COMODO
Creating Trust Online®

Comodo Server Security Server

Software Version 2.4

Quick Start Guide

Guide Version 2.4.041718

Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

1. Comodo Server Security Server – Quick Start Guide

This tutorial explains how to use S³ to manage the purchase and lifecycle of SSL certificates on IIS and Apache web-servers.

Prerequisites and setup

- You have placed at least one order for a Comodo certificate (recently or in the past)
- Your websites are running on Apache web server on Linux (CentOS, Fedora, Ubuntu or Debian)
- You should install the certificate controller software on any Windows or Linux machine on your network
- Once the controller/agent is installed, you can use the S³ portal to add servers, view orders and manage/install certificates

Please use the following links to go straight to the step that you need help with:

Step 1 - Log into S³

- Login to your S³ account at **https://s3.comodo.com** by entering your Comodo account username and password followed by one of your product order numbers
- If you see a message stating your login credentials have expired, click the link to update them
- If you are logging into S³ for the first time, read and accept the 'End User License Agreement'

New users

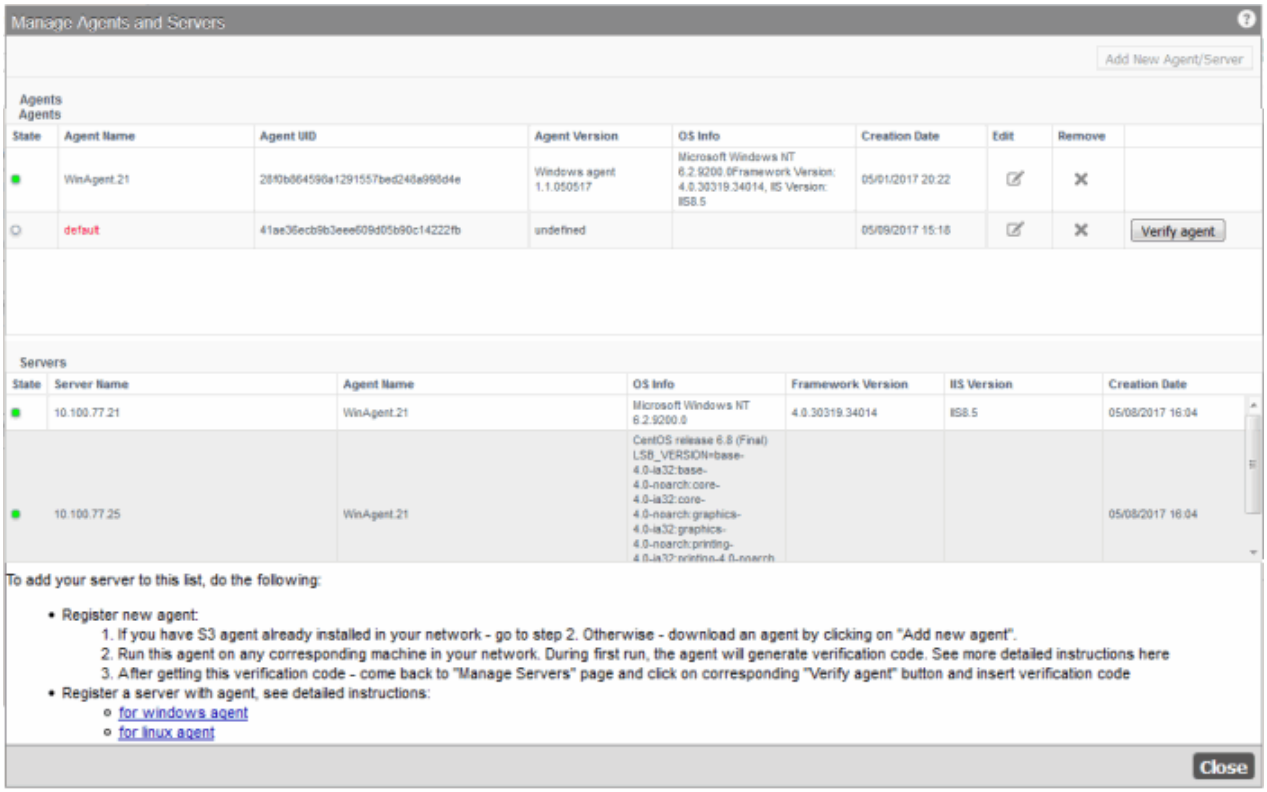
- If you do not have a Comodo account, click 'Don't have account? Create New'. You will be taken to the account creation page
- Complete the enrollment form and agree to the EULA and subscriber agreements
- You will see a confirmation message once your account is created
- **Important** – Please make a note of the order number shown in the confirmation screen. You will need it to login on future occasions.
- Click 'OK' to automatically login to S³.

Step 2 - Add your Servers

In order to establish communications between S³ and your servers, you need to install the S³ agent on a Linux or Windows machine on your network.

To add agents:

- Click the 'Manage Servers' button then the 'Add New Agent/Server' button
- In the 'Agent Download' screen, type a name to identify the agent
- Download the 'Linux' or 'Windows' agent suitable for the machine on which you are going to install the agent



Note: The 'Windows Utility' is **not** an S³ agent. It is a standalone application called 'Comodo Certificate Auto-Installer' which is designed to be directly installed on an IIS server.

- Click 'OK' to register the agent in the 'Manage Agents' interface.

Next, you need to install and activate the agent. Use the following links to find out more:

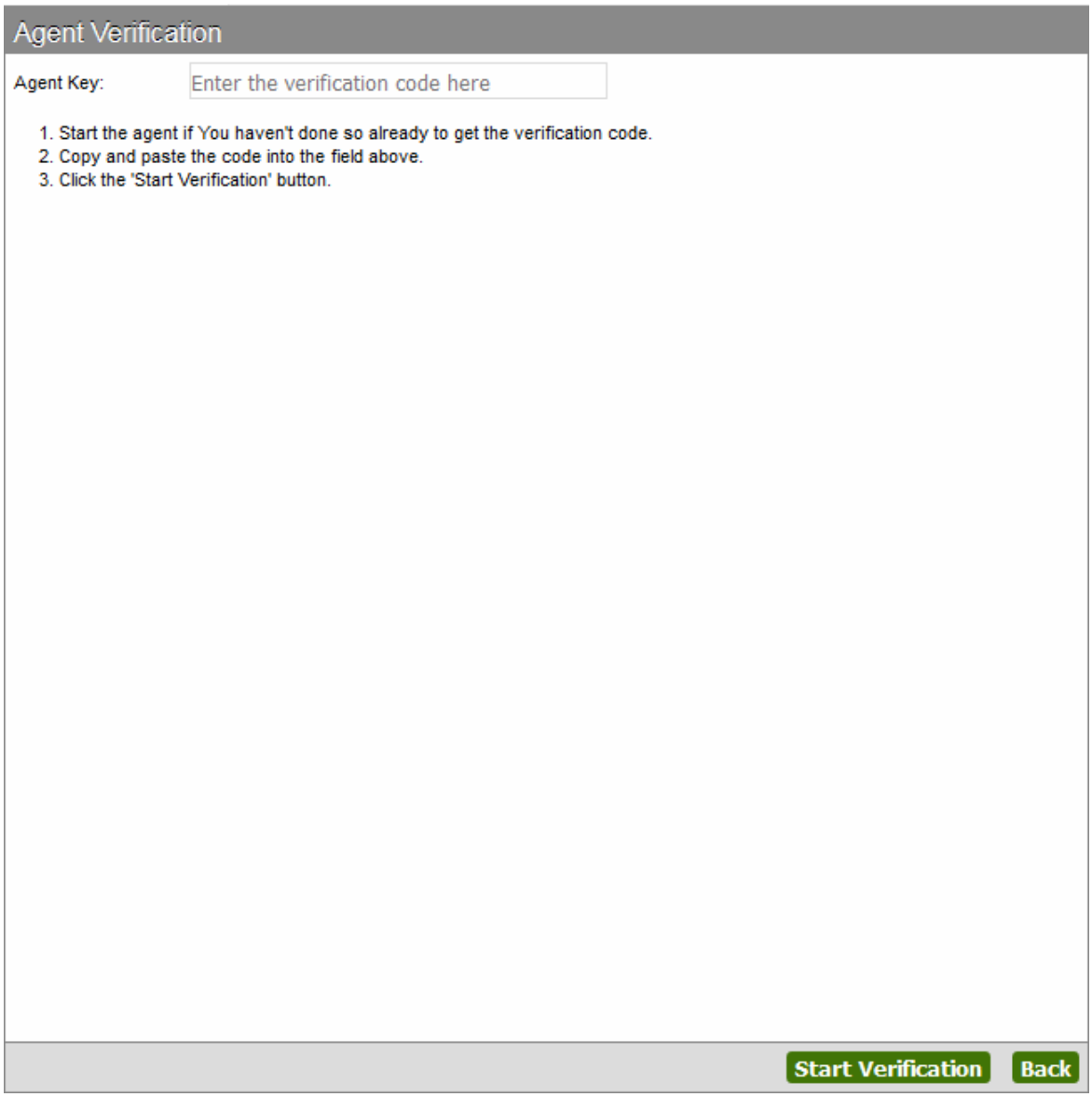
- **Installing the agent on a Windows machine**
- **Installing the agent on a Linux machine**
- **Managing agents and servers**

Install the agent on a Windows machine

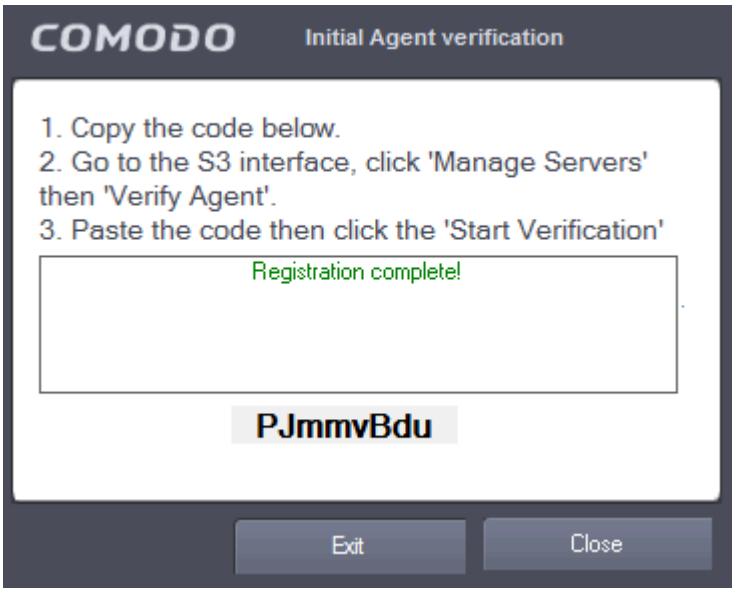
Note: Please ensure you have admin privileges to run the application.

- Extract the contents of the zip file to the Windows machine you wish to use to control your servers
- Open 'ComodoS3Agent.exe' to start the installation process.

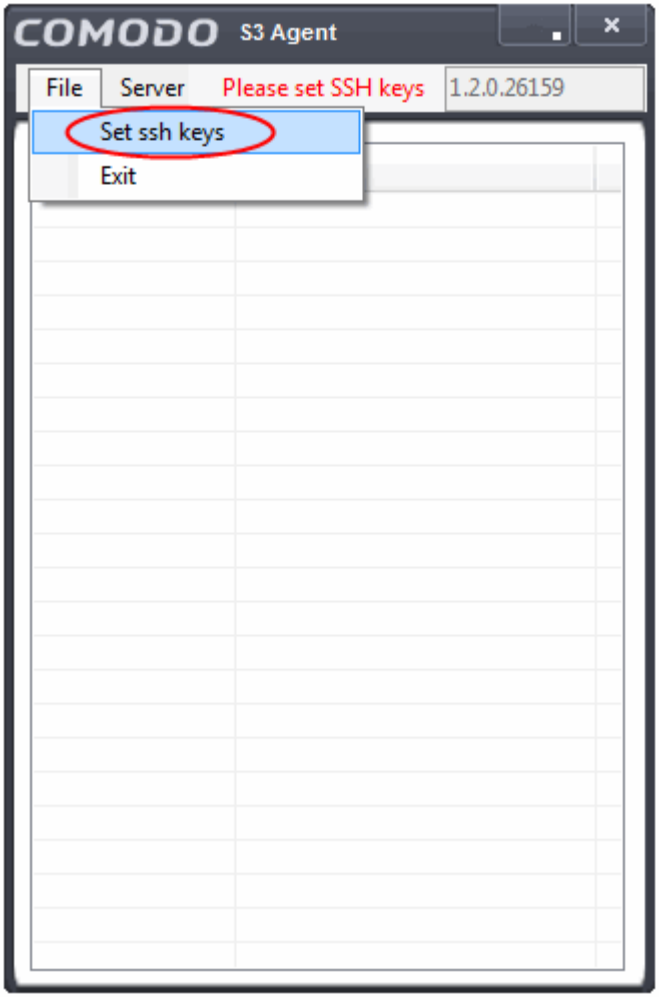
- To synchronize the agent with S³:
  - Copy the unique code from the 'Initial Agent verification' dialog
  - Login to the S³ web interface and click the 'Manage Servers' button
  - Locate the agent you have just installed and click the 'Verify agent' button
  - Paste the verification code into the 'Agent Key' text box then click the 'Start Verification' button:



- Next, go back to the agent verification dialog on your Windows machine and click 'Finish Verification'.



- Click 'Close'. The S³ Agent dialog will open
- Select 'Set ssh keys' from the 'File' menu or choose 'Please set SSH keys'

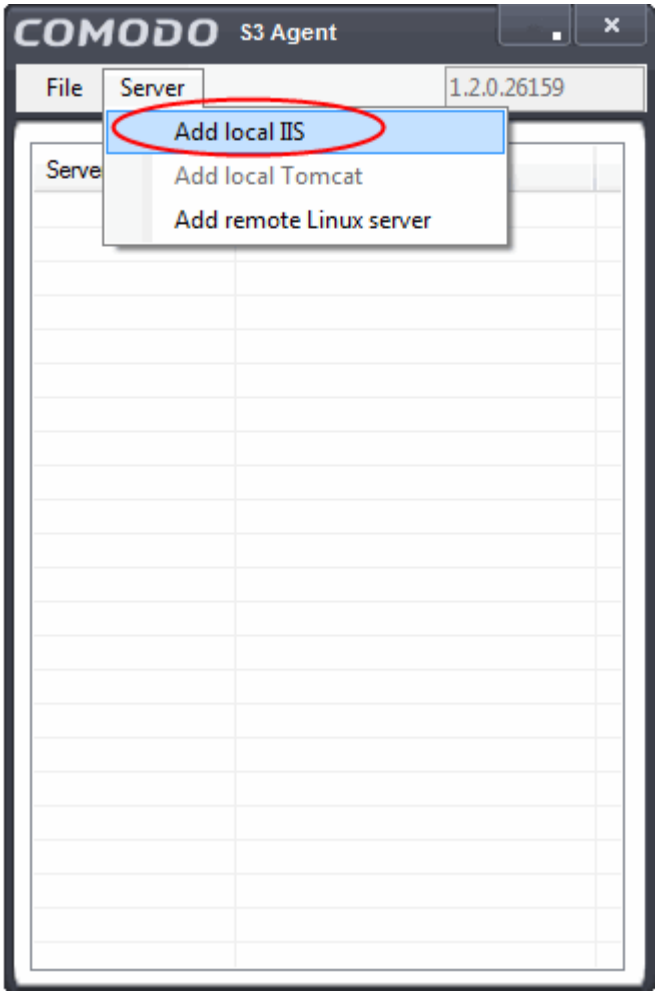


You can configure the SSH key pair in three ways:

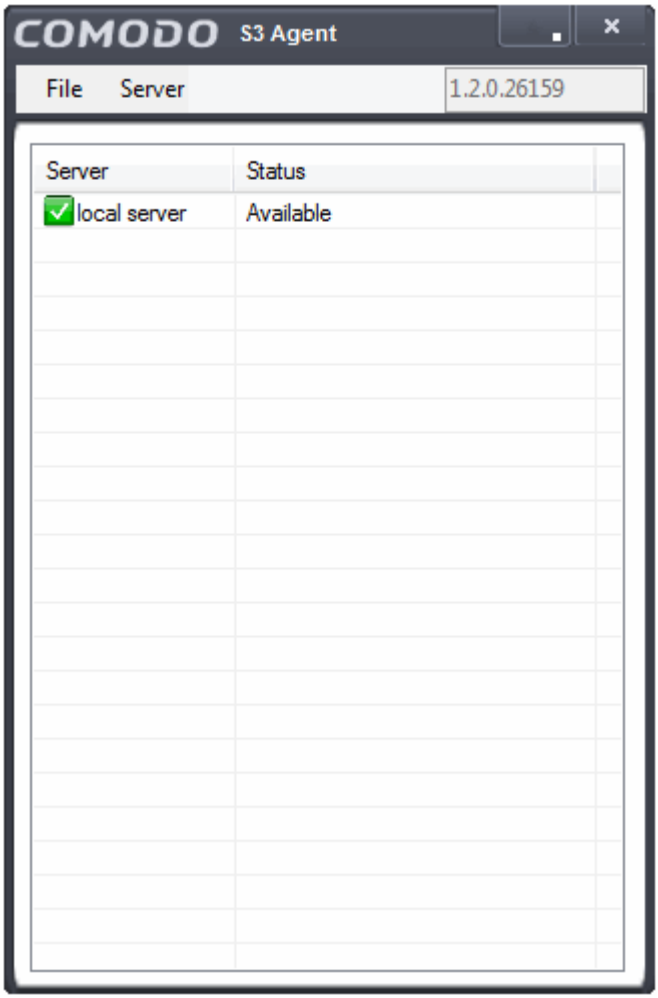
- Generate keys on Comodo server – Automatically generate the SSH key pair on Comodo's servers

- Generate keys on my own Linux PC – Generate keys by entering Linux credentials (server address, login, password and port)
- Provide generated keys (private and public) - Select your SSH keys from file saved on your local computer

- To add servers to S³, open the 'S3 Agent' dialog and select an available server from the 'Server' tab:
  - You can add server in three ways:
    i. Add local IIS. This option is active if IIS web server is running on the server
    ii. Add local Tomcat. This option is active if "CATALINA_HOME" windows environment variable is defined in your Windows server configuration. Tomcat service is registered and running
    iii. Add Remote Linux server. This option is active if SSH keys are generated

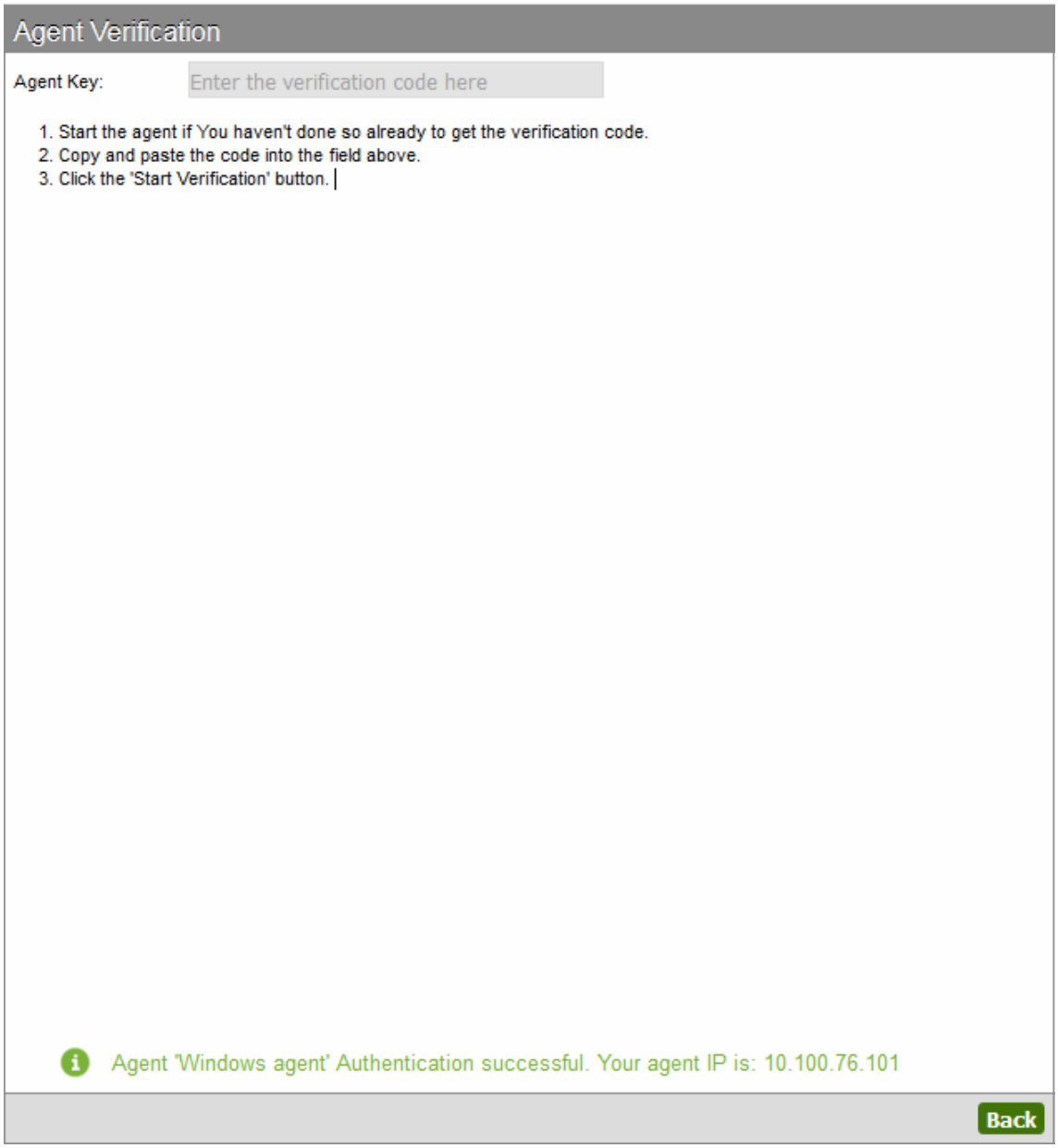


  - 'Add Remote Linux server' opens the 'Add Linux server' dialog to provide SSH Key-Based Authentication on a Linux server (server address, login, password and port). This allows the agent to connect to the server for authentication
- Manage 'Add local IIS' will add the server to the S³ agent list:



Install the agent on Linux machine

- Launch Linux agent: `./autoinstaller` and follow the verification instructions
- Go to the S³ interface, click 'Manage Servers' then the 'Verify Agent' button
- The 'Agent Verification' dialog will open. Copy and paste the code into the 'Verification Code' box and click 'Start Verification'
- Next, go back to the agent console and press 'y'
- Your request will be sent to authenticate the agent and S³. After that, you will see the successful verification message



- After the file is verified, you can add servers by entering the following line at the command line interface:

  ./autoinstaller -m add -ip 192.168.10.10 -u auto

  ...replacing '192.168.10.10' with the IP or hostname of your server.

  ...replacing 'auto' with admin login.

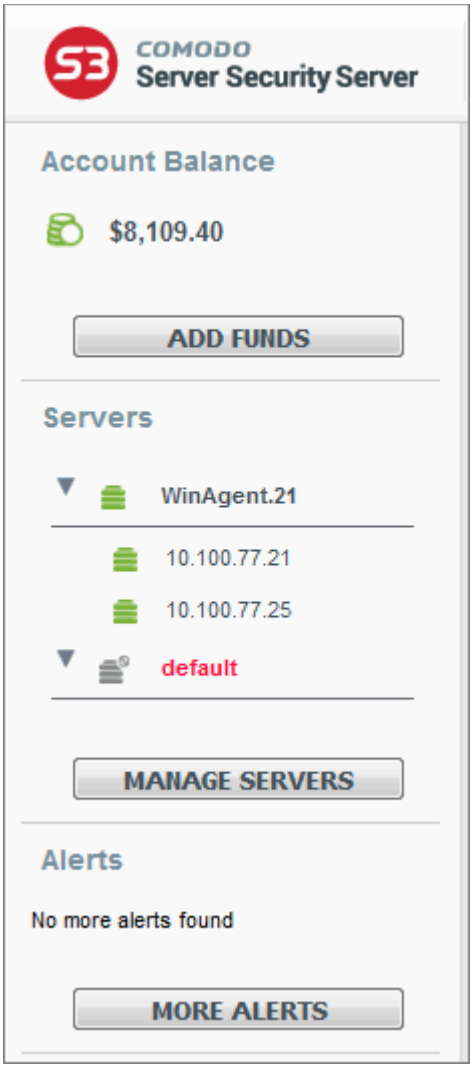
```
auto@ubuntu:~/Agent/deb_x64$  ./autoinstaller -m add -ip 192.168.10.10 -u auto
Parsing autoinstaller config file(./autoinstaller.config) and command line
add:192.168.10.10 auto


192.168.10.10auto
The authenticity of host '192.168.10.10(192.168.10.10' can't be established.
ECDSA key fingerprint is 6e:a8:a9:49:db:3a:d2:6f:0f:78:bb:93:70:9e:bb:38.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.10' (ECDSA) to the list of known hosts.
auto@192.168.10.10's password:
Now try logging into the machine, with "ssh 'auto@192.168.10.10", and check in:

  ~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.



192.168.10.10auto

retcode: 0
auto@ubuntu:~/Agent/deb_x64$
```

Note: Your agent must be activated before adding the server

- Repeat the process to add more servers

Managing agents and servers

Upon successful connection, your servers will appear in the S³ interface area. Each agent is shown separately with its IP addresses listed underneath:



Server statuses:

- A green icon indicates the server is actively connected to S³
- A gray icon indicates the server is not connected. This could be because the agent is not launched
- A red agent name indicates an un-synchronized or outdated agent
- A red key next to green/red server indicates the SSH keys are not present. Launch the agent as administrator and set your SSH key pair as **explained above**

To update an agent,

- Exit the agent then go back to S³ interface and click 'Manage Servers'
- Select the agent then click 'Edit'
- Download, save and unpack the new agent into the current directory
- Run the agent. Agent status will change to 'Active' once successfully connected.

Note: You will be automatically notified when updates are available for the Windows agent.

From the 'Manage Agents and Servers' dialog displays:

- Agents which are shown in the top half of the window allows you to view, edit the agent name and re-

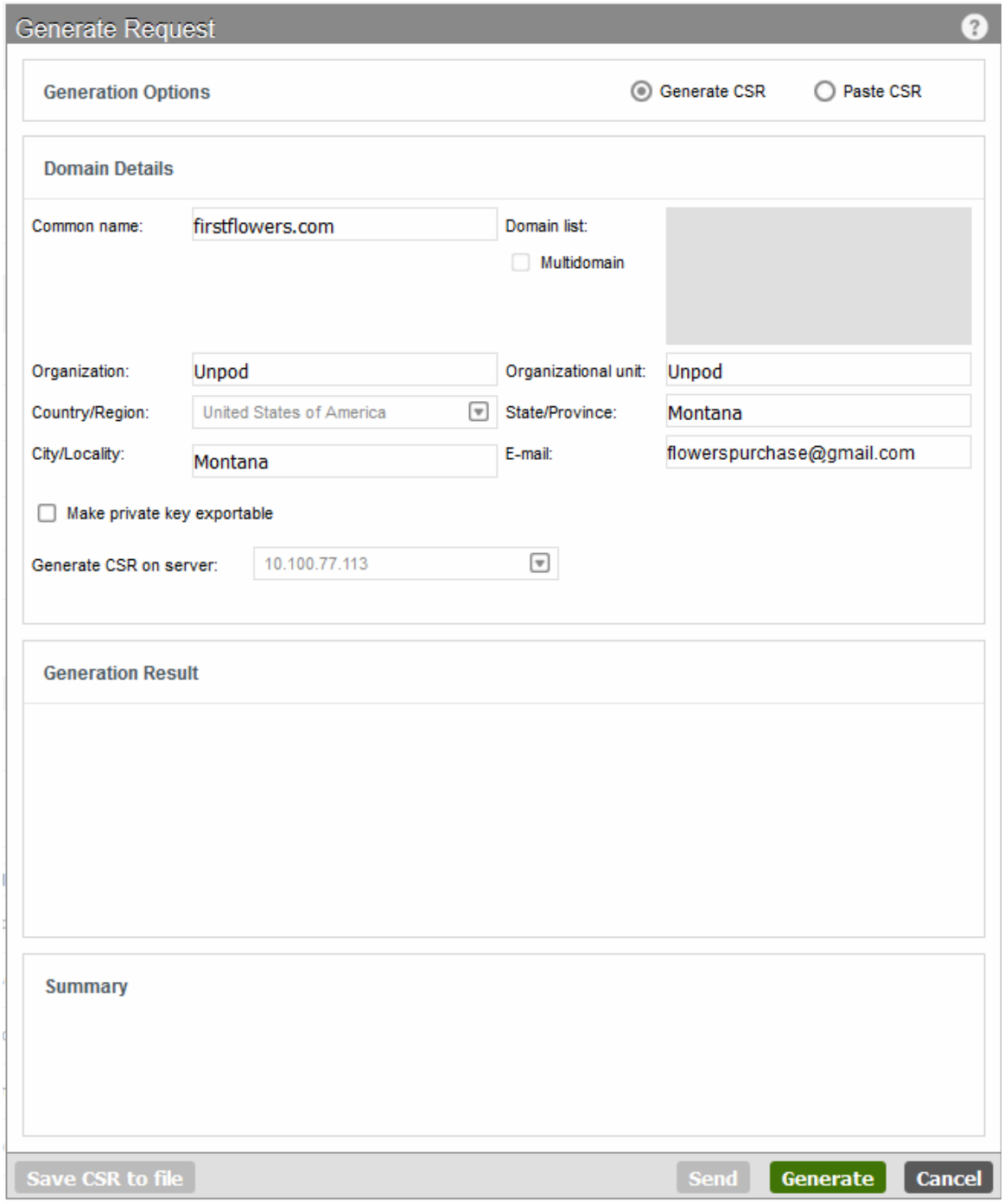
download it if required

- All servers added via those agents are listed at the bottom
- Both agent and server must be active (green icon) for S³ to carry out actions such as installing certificates.

Step 3 - Generate and Submit a CSR

The next step is to generate a certificate signing request.

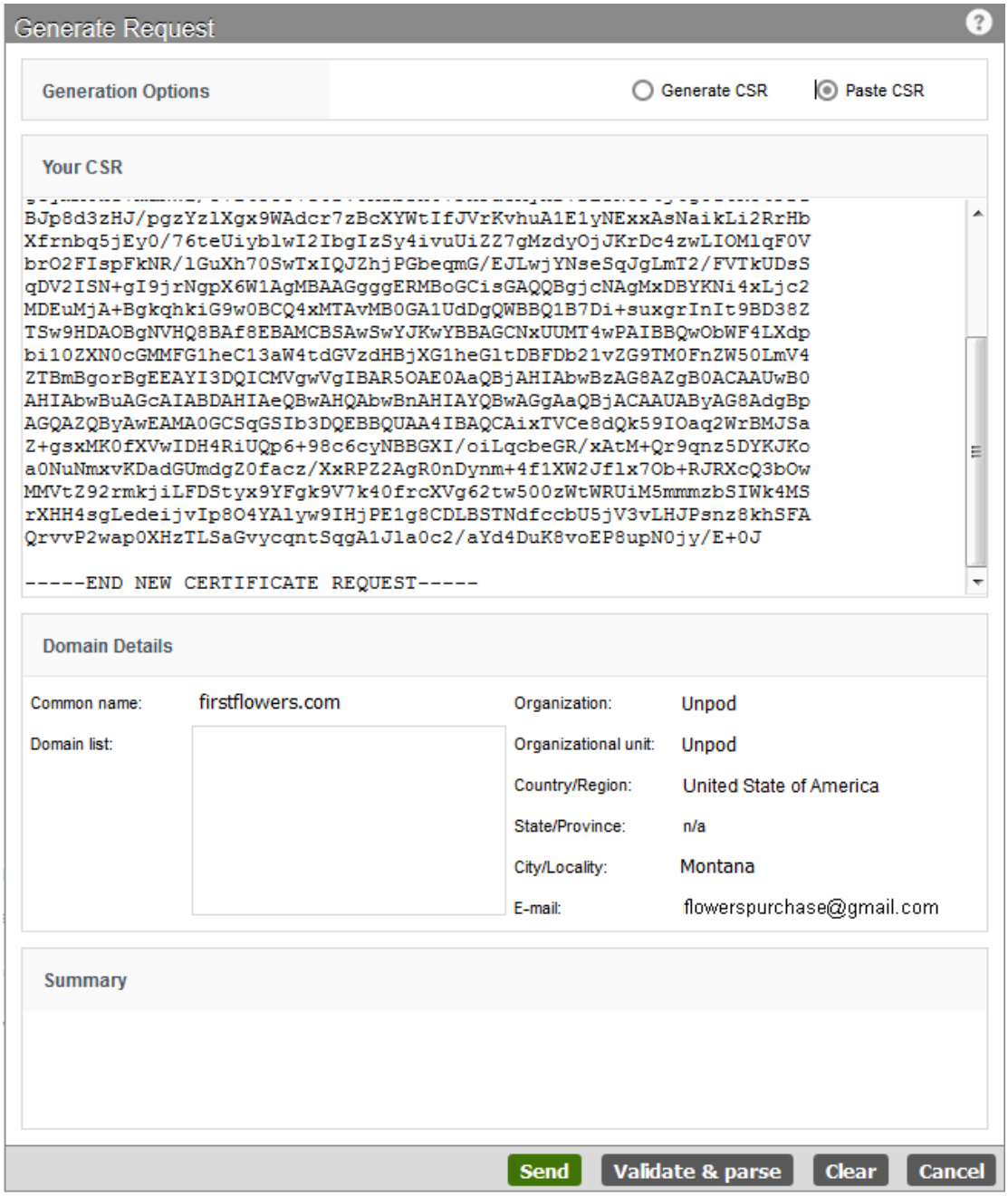
- Choose an order with a 'Certificate Status' of 'Waiting for CSR', select 'Generate request' and click 'Apply'.



- This will open the 'Generate Request' form:

Generation Options:

- If you already have a CSR you wish to use, select the 'Paste CSR' radio button. Paste your CSR into the 'Your CSR' text area. Click 'Validate & parse' to test the CSR is correct then click 'Send' to submit the CSR to Comodo CA.



- If you do not already have a CSR, you need to complete all fields. Note: This requires software agent to be installed and run). Most are self-explanatory, but for those with little experience of certificates:

Domain Details

- Common Name: Fully Qualified Domain Name (for example, www.domain.com). This should be auto-populated.
- Domain list: Enter all domains covered by the certificate. Each domain should be on a separate line. (Active if

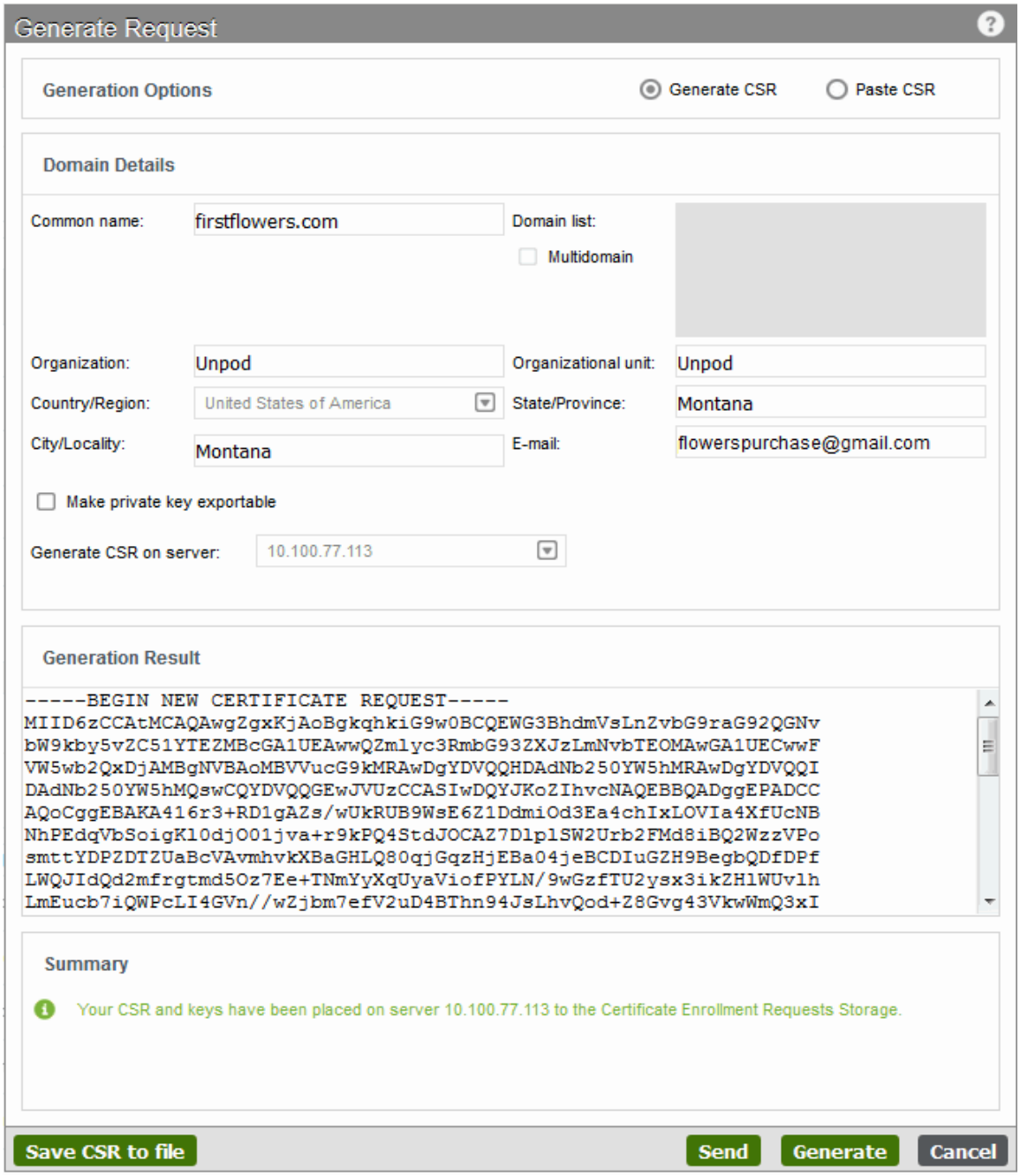
'Multidomain' is checked)

- Multidomain: Check this box if you purchased a multi-domain certificate. You should enter all domains covered by the certificate in the 'Domains List' box. Each domain must be specified in 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)
- Country/Region: The two-level country code for your country
- State/Province: The name of the state or Province in which your organization is located
- City/Locality: The name of the city in which your organization is located
- E-mail: Your contact email address
- 'Make Private Key Exportable' (For Windows only). 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.
- Generate CSR on server: Choose the server on which the CSR should be generated. This should be the server which hosts the domain that you are getting the certificate for.

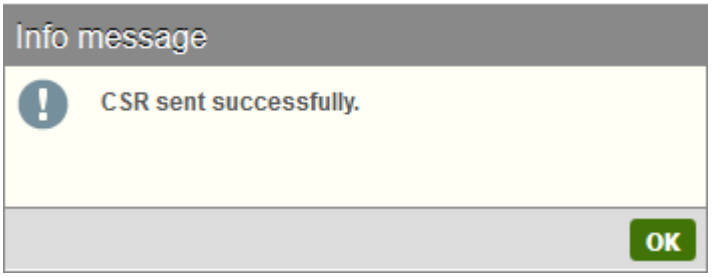
After the CSR form is complete:

- Click 'Generate' to automatically create a CSR from the details you entered:



- Click 'Save CSR to file' to save your CSR in .txt format on your local machine
- Click the 'Send' button to submit the CSR to Comodo.

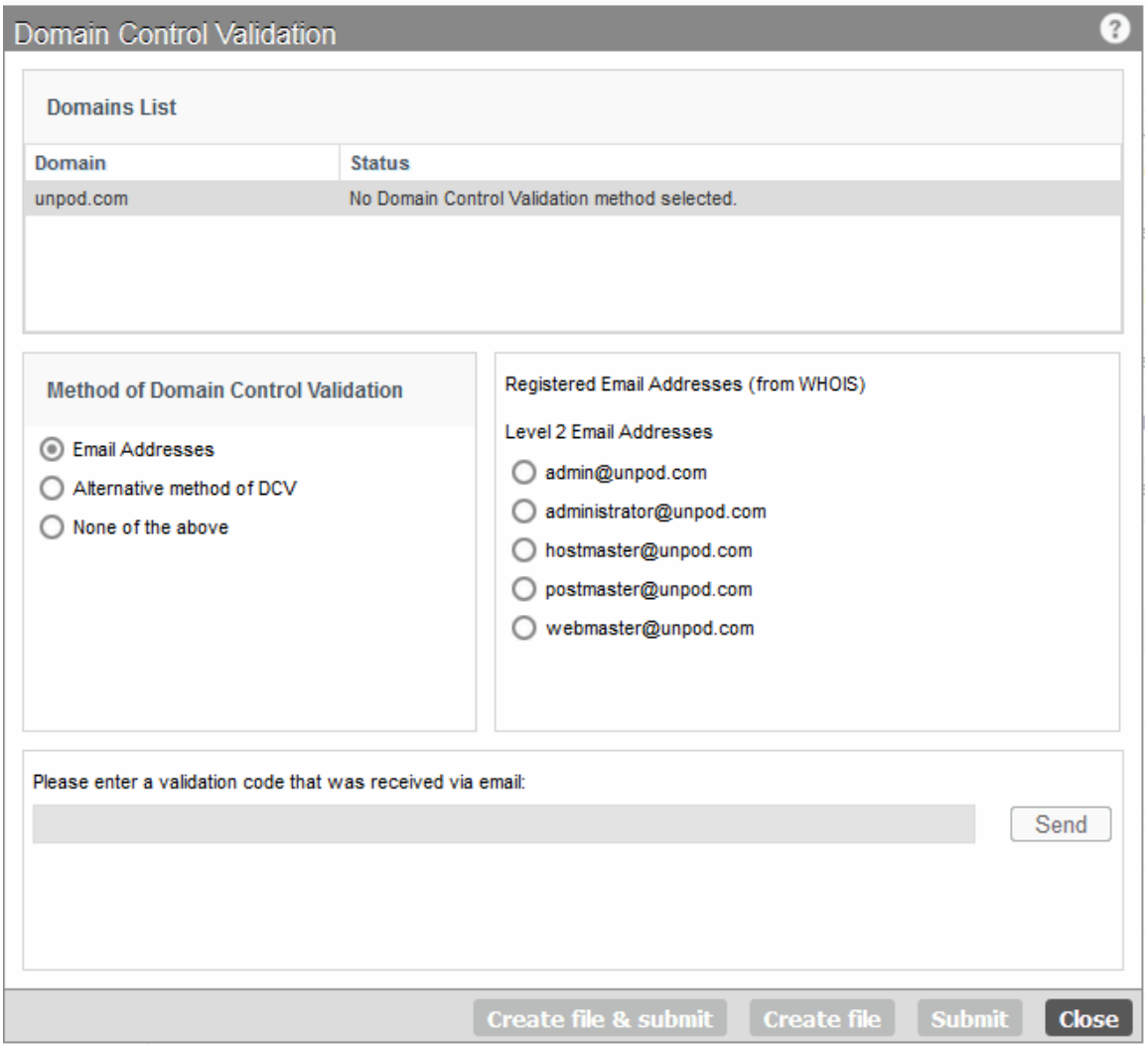
A confirmation message will appear:



- The certificate status will change to 'Processing' and 'Actions' for this certificate will now contain three options – "Replace CSR", "Domain control validation" and "Request Invoice".

Step 4 - Complete Domain Control Validation (DCV)

- Locate the certificate on which you wish to complete DCV in the 'Orders' pane of the home screen
- Select 'Domain control validation' from the 'Actions' drop-down and click 'Apply'
- This will open the DCV configuration screen:



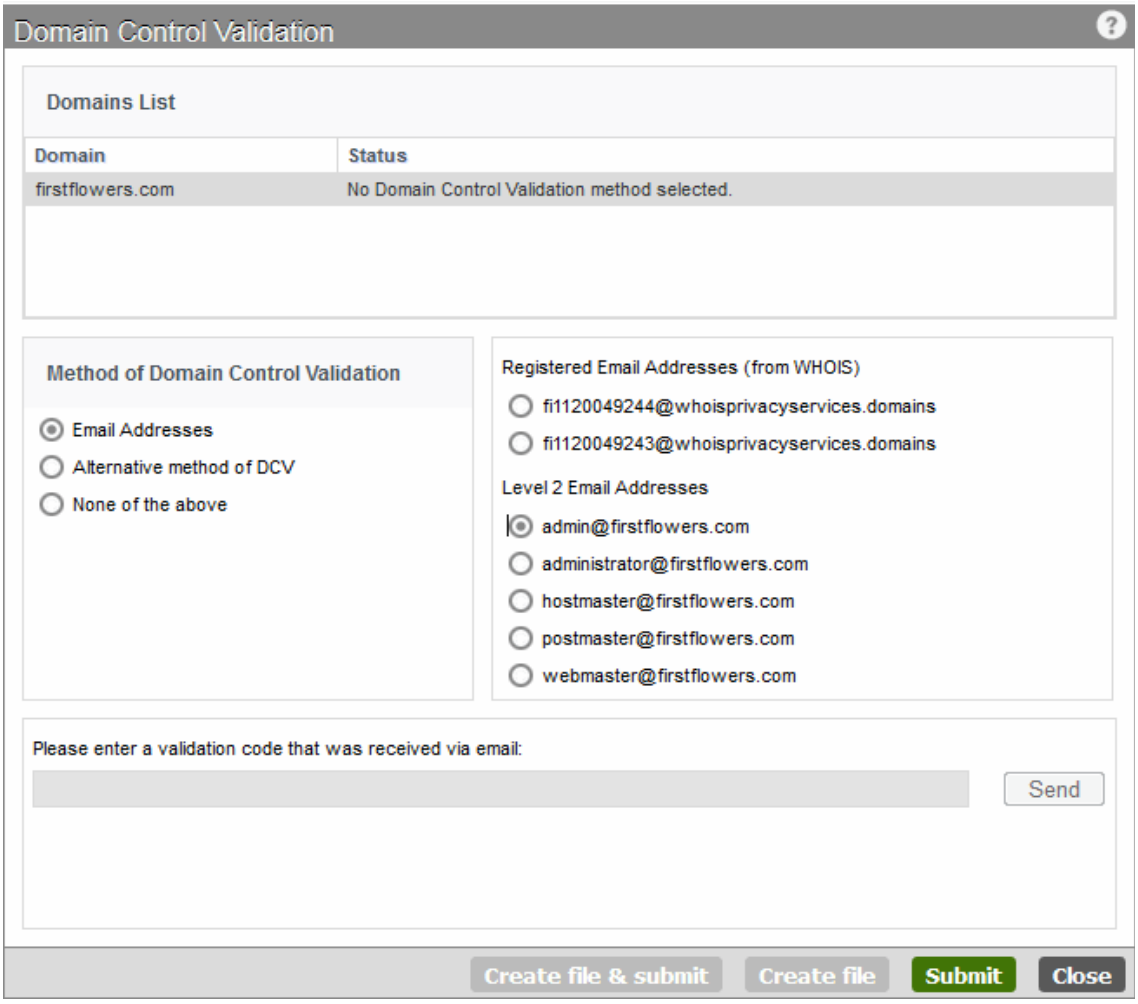
- In the 'DCV Method' box on the left, choose *one* of the following options:
  - **Validation by email address** – You confirm domain ownership by responding to a mail sent to an email address registered for this domain. You are presented with a choice of email addresses drawn from the WHOIS database 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.



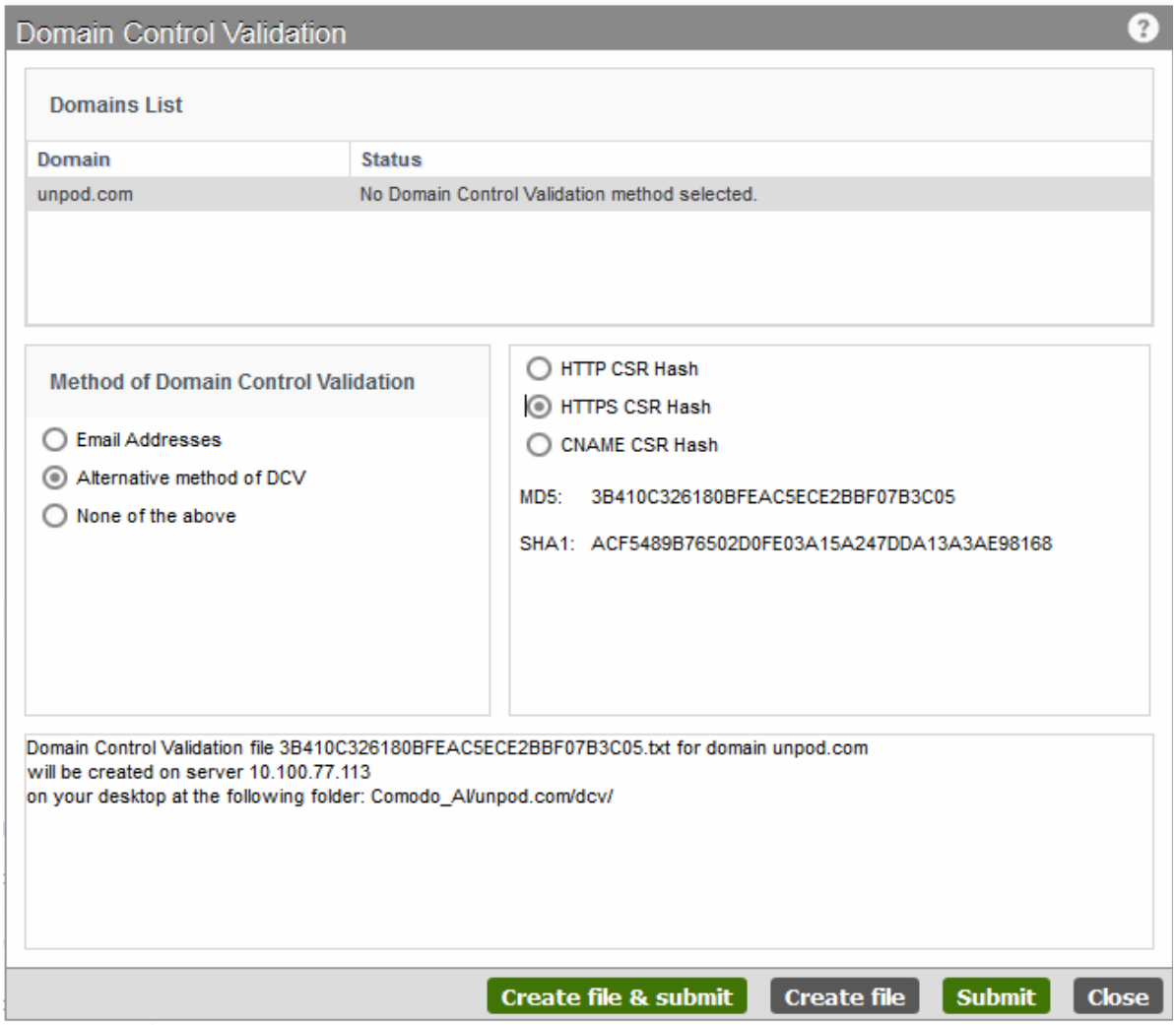
- Select an address at which you can receive mail and click 'Submit'. You will receive and email with a validation link and a unique validation code
- Click the link to follow the instruction on the web page
- Alternatively, copy the validation code and paste it into the field at the bottom of the interface
- Click 'Send' to submit the code for verification.

Validation by alternative methods of DCV

HTTP(S) CSR Hash

The HTTP(S) 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 SHA-256 hashes of your CSR. You can use the S3

DCV interface to automate the file creation, file upload and file checking processes:



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 and Submit'. This button will:
    ii. Generate the required DCV file
    iii. Place the file in the appropriate directory
    iv. Automatically run the DCV check

If you want to handle this process manually then there are more instructions at:
https://support.comodo.com/index.php?/Default/Knowledgebase/Article/View/791/10/

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

Format	**Location:** **http[s]://<**Authorization Domain Name**>/.**well-known**/**pki-validation**/<**MD5 hash**>**.txt **.txt file name:** <md5 hash>.text **.txt file contents:**

	SHA-256 hash comodoca.com Unique value Note – The 'Unique value' is optional and can be omitted if not supplied.
Example	http[s]://example.com/.well-known/pki-validation/C7FBC2039E400C8EF74129EC7DB1842C.txt Text file contents c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f comodoca.com 10af9db9tu

You can copy the MD5 and SHA-256 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: Authorization Domain Name 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:

<Authorization Domain Name**>/.**well-known**/**pki-validation**/<**MD5 hash**>**.txt

subdomain1.**<**Authorization Domain Name**>/.**well-known**/**pki-validation**/<**MD5 hash**>**.txt

<Authorization Domain Name 2**>/.**well-known**/**pki-validation**/<**MD5 hash**>**.txt

CNAME CSR Hash

The MD5 and SHA-256 hash values of your CSR are provided 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:

'_' <*MD5 hash***>.***Authorization Domain Name* **CNAME <***SHA-256 hash***>.[<***uniqueValue***>.]***comodoca.com*

Example :

A CSR is generated with the CN=www.example.com

The CSR is hashed using both the MD5 and SHA-256 hashing algorithms.

MD5: c7fbc2039e400c8ef74129ec7db1842c

SHA-256: c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

To perform DNS CNAME based DCV, the following DNS CNAME record may be created before submitting the order:

_c7fbc2039e400c8ef74129ec7db1842c.example.com CNAME

c9c863405fe7675a3988b97664ea6baf.442019e4e52fa335f406f7c5f26cf14f.comodoca.com

- 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.

Important note: Because of hex (base-16) encoded SHA-256 length, it should be split into two labels, each 32 characters long.

DNS record example 1 of use hex (base-16) encoding and splitting the SHA-256 hash into two labels:

_c7fbc2039e400c8ef74129ec7db1842c.example.com

CNAMEc9c863405fe7675a3988b97664ea6baf.442019e4e52fa335f406f7c5f26cf14f.comodoca.com

DNS record example 2 of use hex (base-16) encoding and splitting the SHA-256 hash into two labels and including a uniqueValue:

_c7fbc2039e400c8ef74129ec7db1842c.example.com.

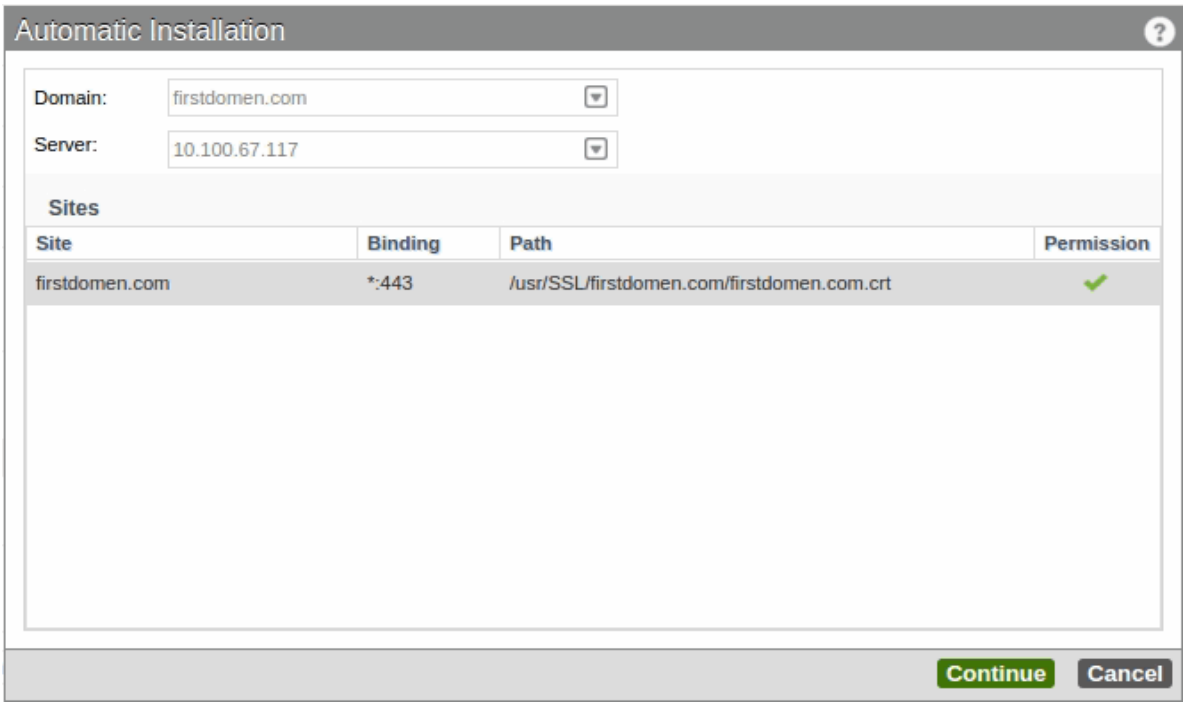
CNAMEc9c863405fe7675a3988b97664ea6baf.442019e4e52fa335f406f7c5f26cf14f.10af9db9tu.comodoca.com

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

10af9db9tu is the optional uniqueValue you can omit in case you are not supply it.

Step 5 - Install your Certificate

Note: The 'Autoinstall' action will remain available even after installation so you can re-install on different hosts as required.

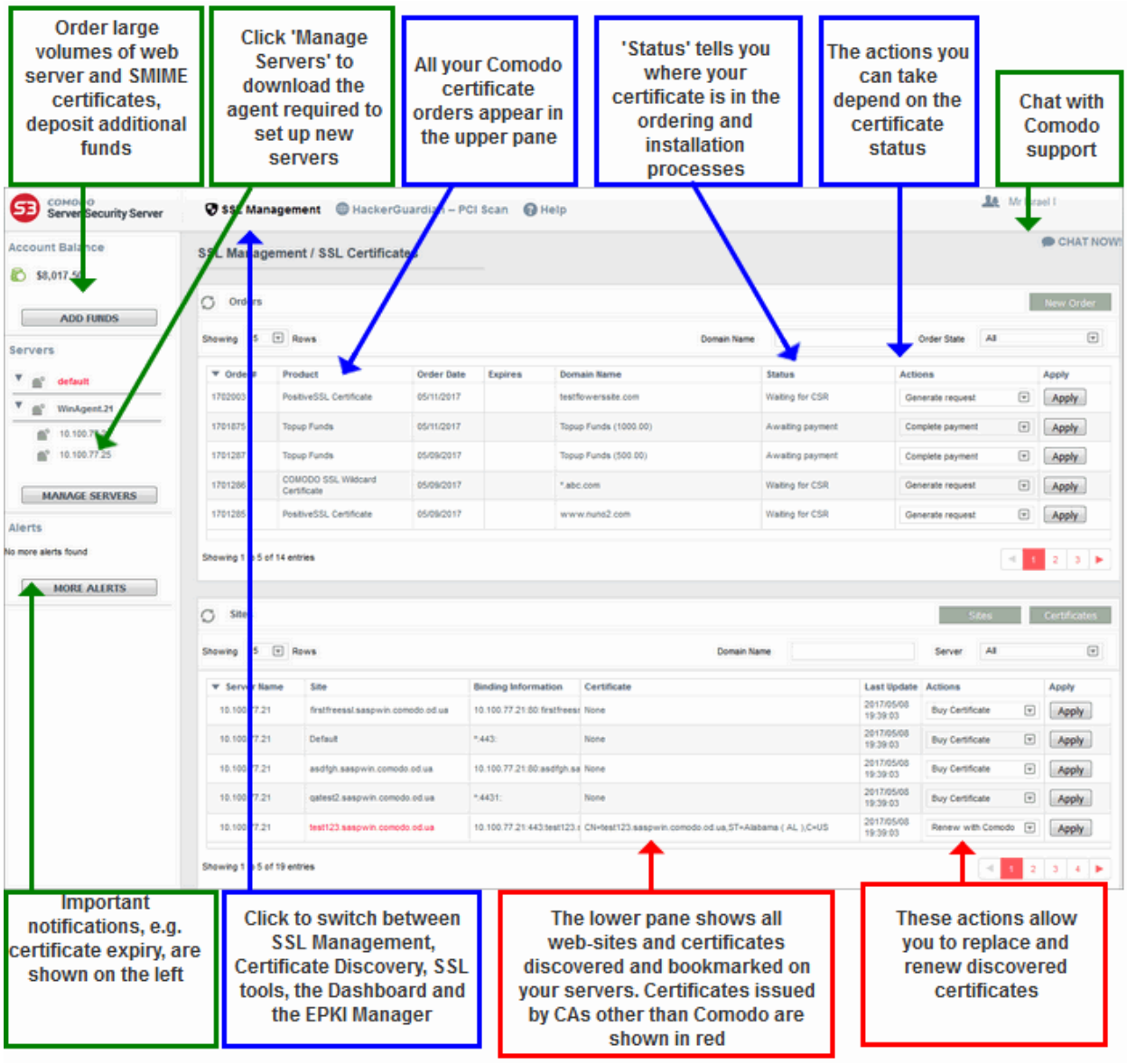


- Select a certificate with a status of 'Issued'
- Choose 'Autoinstall' from the 'Actions' drop-down and click 'Apply'
- This will open the installation configuration screen:

- Select the domain on which the certificate should be installed from the 'Domain' drop-down
- Select the target server from the 'Server' drop-down and click 'Continue'
- A confirmation message will be displayed when your certificate has been successfully installed
- Click 'OK' to close the dialog

Step 6 - Use S³ to Manage your Certificates

Comodo S³ allows you to manage the lifecycle of your certificates, run scans to discover certificates on your network, check whether a certificate is correctly installed and more.



- **Your orders -** All certificate orders associated with your account are listed in the top pane. Each certificate has a status and a corresponding set of actions which can be implemented on it. See **https://help.comodo.com/topic-437-1-843-10840-The-Main-Interface---Actions-and-Statuses.html** for more details.
- **Sites and Discovered Certificates** - All websites and certificates detected and imported from your servers are shown in the lower pane.

- **The Certificate Discovery Tool** - To scan for certificates outside your network, click the 'SSL Management' link then select 'SSL Certificate Discovery'. Internal search requires you to install and run the software agent. See **https://help.comodo.com/topic-437-1-843-11189-SSL-Certificate-Discovery-Tool.html** for more details.
- **Generating a CSR** - If your certificate order has a status of 'Waiting for CSR' then select 'Generate Request' and click the 'Apply' button. See **https://help.comodo.com/topic-437-1-843-10849-Generate-a-CSR.html** to find out more.
- **Renewing a certificate** – Use one of the following methods to renew a certificate:
  - To renew one of your Comodo certificate orders, use the 'Renew Certificate' option in the 'Actions' drop-down'
  - To renew a discovered certificate, locate the certificate in the 'Sites' list and select the 'Renew with Comodo' action from the drop-down. Alternatively, click the 'Certificates' button, locate the certificate in question and click the 'Renew' button:
  - See **https://help.comodo.com/topic-437-1-843-10846-Renewing-a-Certificate.html** for more details.
- **Buying a certificate** – To buy certificate(s) for any domain detected on your servers, locate the certificate in the 'Sites' list and select 'Buy Certificate' action from the drop-down. See **https://help.comodo.com/topic-437-1-843-10847-Buying-a-Certificate.html** to find out more.
- **Completing Payment** – If your certificate has a status of 'Awaiting payment' then click 'Complete payment' from the drop-down. See **https://help.comodo.com/topic-437-1-843-10848-Completing-your-Order.html** for more details.
- **The SSL Analyzer** – To find out if your certificate is installed correctly, or to diagnose web server problems, click the 'SSL Management' link then select 'SSL Tools'.
  - Select 'Basic SSL Check' for basic certificate information
  - Select 'Advanced SSL Check' for in-depth analysis about web-server configuration
  - See **https://help.comodo.com/topic-437-1-843-11190-SSL-Tools.html** to find out more.
- **Chat with Support** – To get a sales assistance or tech support, click the 'Chat Now!' link at the right top of the interface
- **The SSL Dashboard** – Click 'SSL Management' then 'Dashboards' to view a graphical overview of your certificate orders and certificates imported from your network. See **https://help.comodo.com/topic-437-1-843-11340-S³-Dashboards.html** for more details.
- **EPKI Manager** – Allows Comodo EPKI users to view their balance, view their certificate buy prices and deposit additional funds. See **https://help.comodo.com/topic-437-1-843-11490-EPKI-Manager.html** for more details.
- **Alert Settings** – Configure how many days before expiry you wish to be notified about a certificate. You can receive alerts in the web interface and via email.
- **Support** – To view or download the online user guide, click 'Help' link then select 'Help'. See **https://help.comodo.com/topic-437-1-843-11191-About-S³-and-Support-Details.html** for more details.

About Comodo

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