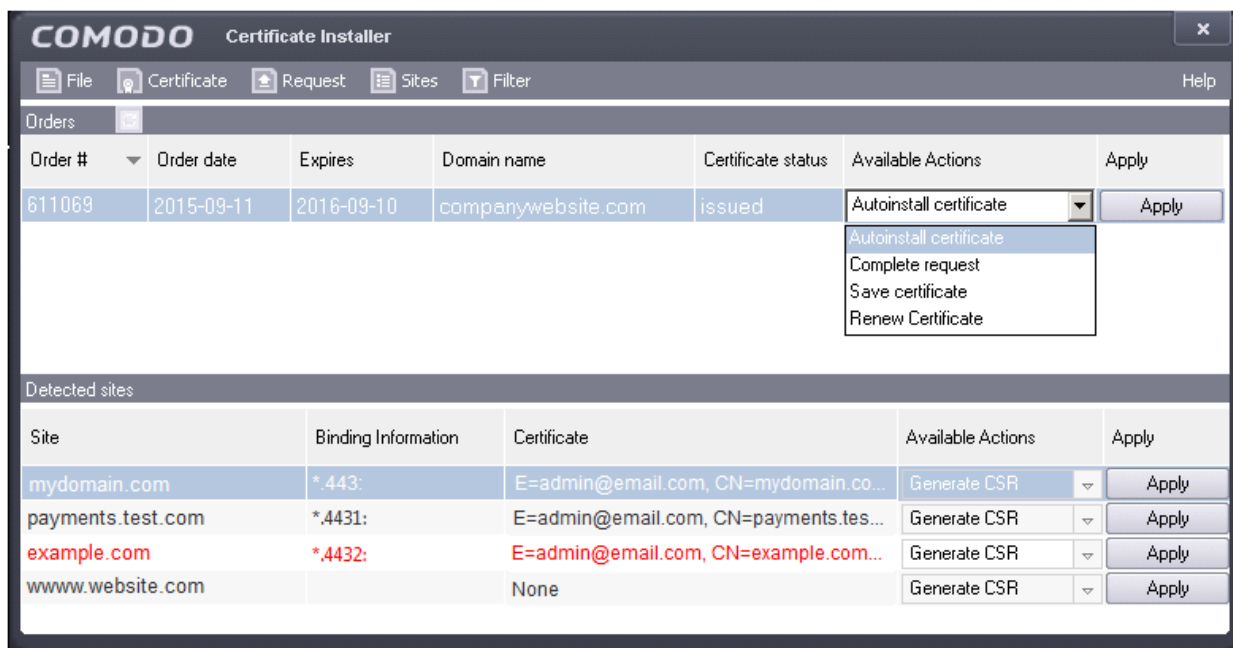


## Overview and Tutorial

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 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



Prerequisites:

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

This document contains the following sections:

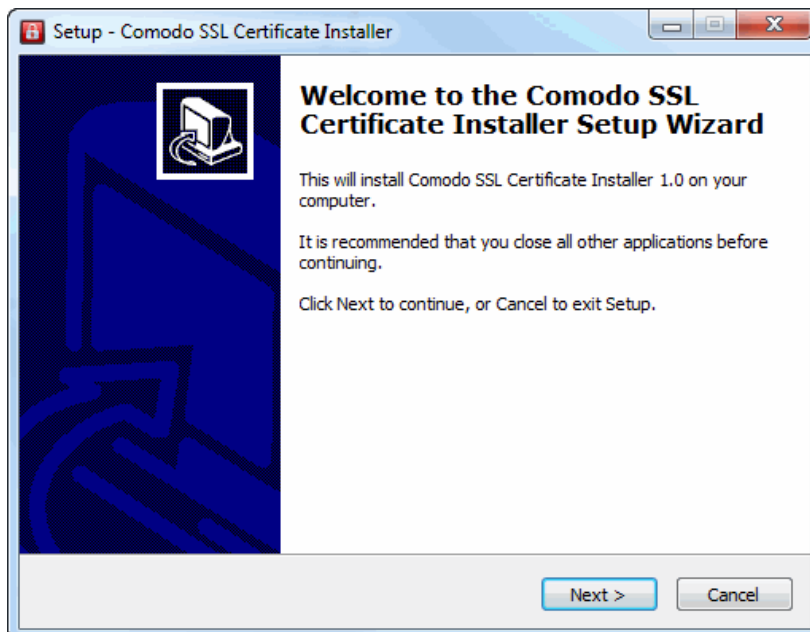
- **Download, install and run the utility**
- **The main interface / actions and statuses**
- **Tutorial**
  - **Step 1 - Generate and submit a CSR**
  - **Step 2 – Complete Domain Control Validation (DCV)**
  - **Step 3 - Install and bind a certificate**
- **Renewing a certificate**
- **Buying a certificate**
- **Completing your order**
- **Generate a CSR**

## Download, install and run the utility

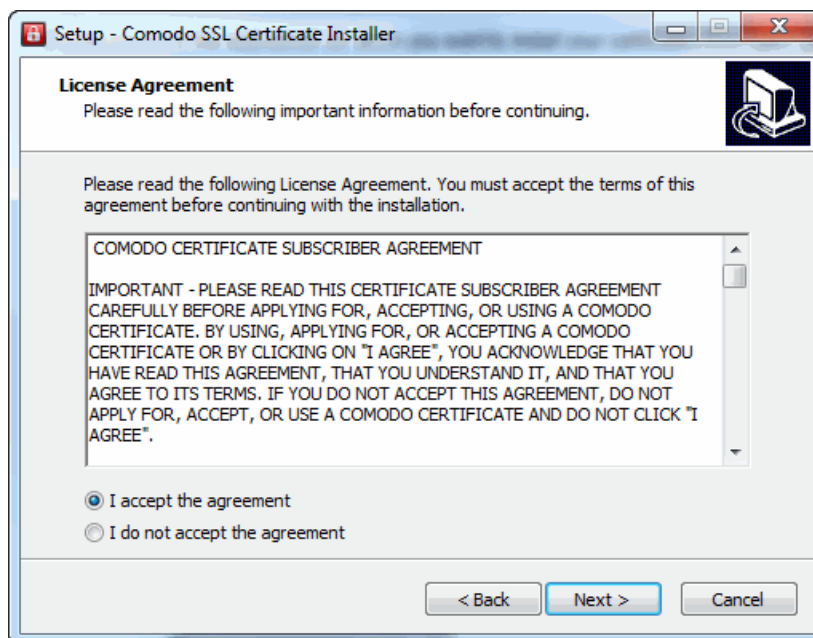
The certificate auto-installer can be downloaded from:

[http://download.comodo.com/ssl\\_autoinstaller/ComodoSSLCertificateInstallerSetup.exe](http://download.comodo.com/ssl_autoinstaller/ComodoSSLCertificateInstallerSetup.exe)

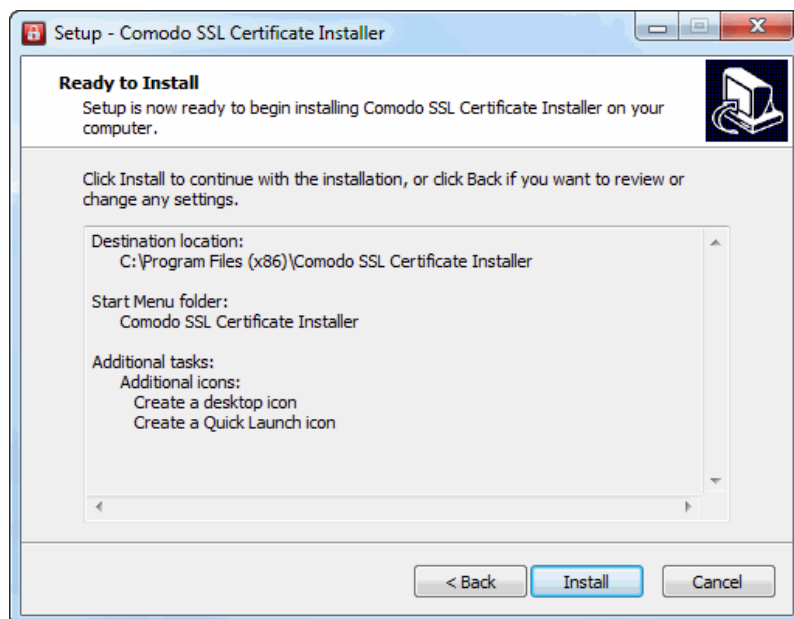
Please save and run this file on the web-server on which you want to install your certificates:



Click 'Next'.

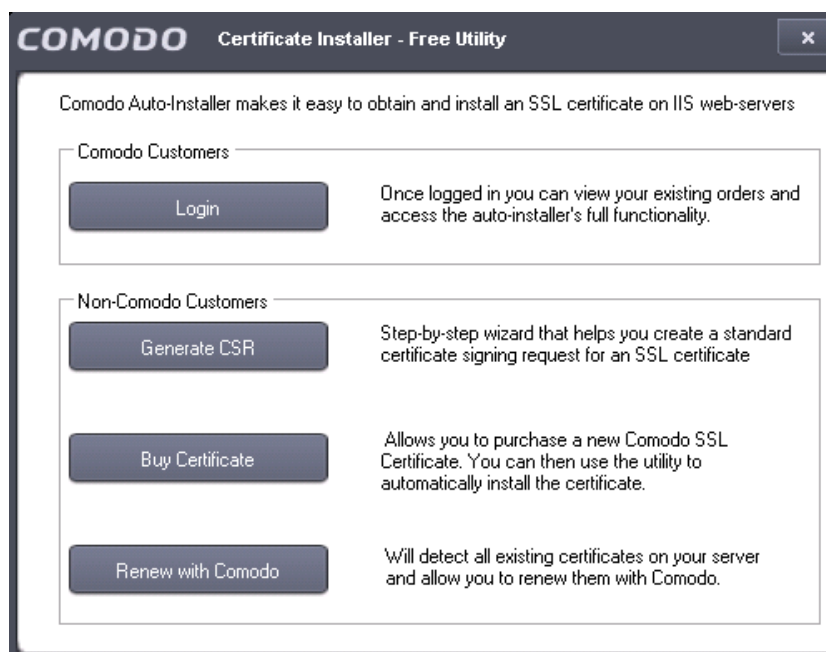


After agreeing to the user license, you will be asked to choose where to install the utility and to confirm start menu options before continuing to the setup review screen:

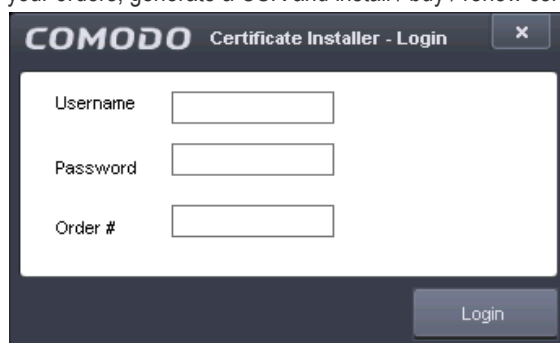


Click 'Install' to continue to begin installation. The utility requires .NET Framework versions 3.5.1 or above. To enable this on IIS, select Start > All Programs > Administrative Tools> Server Manager > Features > Add Features and select your .NET framework.

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** – 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:



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

## The Main Interface / Actions and Statuses

After logging in, the main interface will display a list of all certificates associated with your account, and a list of all sites that the utility detected on your IIS server:

The screenshot shows the Comodo Certificate Installer interface. The top pane, titled 'Orders', contains a table with columns: Order #, Order date, Expires, Domain name, Certificate status, Available Actions, and Apply. A callout box points to this pane, stating: "All your Comodo certificate orders appear in the upper pane". The 'Available Actions' dropdown menu is open, showing options: Autoinstall certificate, Complete request, Save certificate, and Renew Certificate. A callout box points to this menu, stating: "The actions you can take depend on the certificate status". The bottom pane, titled 'Detected sites', contains a table with columns: Site, Binding Information, Certificate, Available Actions, and Apply. A callout box points to this pane, stating: "The lower pane shows all web-sites discovered on your IIS server". The 'Available Actions' dropdown menu is open, showing the option: Generate CSR. A callout box points to this menu, stating: "Allows you to view and renew existing certificates". Another callout box points to the 'Certificate' column in the 'Detected sites' table, stating: "Lists existing certificates which are installed and bound to discovered sites. 'Red' certificates are non-Comodo".

Order #	Order date	Expires	Domain name	Certificate status	Available Actions	Apply
611069	2015-09-11	2016-09-10	companywebsite.com	issued	Autoinstall certificate Complete request Save certificate Renew Certificate	Apply

Site	Binding Information	Certificate	Available Actions	Apply
mydomain.com	*.443:	E=admin@email.com, CN=mydomain.co...	Generate CSR	Apply
payments.test.com	*.4431:	E=admin@email.com, CN=payments.tes...	Generate CSR	Apply
example.com	*.4432:	E=admin@email.com, CN=example.com...	Generate CSR	Apply
www.website.com		None	Generate CSR	Apply

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><b>Waiting for CSR</b></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><b>Processing</b></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>Domain Control Validation Replace CSR</p>
<p><b>Issued</b></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 Save Certificate Renew Certificate</p>
<p><b>Installed</b></p> <p>Certificate has been issued by Comodo CA and installed on the web-server but has not been bound in IIS.</p>	<p>Auto-install certificate Bind to site Save Certificate Renew Certificate</p>
<p><b>Bound</b></p> <p>Certificate has been installed and assigned to the domain in IIS.</p> <p>'Bound' certificates should also appear in the 'Detected Sites' area.</p>	<p>Auto-install certificate Save Certificate Renew Certificate</p>
<p><b>Awaiting Payment</b></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 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
- 2) Creates a site in IIS for the domain listed in the 'Domain Name' column (if one doesn't already exist)
- 3) Binds the certificate to the domain in IIS

Note - If the certificate has status of 'Installed' then 'Auto-install' will only perform 2) and/or 3) as required

## Complete Request

- 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

- 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.

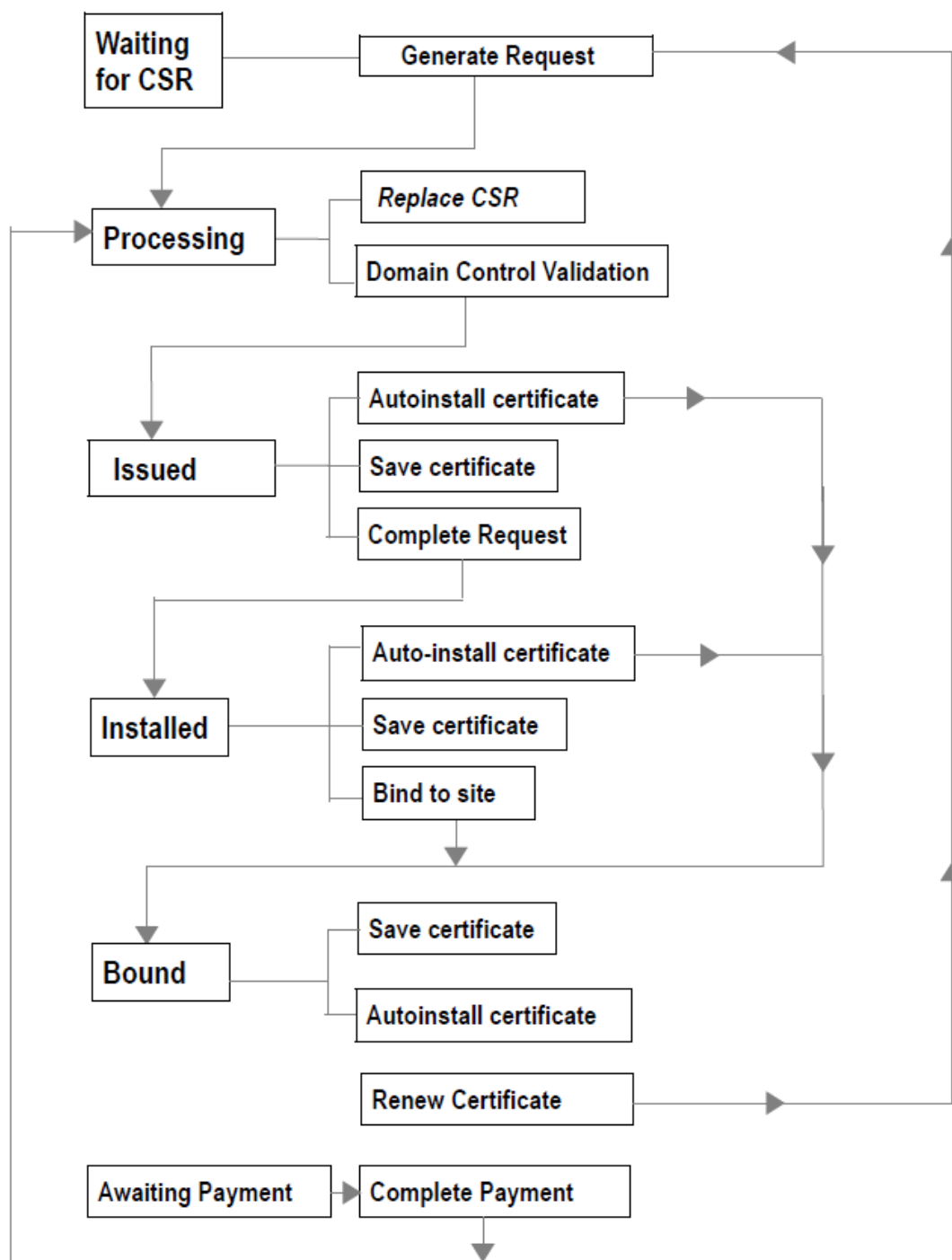
## Complete Payment

- Opens the Comodo order forms where you can enter payment details. Payment must be received before further processing can take place on your order.

## Save Certificate

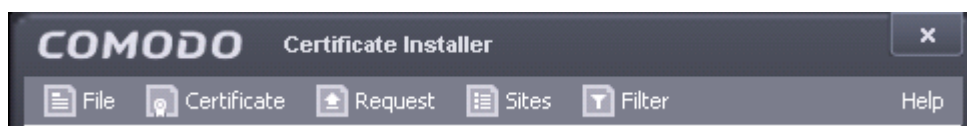
- Allows you to save a zip file containing your certificate to a location of your choice

This diagram illustrates the relationship between the statuses and actions:



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 'Detected Sites' shown in the lower pane.

## 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.
- 'Auto-install', 'Complete Request', 'Bind to site', 'Save to File', and 'Renew Certificate' - 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.

**Sites:** Displays a list of web-sites discovered on the IIS server. You can use the 'Generate CSR' feature to:

- Obtain a new certificate for a domain that does not have one
- Replace an existing certificate with a Comodo certificate

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

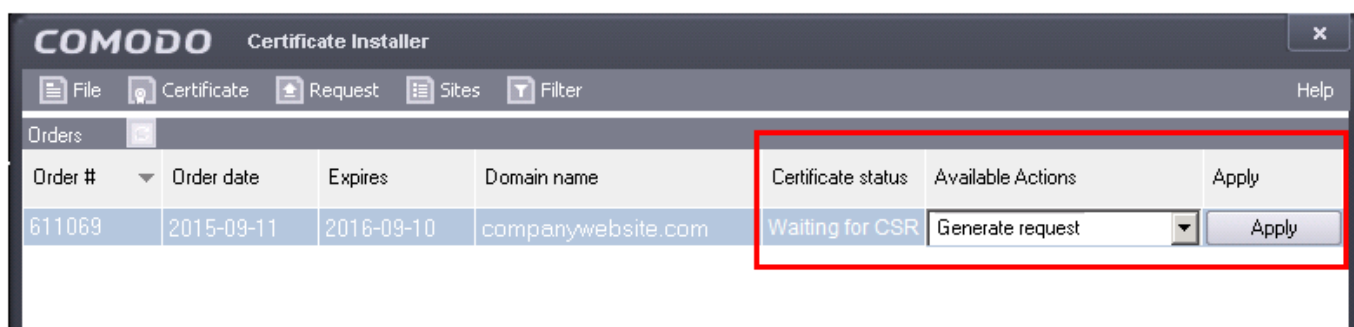
**Help:** Displays software version information and allows you to view the online user guide.

## 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

Generate  Paste

Common name:   
 multidomain

Domains list:

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

Make private key exportable

Generate

Send Copy to clipboard Save to file Cancel

- 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](http://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
- **'Make Private Key Exportable'**. 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.

COMODO Certificate Installer - Generate CSR

Generate  Paste

Common name:   
 multidomain

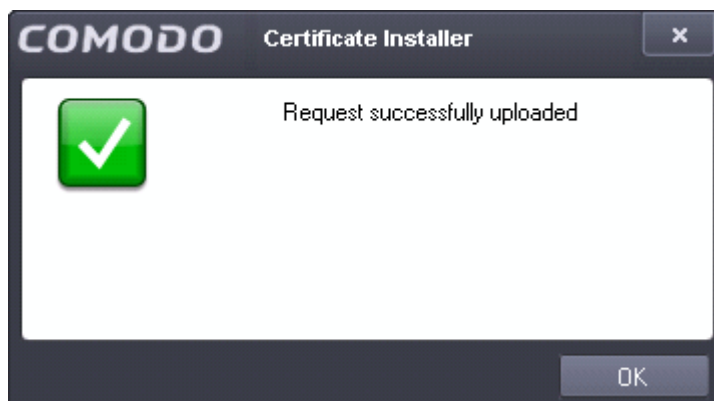
Domains list:

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

Make private key exportable

-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIEJDCCAwwCAQAwgBExCzAJBgNVBAYTAkJSMS0wKwYJKoZIhvcNAQkBFh55dwxp  
eWUyYmFzaGthdG92YUJjb21vZG8ub2QudWEuFDASBgNVBAgMC01hdG8gR3Jvc3Nv  
MQ8wDQYDVQQHDAZDdWlhYmEwJDAsBgNVBAMMG21haWw0ZkN0cWFhdXRvaW5zdGFs  
bGVyLm5ldESMBAGA1UECgwJRmxvd2VydWJkNvMRIwEAYDVQQQLDAIGbG93Zl1mQ28w  
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCb5TqvhoMw/t032e1dYFNd  
uWDFV/mXkLQJqTgavCatvPY8fEPVjNq6/5aqhsZu6X1Xw+ZiBe+Co95reJholgmh  
V1bgKZuuENdT h5JeY00WwvZNVJts+IITUvwJ32oMDYqTcPKZsHjq6niGjUKT d0X  
lw3fVxtf2Joy+MXgrRAbAgoip2uM7XGPtn5gRukN758DZ+P+6pP9QoA3gxHbyAu  
sp1IkJST1uWcfE/bZDhTiy88URTSwHQ80mwEWijAqx3/vKuSavw3ImGY+krpLy4D

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:

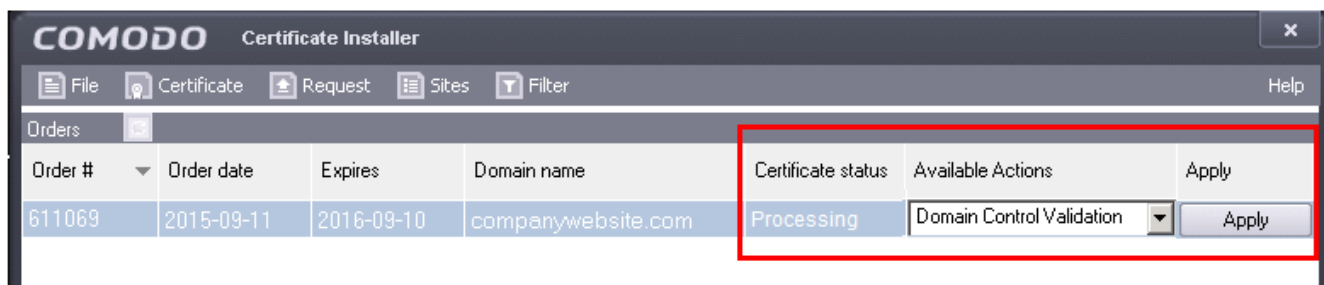


The certificate status will change to 'Processing' and 'Available Actions' for this certificate will now contain two options – 'Replace CSR' and 'Domain Control Validation'.

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:

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**

Submit

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 your 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 web 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**

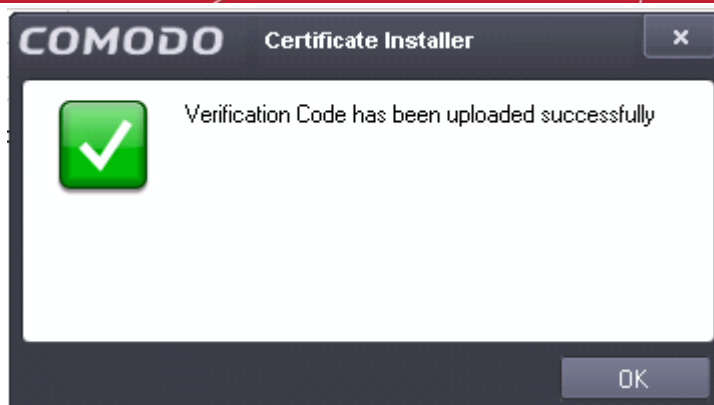
Please enter a validation code that was received via email: \_\_\_\_\_

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/>

However, in short, you need to create a .txt according to the following specifications:

File name	<Upper case value of MD5 hash of CSR>.txt
Content	<Value of SHA1 hash of CSR> comodoca.com

You can copy the MD5 and SHA1 hashes from the interface above. You then need to save it to your root directory then click 'Check File'

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.

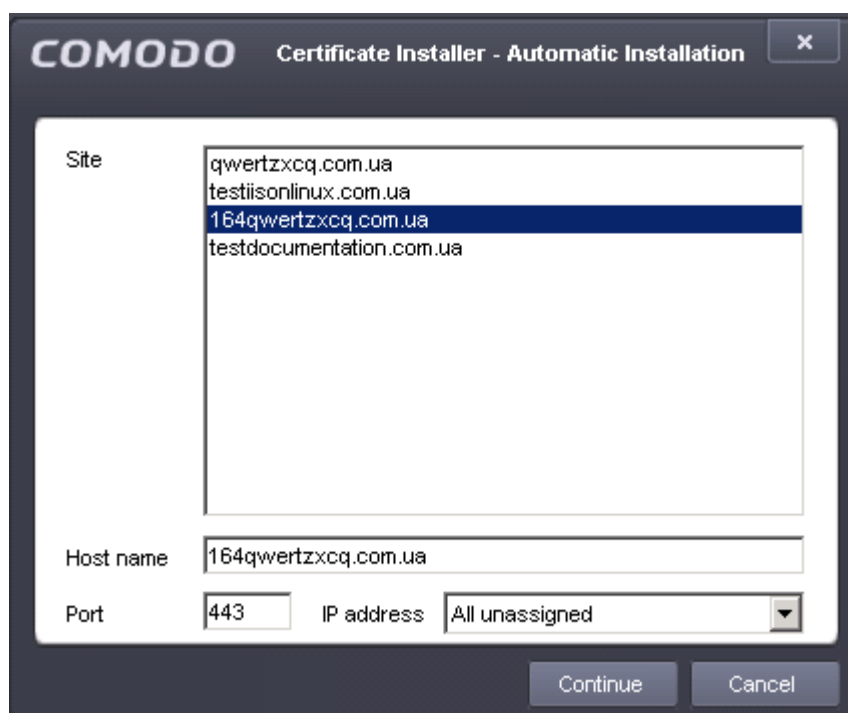
## Step 3 - Install and bind a certificate

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

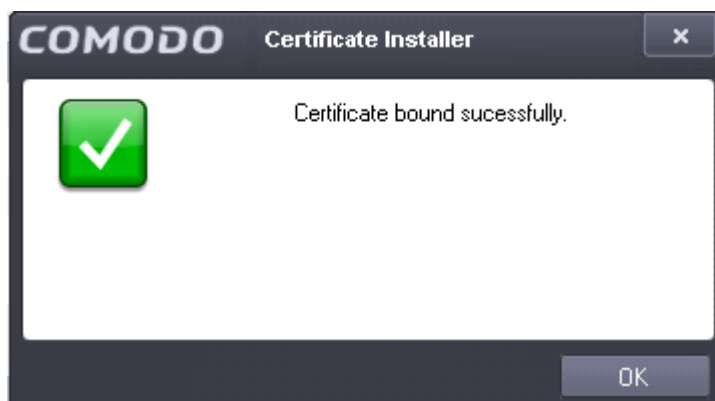
- 'Auto-Install' will install and bind your certificate in IIS and lead to a certificate status of 'Bound'
- 'Complete Request' will install the certificate but will not bind it. Leads to a certificate status of 'Installed'.
- If you choose the 'Complete Request' action, you will be presented with the 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:

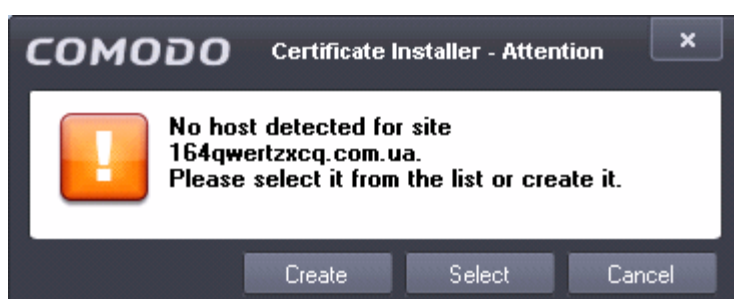
- In the main interface, select 'Autoinstall certificate' from 'Available Actions' and click 'Apply'. Choose the site you wish to install to from the 'Site' list box and click 'continue'. Doing so will instruct the auto-installer to install and bind the certificate to the website and host specified by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



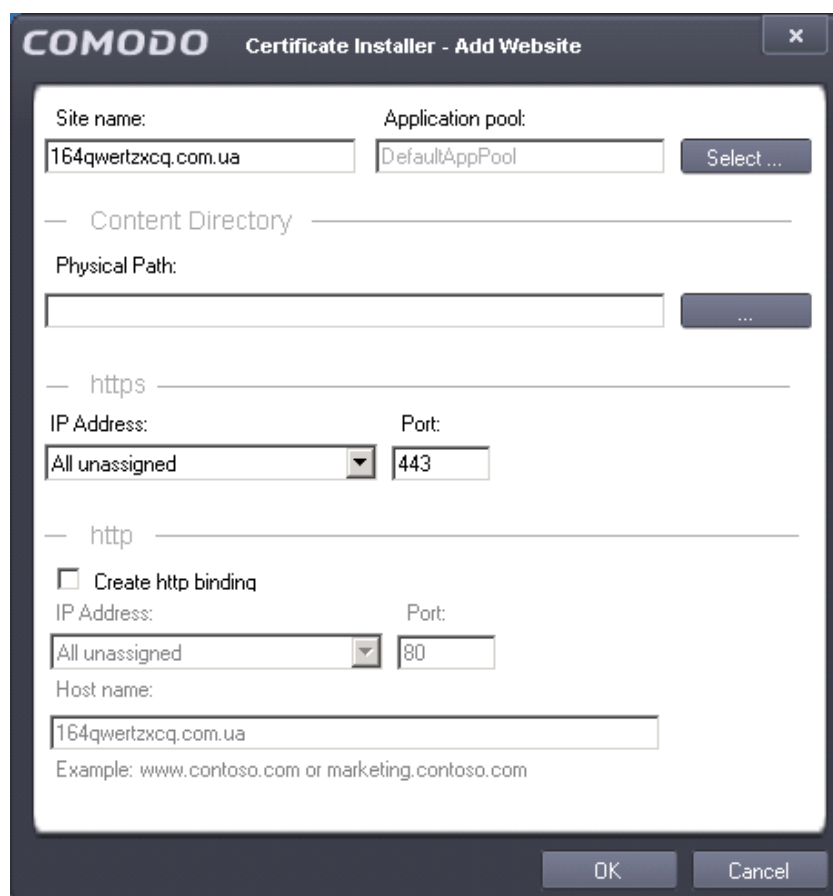
- If the site exists and is configured correctly, then you will see a confirmation message as follows



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

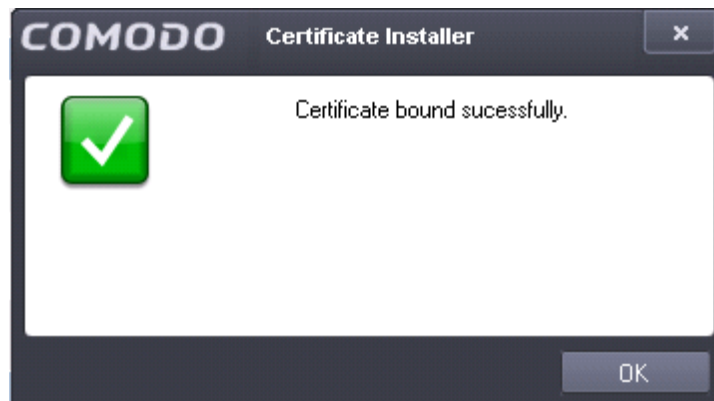


- Click 'Select' to go back and choose a different site. Click 'Create' to open the 'Add Website' interface:



- Type your website domain in the 'Site Name' text box.
- Application Pool (advanced users). If you have a particular application pool in IIS 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.



## Renewing a certificate

There are three ways you can renew a certificate:

- 1) 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.

- 2) 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.

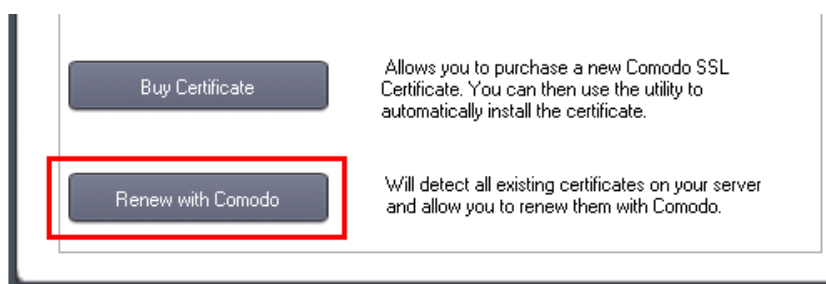


- Alternatively, you can renew a certificate by using the 'List of installed certificates' feature to find ALL installed certificates on your IIS server (the 'Detected Sites' area only shows certificates that are installed AND bound to a domain in IIS)

Detected Certificates	Valid From	Valid To	Subject	View	Renew
kk201504291051.com	4/30/2015	4/24/2016	CN=kk201504291051.com, C=US	View	Renew
UTN-USERFirst-Hardware	6/7/2005	5/30/2020	CN=UTN-USERFirst-Hardware, OU=http://www.i	View	Renew
kk201504220940.com	4/22/2015	4/16/2016	E=kk_2015-04-22-09-40@kkutsakov.comodo.oc	View	Renew

- 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:

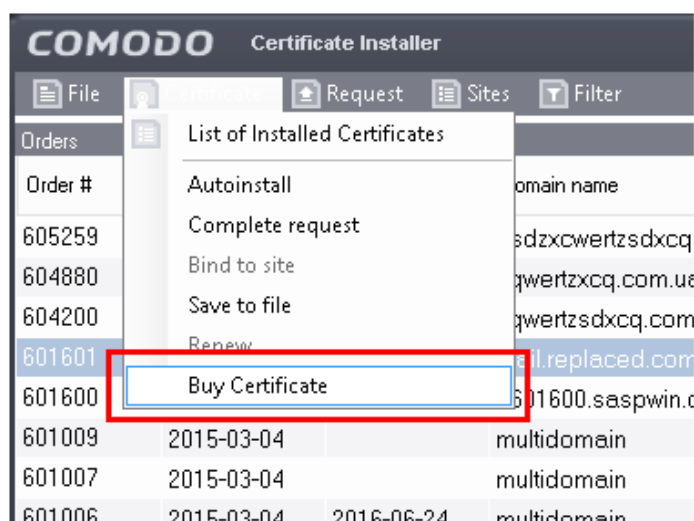


After choosing a certificate to renew using any of these methods, you will move onto the next step, **Completing Your Order**.

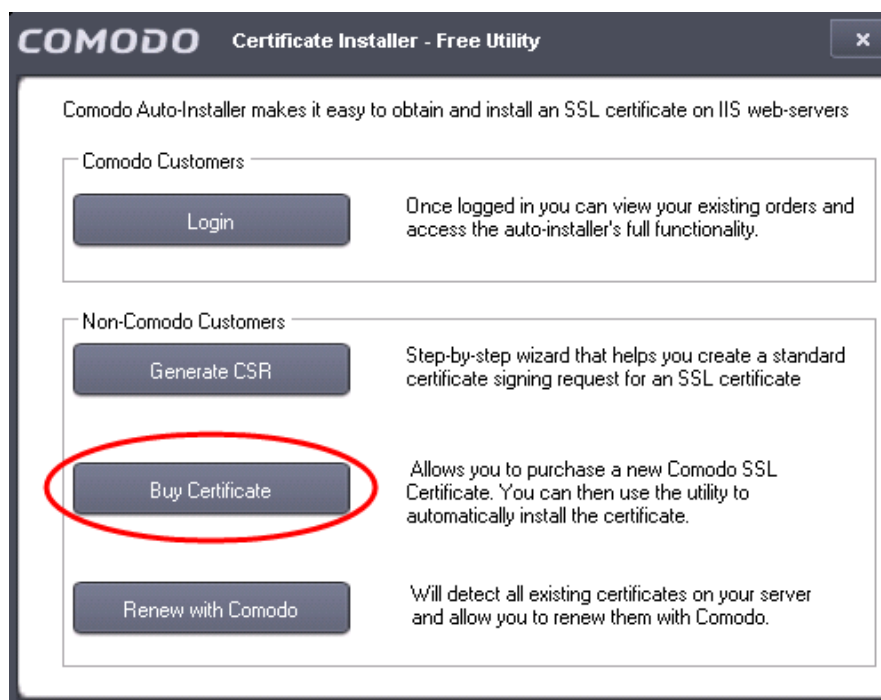
## Buying a certificate

There are three possible ways you can buy a certificate:

- 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**.

## Completing your order

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

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 yr(s): \$ 110.00/yr.

Currency: USD

**Domain details**

Common name \*

Domains list:

DCV Method \* Manual

[What's this?](#)

Hashing Algorithm NO PREFERENCE

[What's this?](#)

Generate CSR

Make private key exportable

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

**Summary**

COMODO SSL Certificate for \$ 110.00

< Prev Next >

- **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 deciding.

- **Price and currency:** Displays the price of your current selection and allows you to change payment currency.
- **Common Name** = Fully Qualified Domain Name (for example, [www.domain.com](http://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 IIS 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.
- **Hashing Algorithm:** Select your preferred algorithm from the drop box. Comodo strongly recommend SHA-2 unless you know you have legacy systems which require the older SHA-1 algorithm. If you choose 'No Preference', then this will default to SHA-2.
- **Generate CSR:** If enabled, the utility will automatically generate and send a certificate signing request with this application (recommended).

Click 'Next'.

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

COMODO Certificate Installer - Create new order

**Enter Your Account Details:**

Login Name \* testuser720@gmail.com  
*Login name should be min. 5 characters long.*

Password \* [REDACTED]  
*Passwords should be min. 8 characters long and contain at least one uppercase letter, one lowercase letter and one number*

Confirm Password \* [REDACTED]

**Enter Your Contact Details:**

First Name \* Peter

Last Name \* Johnson

Email Address \* testuser720@gmail.com

Telephone \* 0962356456

Job Title \* Flowers&CO

**Enter Your Company Details:**

Organization Name \* Flowers&CO

Street Address \* Companyaddress

Country \* United States (US)

Postal / Zip code \* 29072

City \* Cityname

State / Province \* Alabama (AL)

PO Box (Optional)

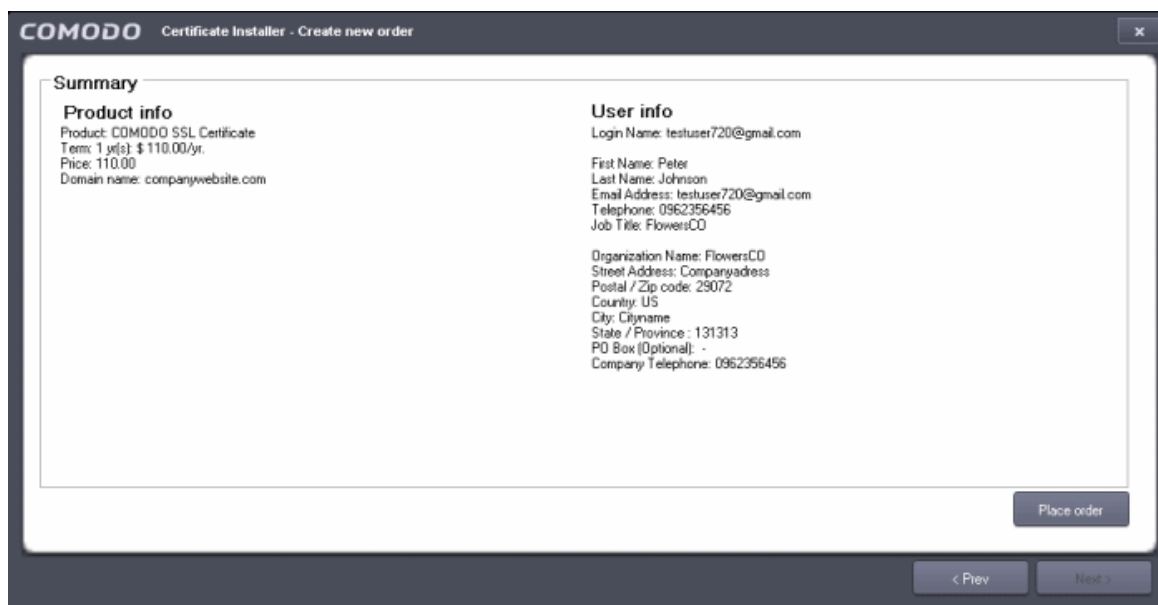
Company Telephone \* 0962356456

< Prev      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 'Next' when all fields are complete.

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



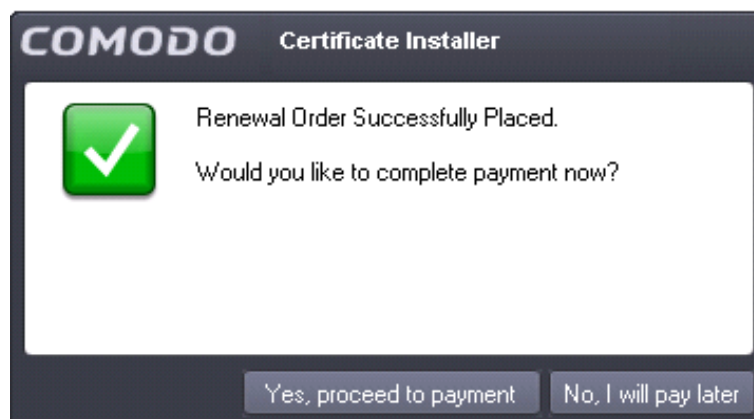
The screenshot shows a window titled "COMODO Certificate Installer - Create new order". It contains a "Summary" section with two columns of information:

Product info	User info
Product: COMODO SSL Certificate	Login Name: testuser720@gmail.com
Term: 1 y(s): \$ 110.00/yr.	First Name: Peter
Price: 110.00	Last Name: Johnson
Domain name: companywebsite.com	Email Address: testuser720@gmail.com
	Telephone: 0962356456
	Job Title: FlowersCO
	Organization Name: FlowersCO
	Street Address: Companyaddress
	Postal / Zip code: 25072
	Country: US
	City: Cityname
	State / Province: 131313
	PO Box (Optional): -
	Company Telephone: 0962356456

At the bottom right of the summary area is a "Place order" button. At the bottom of the window are navigation buttons: "< Prev" and "Next >".

- Click 'Place Order' to continue.

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



The screenshot shows a dialog box titled "COMODO Certificate Installer". It features a green checkmark icon on the left. The text reads:

Renewal Order Successfully Placed.  
Would you like to complete payment now?

At the bottom, there are two buttons: "Yes, proceed to payment" and "No, I will pay 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:

Secure Payment

Welcome:  
Auto Installer  
AI Development

Logout

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:

Account Options

Sign Up

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](mailto:sales@comodo.com)

Telephone:  
+1 288 286 6361  
+1 203 581 6361

Cancel & Start Again    Make Payment

© Copyright 2015. All rights reserved.    Using VPN (Comodo Office)  
Client IP: 192.168.75.102    Thursday, July 23, 2015  
Server IP: 192.168.0.190

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 \* Manual   
[What's this?](#)

Hashing Algorithm NO PREFERENCE   
[What's this?](#)

Generate CSR

Make private key exportable

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

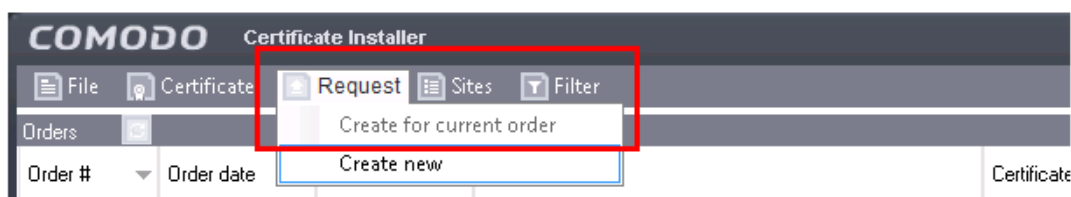
2. To generate a CSR for one of your existing certificate orders:

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



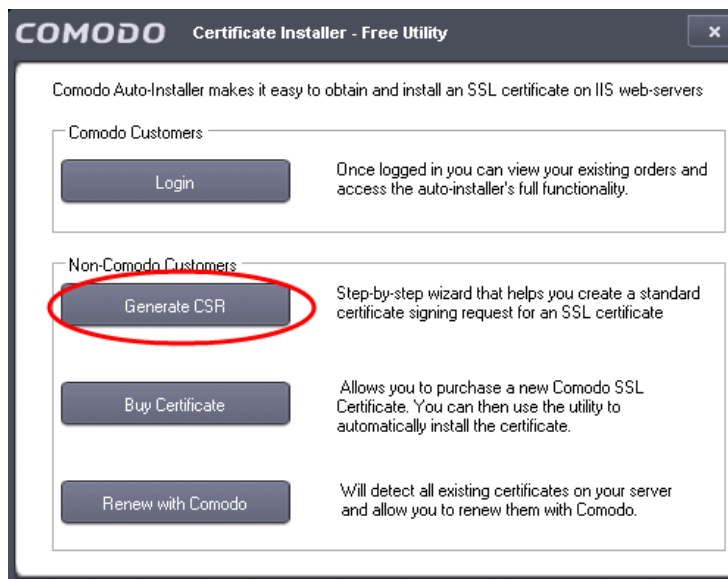
OR

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



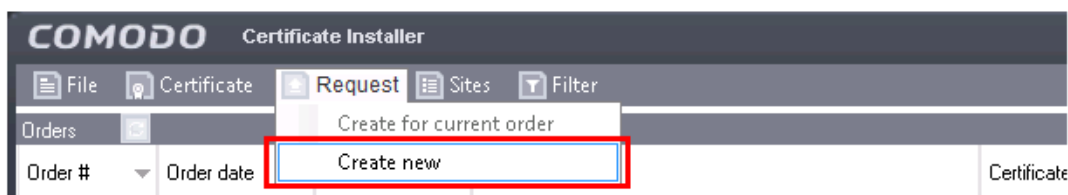
Both methods will start a wizard that will help you create and submit a CSR for the domain listed in the 'Domain Name' column. [Click here](#) to find out more.

3. You can also generate a standalone a CSR for later use by either:
  - (i) Clicking 'Generate CSR' at the start-up dialog:

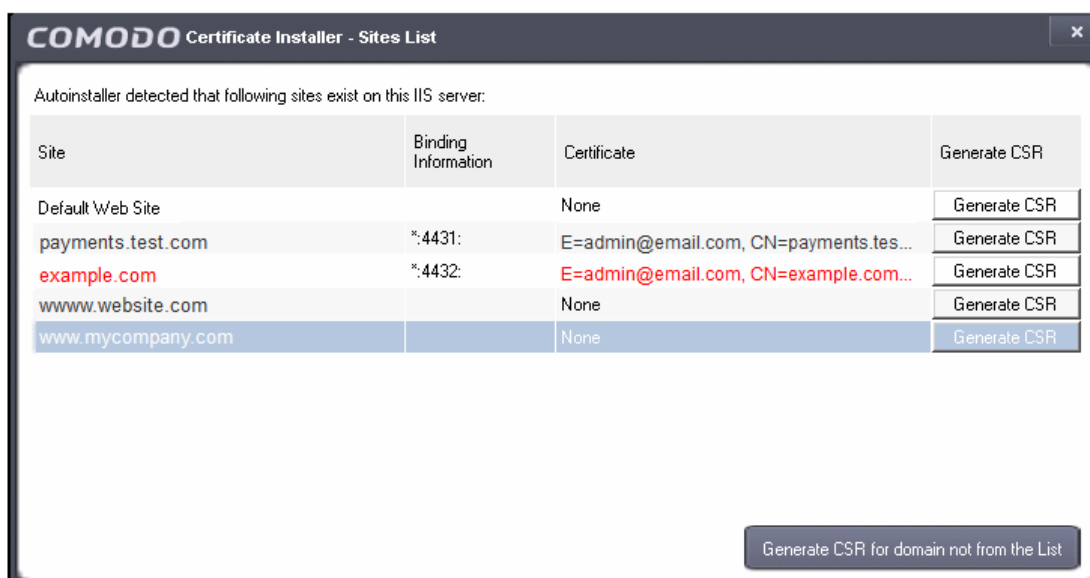


OR

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



In both cases, this will open the 'Sites List' window which shows all domains that the utility discovered on your IIS 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.

## 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**

1255 Broad Street

STE 100

Clifton, NJ 07013

United States

Tel : +1.877.712.1309

Email: [EnterpriseSolutions@Comodo.com](mailto:EnterpriseSolutions@Comodo.com)

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