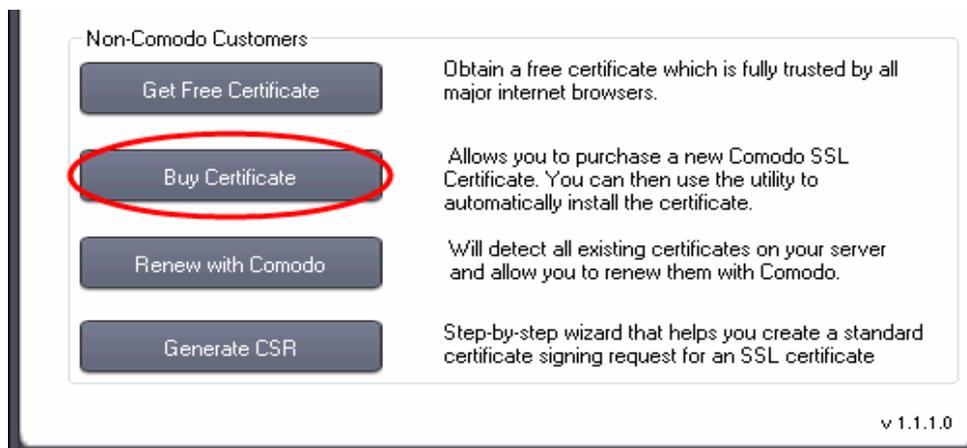
Buy a certificate

There are three possible ways you can buy a certificate:

- 1) Existing customers should log into the utility and select 'Buy Certificate' from the 'Certificates' menu:



- 2) Non-Comodo customers can select 'Buy Certificate' from the start-up dialog:



- 3) Logged-in customers can also buy a certificate for a 'Detected Site' that does not have one by selecting the 'Renew with Comodo' option:

Site	Binding Information	Certificate	Available Actions	Apply
mydomain.com	*.443:	None	Renew with Comodo	Apply
payments.test.com	*.443:	E=admin@email.com, CN=payments.tes...	Generate CSR	Apply

After choosing a certificate to purchase using any of these methods, you will move onto the next step, **Completing Your Order**.

Complete your order

After you have chosen a certificate to purchase or renew, the next step is to complete the 'Create New Order' form:

- **Choose certificate type**

Product: Choose between Extended Validation or Domain Validated certificate categories then choose a certificate type from the drop-down box.

Place your mouse over the 'What's This?' and 'Explain My Choices' links if you need help to decide.

Price and currency: Displays the price of your current selection and allows you to change payment currency.

- **Domain details**

Common Name = Fully Qualified Domain Name (for example, **www.domain.com**). This should be auto-populated if you are renewing a certificate.

DCV Method: Select a method for completing Domain Control Validation. Place your mouse over 'What's This?' to see an explanation of each option. DCV options are also **explained here**.

- **Create file for DCV check:** Automatically generates the .txt file required for Domain Control Validation and places it in the root directory of your web-server. This option becomes available if the utility detects *all* domains in your CSR are set up on your web server, and it can determine the root directory path of each. **Click here** if you need more information about DCV checks.

Note: 'HTTP CSR HASH' + 'Create File for DCV Check' are the recommended options. The form will default to these options *if we detect it is possible to complete validation this way on your server*. To 'unlock' the drop-down and reveal the other DCV options, please un-check the 'Create File for DCV Check' box.

- **Generate CSR:** If enabled, the utility will automatically generate and send a certificate signing request with this application (recommended).
 - Deselect check 'Make private key exportable' box if you do not want to export a certificate with its private key
- **Remote Host Connection Status (Apache only)**
 - Indicates whether or not you are connected to an Apache server. The 'Connect Now' button opens the host login box.
- Click 'Next'.

The next step is the account and contact details screen. Fields marked * are mandatory.

The screenshot shows the 'COMODO Certificate Installer - Create new order' window. It is divided into two main sections: 'Enter Your Account Details' and 'Enter Your Company Details'.
Enter Your Account Details:
- Login Name *: testuser720@gmail.com
- Password *: [masked] (Note: Login name should be min. 5 characters long. Passwords should be min. 8 characters long and contain at least one uppercase letter, one lowercase letter and one number)
- Confirm Password *: [masked]
Enter Your Company Details:
- Organization Name *: Flower&Co
- Street Address *: Companyaddress
- Country *: United States (US)
- Postal / Zip code *: 29072
- City *: Cityname
- State / Province *: Alabama (AL)
- PO Box (Optional): 11111
- Company Telephone *: 123-456-789
At the bottom, there are buttons for 'Save to file', 'Read from file', '< Prev', and 'Next >'.

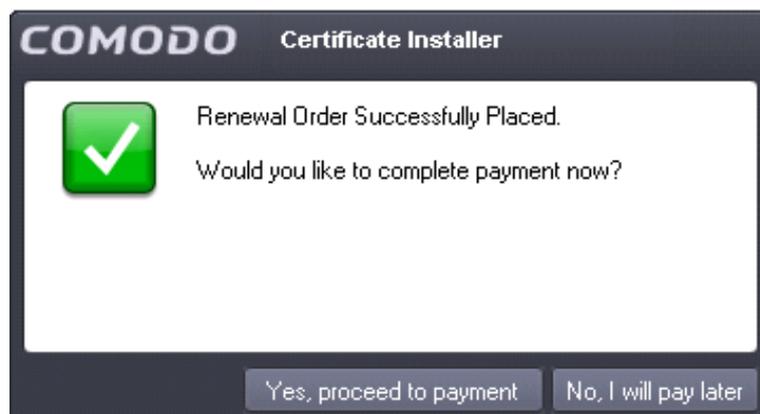
- New customers – Please create a Comodo user-name and password and complete all fields. Afterwards, you will be able to log in to the auto-installer to install, bind and manage your certificates.
- Existing/logged in customers – In many cases we will be able to draw all the company and contact details we need from our records, so you may not see this screen at all. In certain cases, however, we may need you to submit additional information. For example, an EV certificate application requires additional information that you might not have previously submitted. Please complete any mandatory fields that are required.
 - Click 'Save to file' to save the information you have entered so far in a .txt file (default= C:\Program Files (x86)\Comodo SSL Certificate Installer\user_data.txt).
 - Click 'Read from file' to auto-populate these fields from a saved file.
- Click 'Next' when all fields are complete.

After agreeing to the subscriber agreement, you will have a chance to review your order before submitting:

The screenshot shows the 'COMODO Certificate Installer - Create new order' window at the 'Summary' stage. It is divided into two columns: 'Your Order' and 'User info'.
Your Order:
- Product: COMODO SSL Certificate
- Term: 1 year: \$ 110.00/yr.
- Primary Domain: domainwebsitename.com
- Total Domains: 1
- DCV Method: HTTP CSR Hash
- Voucher: Not used
- Total (excluding taxes): \$110.00
User info:
- Login Name: testuser720@gmail.com
- First Name: Peter
- Last Name: Johnson
- Email Address: customeraddress@gmail.com
- Telephone: 123-456-789
- Job Title: FlowerCo
- Organization Name: Customer owner
- Street Address: Comanyaddress
- Postal / Zip code: 29072
- Country: United States (US)
- City: Cityname
- Company Telephone: 123-456-789
At the bottom right, there is a 'Place order' button. At the bottom center, there are '< Prev' and 'Next >' buttons.

- Click 'Place Order' to continue.

You will then be asked whether you would like to complete payment now or later:



- If you select 'No', then your CSR will be submitted to Comodo and your new order will appear in the auto-installer interface with a status of 'Awaiting Payment'. You can continue certificate processing by selecting 'Complete Payment'.
- If you select 'Yes', you will be directed to the Comodo order forms:

[Logout](#)

Secure Payment

Welcome: Auto Installer AI Development

Account Options

- ▶ [Signup](#)
- [Management](#)

Having problems paying?
If so, please contact our Sales department, who will be able to assist you with your payment.

Email: sales@comodo.com

Telephone:
+1.888.266.6361
+1.703.881.6361

Secure Payment Page
Your Order Number: 1439111
Total Amount: \$177.90

Required fields are displayed in RED.

Card Details

Card Number:

Card Code (3 or 4 digits):

Expiry Date: /

Cardholder's Name:

Cardholder Address and Contact Details

Company Name:

Address 1:

City / Town:

State / Province / County:

Zip / Postcode:

Country:

Phone:

Email:

© Copyright 2015. All rights reserved. Using VPN (Odessa Office)
Client IP: 192.168.75.102
Server IP: 192.168.0.190

Thursday, July 23, 2015

Fill out the required card payment details and click 'Make Payment'. Once payment is complete, your new certificate will appear in the auto-installer interface as a new order with one of the following statuses:

- **Processing** -This status indicates that domain control validation (DCV) is not yet complete.
 - If you selected 'email' as the DCV method during ordering, then please check your email account for a verification mail. [Click here](#) for more details on email DCV
 - If you selected HTTP CSR, HTTPS CSR or DNS CNAME as the DCV method, then please [click here](#) for further guidance.
- **Issued** - If you have successfully completed domain control validation then Comodo will issue your certificate and you should next choose either 'Auto-Install' or 'Complete Request' as explained in [Installing and Binding Your Certificate](#).

Generate a CSR

There are three methods you can use to generate a CSR with Comodo Auto-Installer:

1. You can have a CSR automatically generated during order creation by enabling the 'Generate CSR' box when [renewing a certificate](#) or [buying a certificate](#):

Domain details

Common name *

Domains list:

DCV Method * HTTP CSR Hash

Create file for DCV check [What's this?](#)

Generate CSR

Make private key exportable

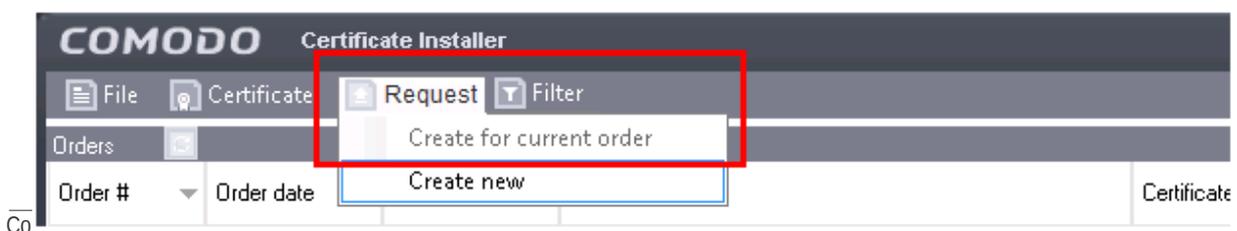
2. To generate a CSR for one of your existing certificate orders:

(i) Select an order then choose 'Generate Request' and click 'Apply':



OR

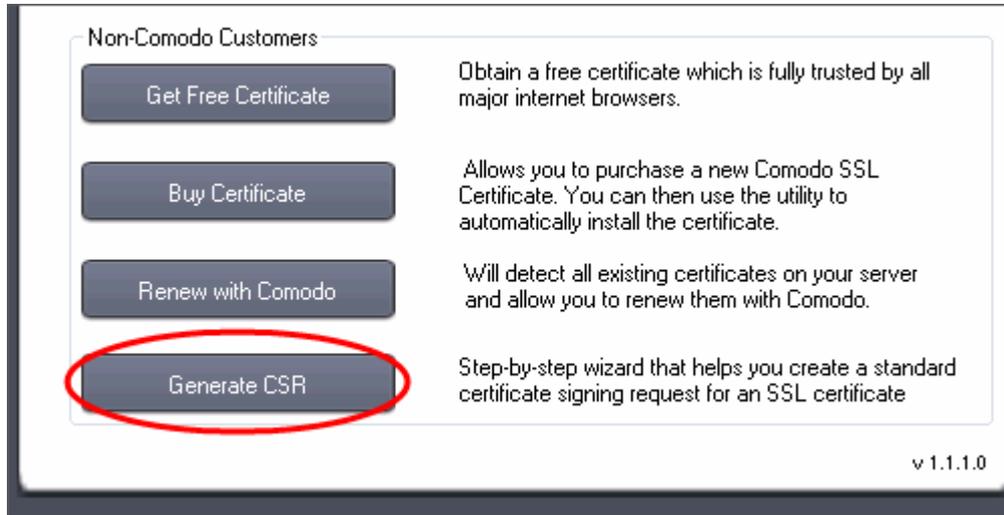
(ii) Select an order then choose 'Create For Current Order' from the 'Request' menu:



Both methods will start a wizard that will help you create and submit a CSR for the domain listed in the 'Domain Name' column. [Click here](#) to find out more.

3. You can also generate a standalone a CSR for later use by either:

(i) Clicking 'Generate CSR' at the start-up dialog:

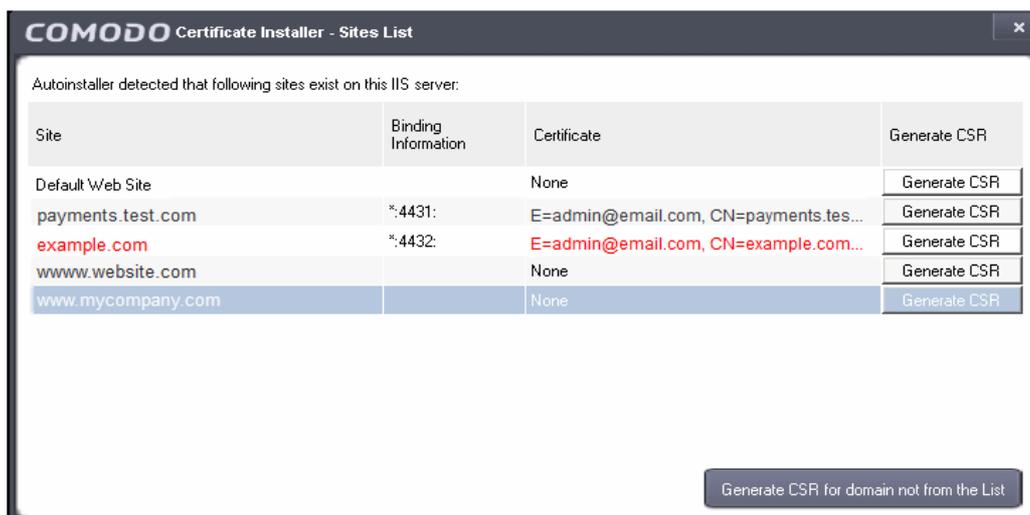


OR



(ii) Select 'Create New' from the 'Request' menu:

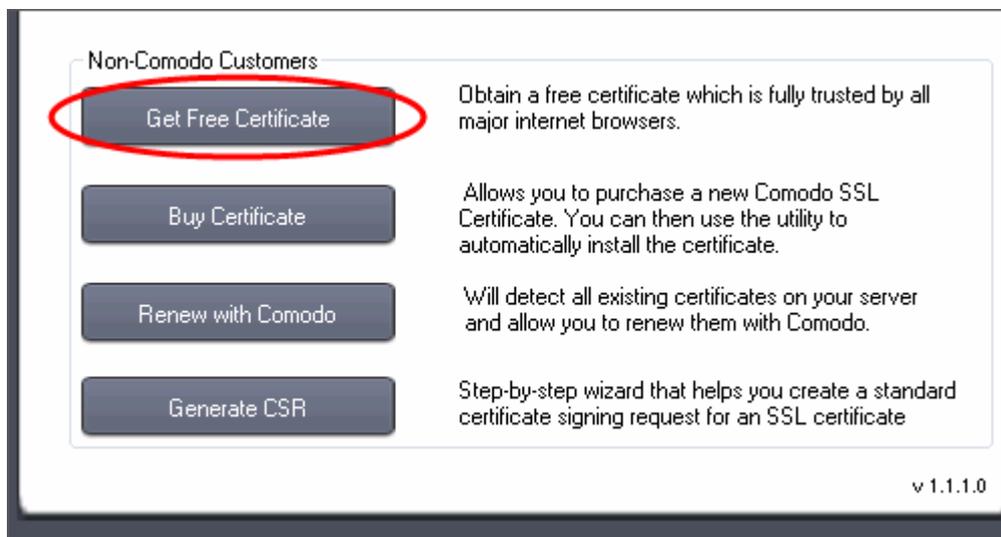
This will open the 'Sites List' window which shows all domains that the utility discovered on your server:



- Select a domain and click 'Generate CSR' to open the 'Generate CSR' form. [Click here](#) if you need help completing the fields on the CSR form.
- Alternatively, click 'Generate CSR for a domain not on the list' to create a request for domain that is not listed.

Get a free certificate

Non-Comodo customers looking to test certificate functionality and compatibility before committing to a purchase can obtain a free Comodo certificate which is valid for 90 days. Free certificates are trusted by all major browsers and mobile devices and are limited to one per account. Click 'Get Free Certificate' to start the ordering process:



After this, your next step is to complete the "Create New Order" form", as described in [Completing Your Order](#).

After submitting your order, it will appear in the 'Certificate Installer' main interface with a status of 'Processing'

- See [The Main Interface / Actions and Statuses](#) for a basic understanding of the utility
- See [Completing Domain Control Validation \(DCV\)](#) if you need help with DCV
- See [Install and bind a certificate](#) for an overview of the certificate installation process

Redeeming a voucher

Available for selected Comodo partners only. Voucher holders can claim their pre-paid SSL certificate by clicking the 'Redeem Voucher' button from the launch menu.

1. Enter your voucher and verification codes in the appropriate fields then click the 'Login' button:

COMODO Certificate Installer - Login

Voucher

Code

Login

2. After your codes have been validated, the next step is to finalize your order. The 'Choose a certificate Type' area on the left will be grayed out because this is a pre-paid certificate. However, you will need to enter your domain name and any alternative names. If possible, we advise you leave the 'Create file for DCV',

'Generate CSR' and 'Make Private Key Exportable' options enabled. If you would like more help with this step, see [Completing Your Order](#).

COMODO Certificate Installer - Create new order

Choose a certificate type

Show All Domain Validation Extended Validation
[What's this?](#)

Product: COMODO SSL Certificate
[Explain My Choices](#)

Term: 1 year: \$ 110.00/yr.
Currency: USD

Remote Host Connection Status (Apache Only)
Connect Now Not Connected

Domain details

Common name: companydomainname.com

Domains list:

DCV Method: HTTP CSR Hash
[What's this?](#)

Create file for DCV check [What's this?](#)
 Generate CSR
 Make private key exportable

Summary
next Voucher will be used:
24xshNWdDEza31cJZoufxQ3hp8gjjQ2024

< Prev Next >

Click 'Next' to submit your order. Note – Your order will not be affected if you back out and close the window at this stage. You can return and complete this step at any time.

3. After successfully submitting your order it will appear in the 'Certificate Installer' main interface with a status of 'Processing'.

COMODO Certificate Installer

File Certificate Request Filter Help

Orders

Order #	Order date	Expires	Domain name	Certificate status	Available Actions	Apply
622096	2016-03-03		websitewithvoucher.com	processing	Domain Control Validation	Apply

Detected sites on local server

Site	Binding Information	Certificate	Available Actions	Apply
Default Web Site		None	Generate CSR	Apply

- See [The Main Interface / Actions and Statuses](#) for a basic understanding of the interface
- See the [tutorial](#) for a step-by-step guide to completing your order and installing your certificate
- See [Completing Domain Control Validation \(DCV\)](#) if you need help with DCV
- See [Install and bind a certificate](#) for an overview of the certificate installation process

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