COMODO
Creating Trust Online®

Comodo Server Security Server

Software Version 2.4

Administrator Guide

Guide Version 2.4.041718

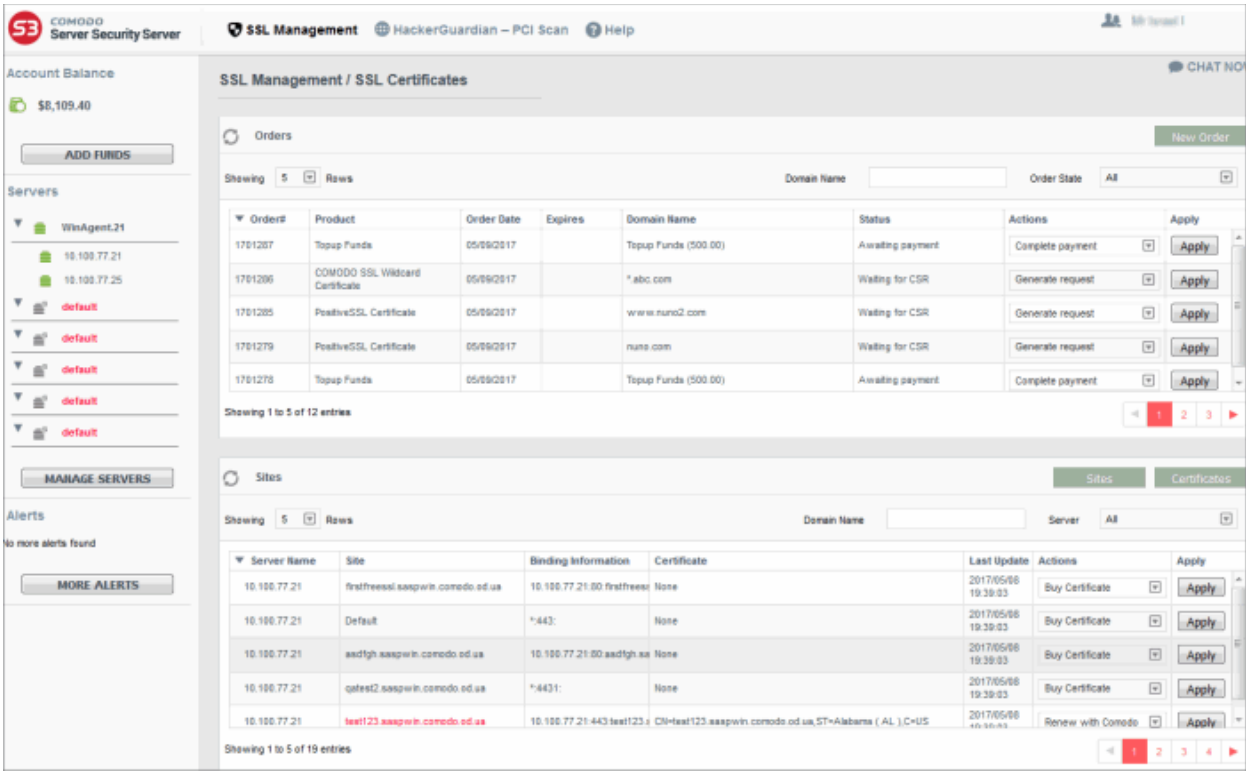
Comodo Security Solutions
1255 Broad Street
Clifton, NJ 07013

Table of Contents

1. Introduction to S³

Overview

Comodo Server Security Server (S³) allows customers to manage the purchase, installation and lifecycle of SSL certificates on IIS and Apache web-servers. Customers can also run scans to discover and import all existing certificates in their network and can use the SSL checker tool to identify whether a certificate is correctly configured. EPKI manager users can purchase certificates via S3 using their account funds.



Key features:

- Automatically install new certificates on IIS and Apache web-servers
- Easily purchase new certificates using in-app ordering
- Quickly create and submit certificate signing requests
- Use the SSL discovery tool to create an inventory of all certificates on your network
- Use the SSL checker to diagnose certificate installation problems
- Receive alerts when any certificate is close to expiry for easy renewal
- Use built-in wizards to complete Domain Control Validation (DCV)
- Offline mode allows customers to manage certificates without installing an agent
- Dashboard charts provide a graphical heads-up on your entire certificate inventory
- EPKI users can purchase using account funds and can deposit additional funds

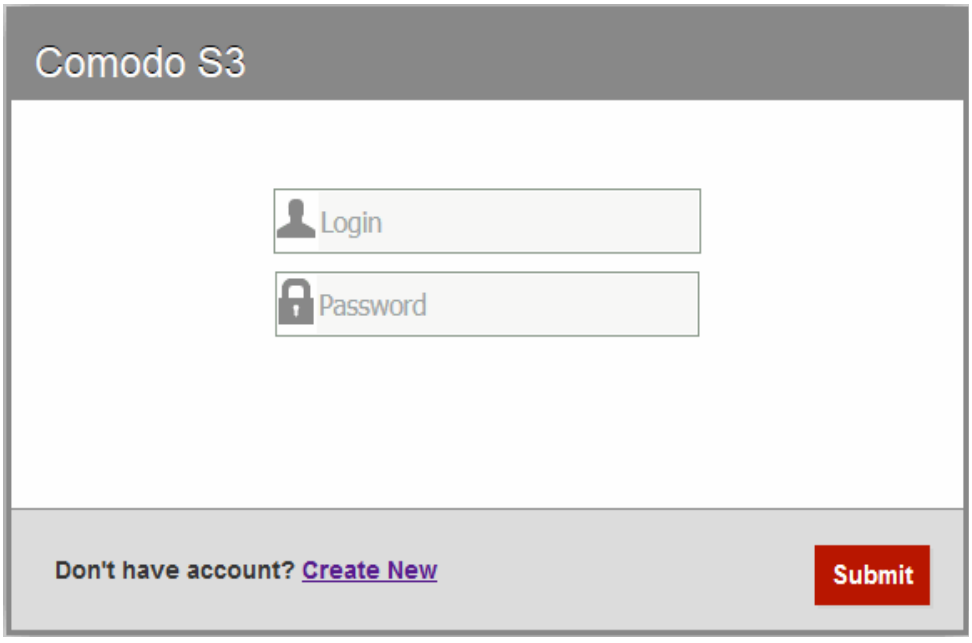
Guide structure

- **Introduction to S³**

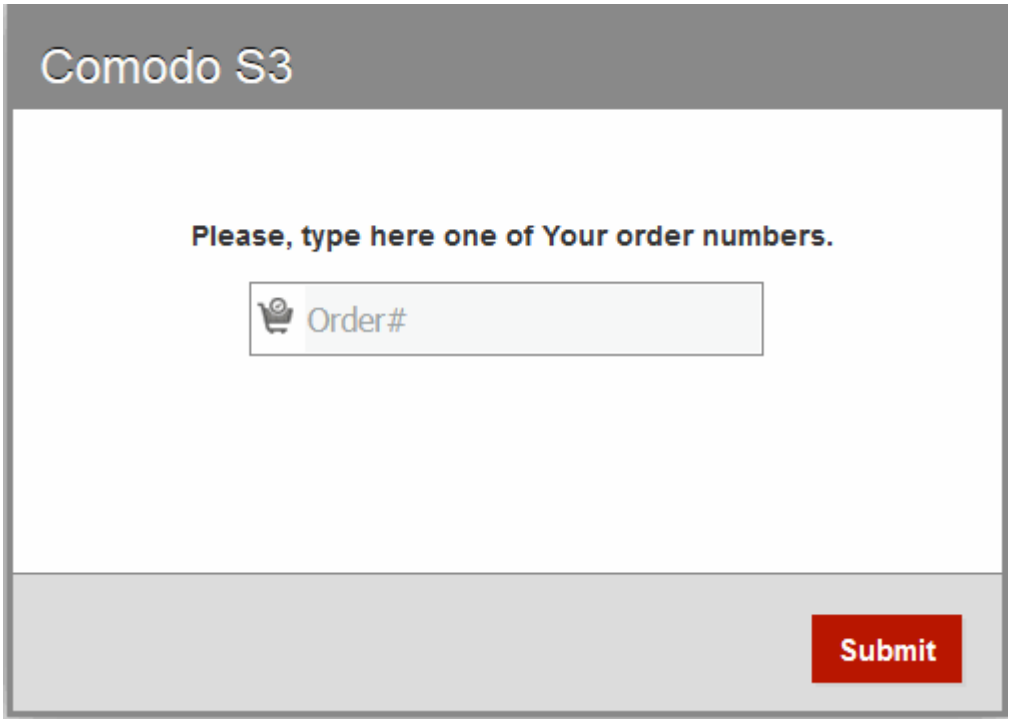
1.1. Login into the Console

To access the S³ interface, please login at **https://s3.comodo.com**

- If you are an existing Comodo user, please enter your Comodo account username and password followed by one of your product order numbers:



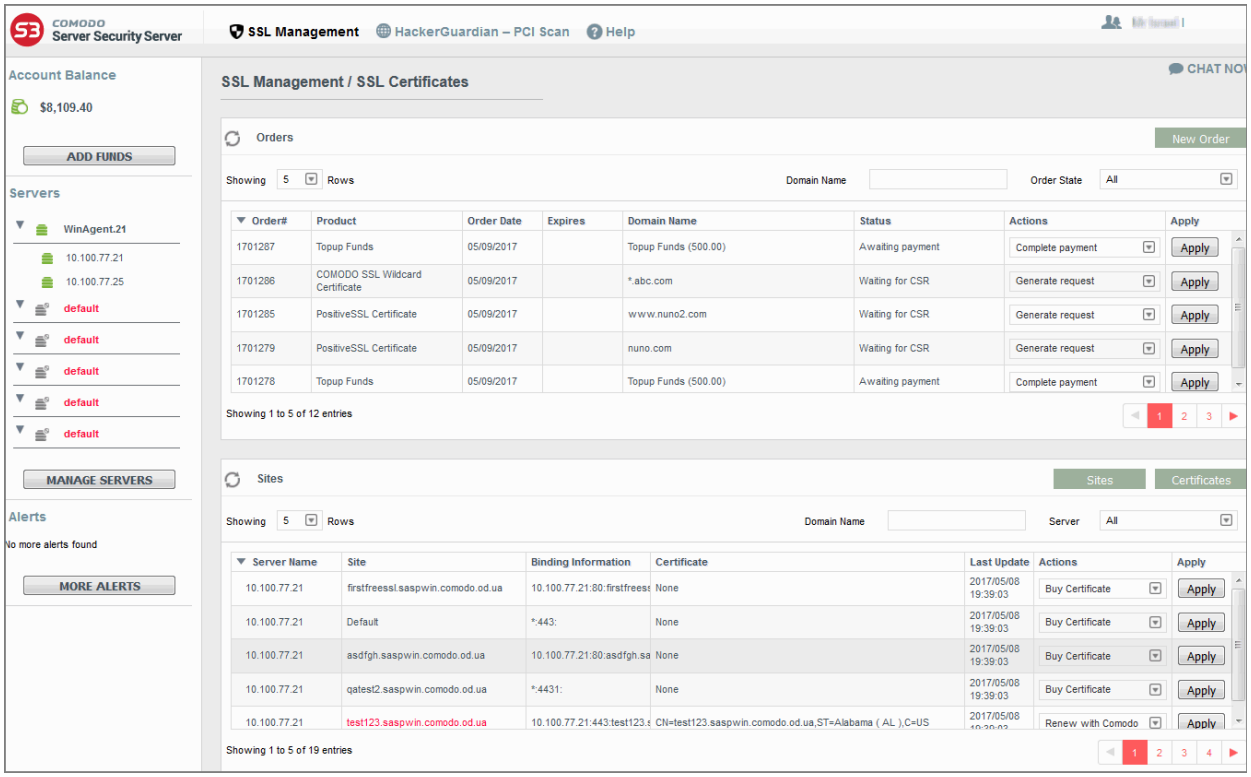
- Your username and password are case sensitive. Please make sure 'Caps Lock' is off.



- If you are logging into S³ for the first time, please read and accept the 'End User License Agreement':

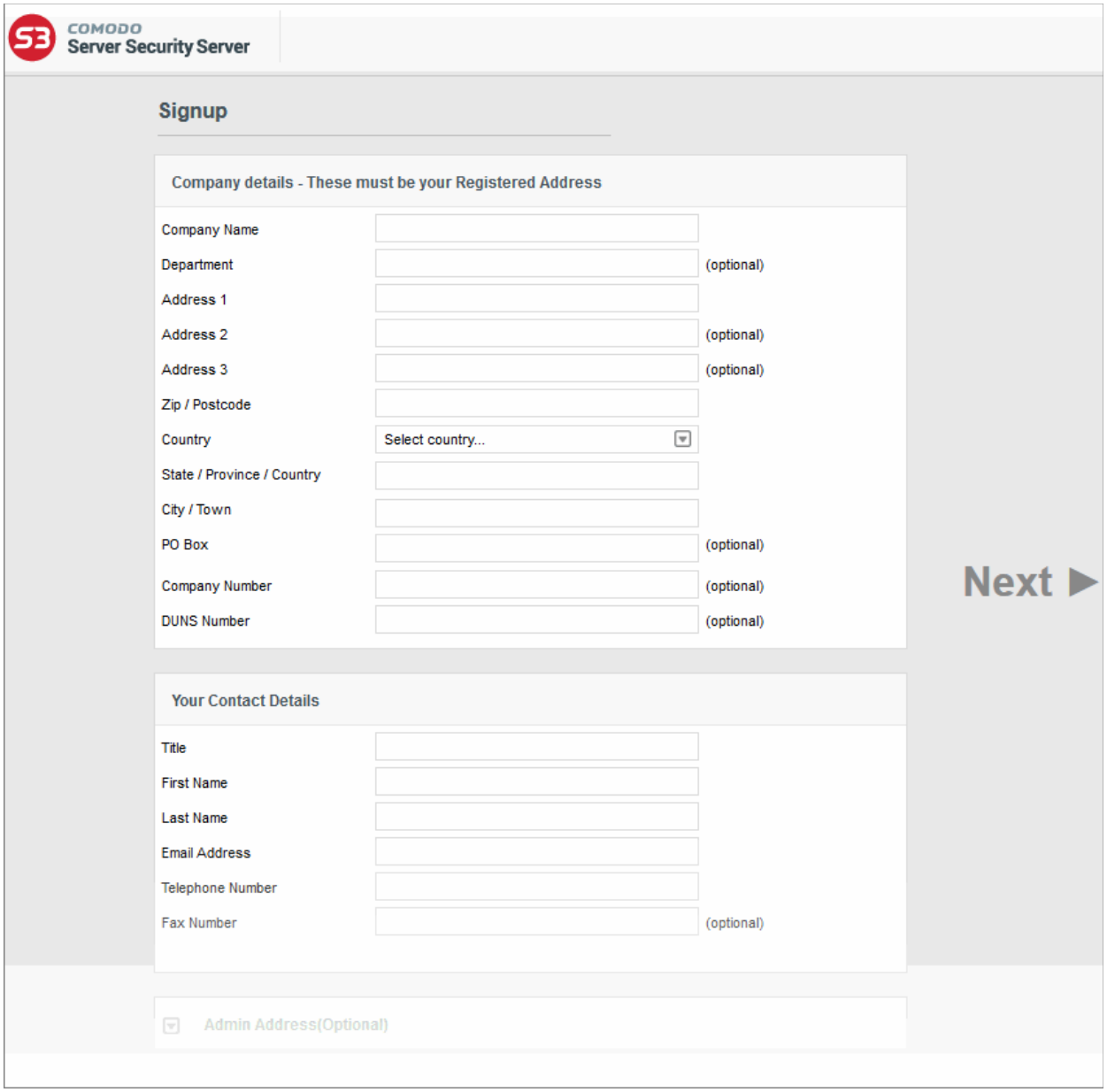
- If you see a message stating your login credentials have expired, please follow the link in the message to update them.

- After your credentials have been verified, you will be logged into the S[3] console:

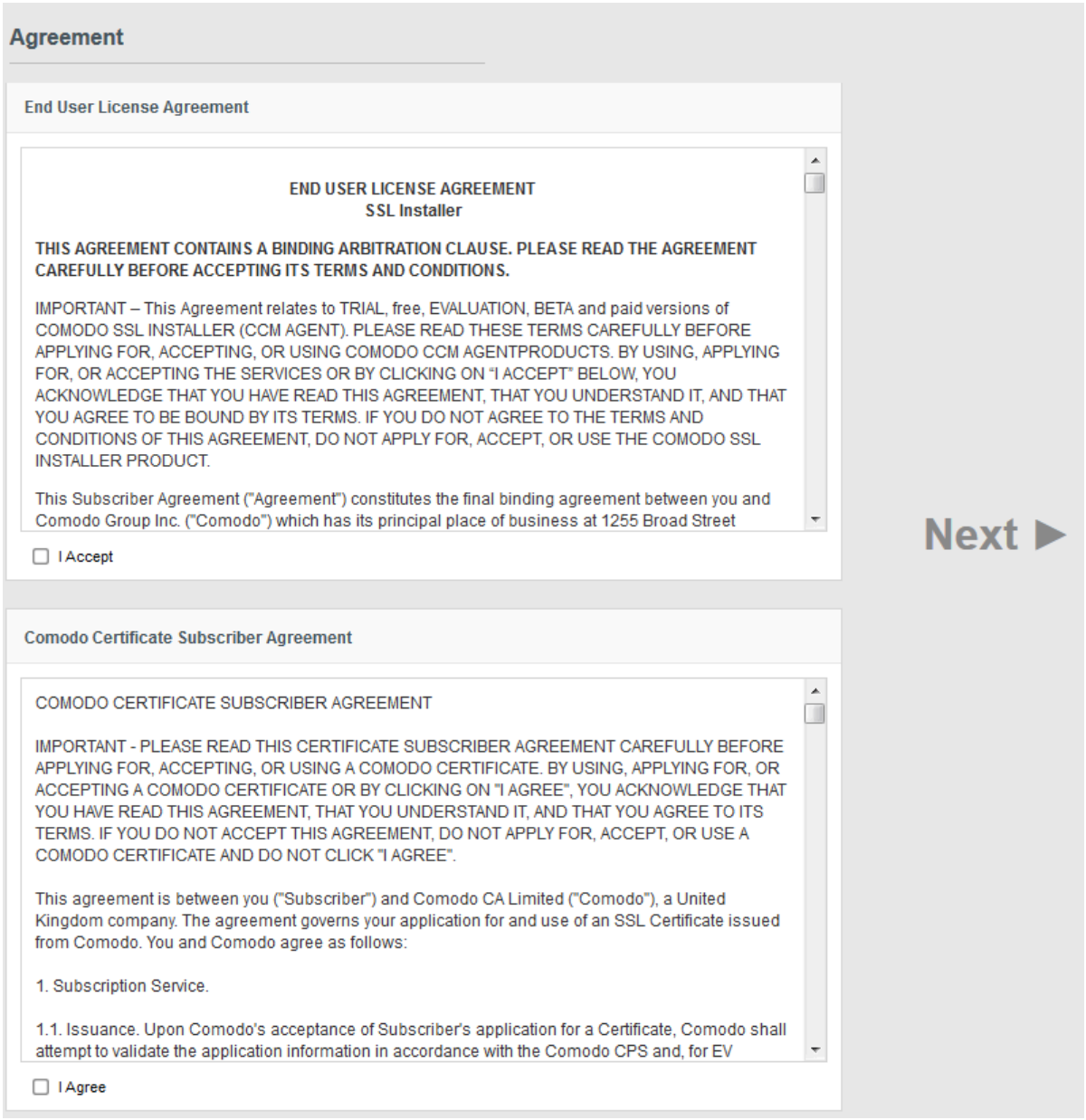


New users

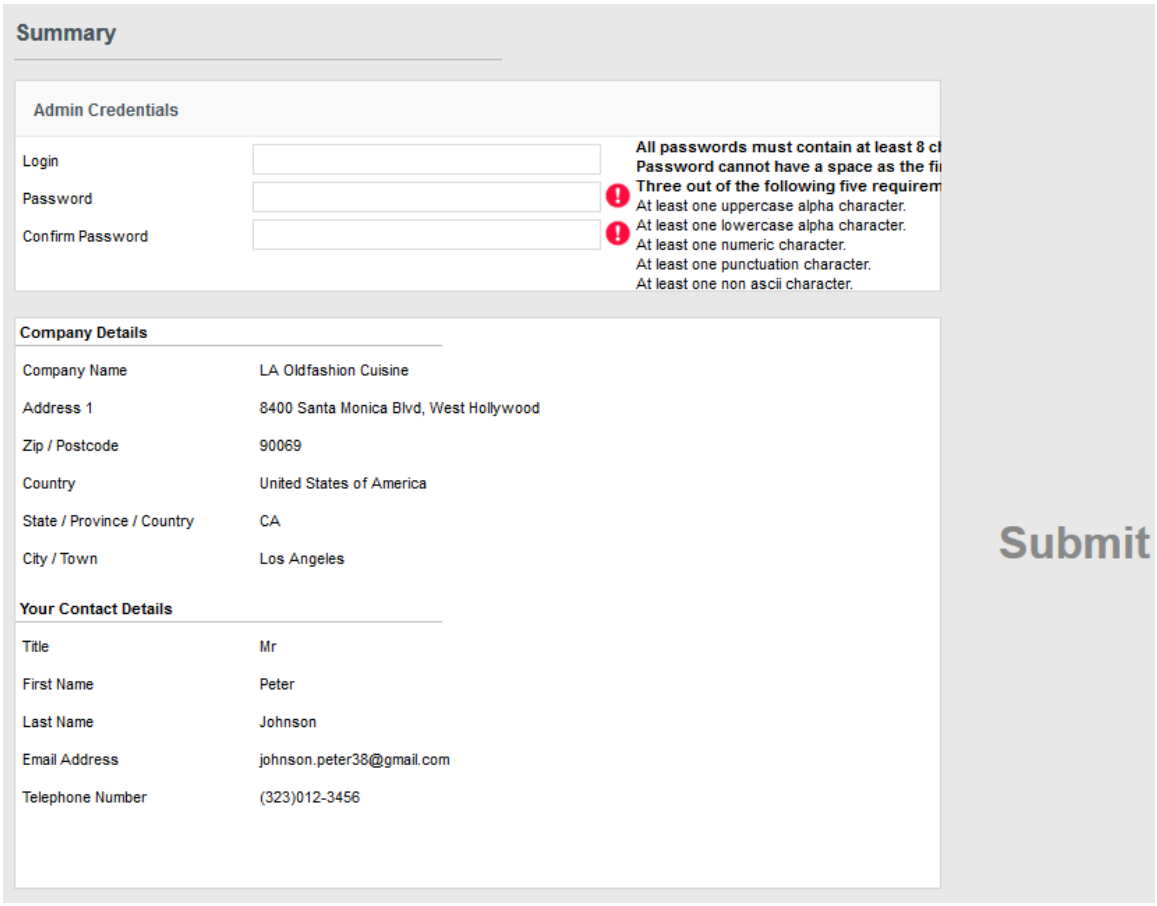
If you do not have a Comodo account, click 'Don't have account? Create New'. You will be taken to the account creation page:



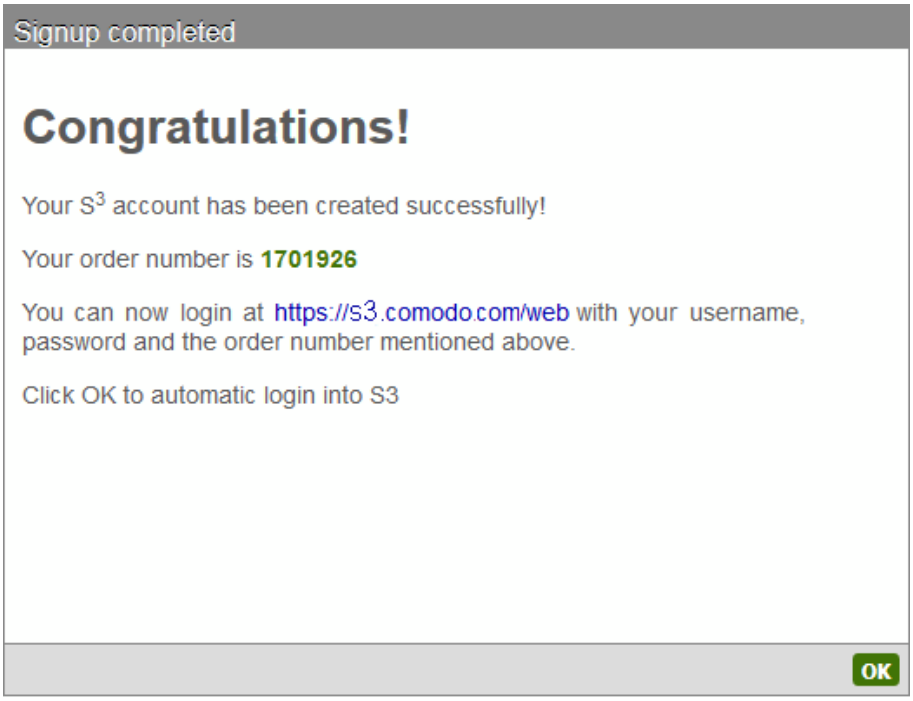
- Please complete all mandatory fields then click 'Next' to proceed.
- Next, please agree to the EULA and subscriber agreements:



- Click 'Next' to continue.
- Please review your account details on the summary screen. Click 'Back' if you wish to update any items:



- Create a username and password to finalize your enrollment then click 'Submit':
- You will see the following confirmation message once your account is created.



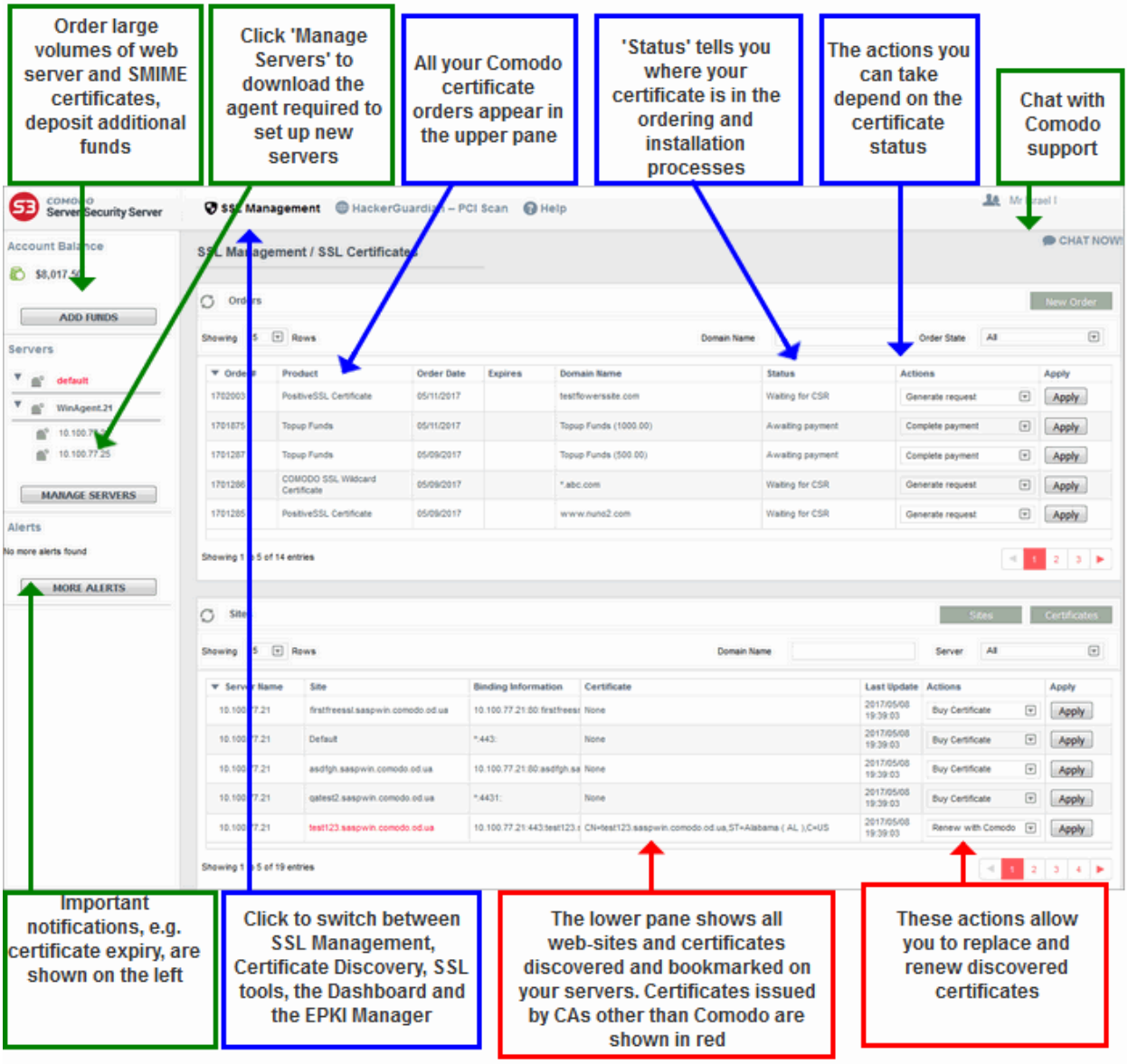
- **Important** – Please make a note of the order number shown in the confirmation screen. You will need it to login on future occasions:
- Click 'OK' to automatically login to S^3.
- You can login at **https://s3.comodo.com/web** in future.

Next, see **The Main Interface / Actions and Statuses**.

2. The Main Interface / Actions and Statuses

The 'SSL Management' interface allows to you view a list of all certificates associated with your account and a list of all sites and certificates detected on your server. You can use the interface to generate and submit a certificate signing request (CSR), complete domain control validation, install certificates, buy/renew certificates and more.

- All certificate orders associated with your account are listed in the top pane
- Click 'Manage Servers' to begin adding servers for auto-installation and certificate discovery
- All websites and certificates detected and imported from your servers are shown in the lower pane
- Click the 'SSL Management' link then select 'SSL Certificate Discovery' to scan for SSL certificates inside or outside your network (internal search requires software agent to be installed and run)
- Click the 'SSL Management' link then select 'SSL Tools' to open the SSL checker. This helps to identify whether a certificate on a domain is installed correctly and whether your web server is configured correctly
- Click 'SSL Management' them select 'Dashboards' to see a graphical overview of all certificates purchased under your account
- EPKI users should click 'SSL Management' then 'EPKI Manager' to view their fund balance, view buy prices and to add funds to their account.
- The 'Help' menu on the top navigation allows you to view product version and the online help guide
- You can chat with Comodo support by clicking the 'Chat Now' link at top-right
- Important S^3 notifications are shown on the left. (e.g. alerts on expiring certificates). Click 'More Alerts' > 'Alert Settings' to change alert settings. You can choose how many days before certificate expiry you want notifications to begin. You can also activate email notifications.



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

Certificate Status	Available Actions
Awaiting Payment Your order has been placed with Comodo, but payment has not yet been received. Please complete payment for order processing to continue.	Complete Payment
Waiting for CSR 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.	Generate request Request Invoice
Processing CSR has been submitted and received. Comodo CA is now processing the order and validating the application. Note – you must next complete Domain Control	Domain Control Validation Replace CSR

Certificate Status	Available Actions
Validation (DCV) before your certificate can be issued. ***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.	Request Invoice
Issued 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.	Auto-install certificate Save Certificate Renew Certificate Installation Check Request Invoice
Installed Certificate has been successfully installed.	Auto-install certificate Save Certificate Renew Certificate Request Invoice
Paid Only relevant to EPKI users. Indicates that funds have been successfully added to your account.	N/A

Available Actions:

Generate Request

- Starts a wizard that will help you create and submit a CSR 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

- Installs the certificate to the domain listed in the 'Domain Name' column

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.

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.

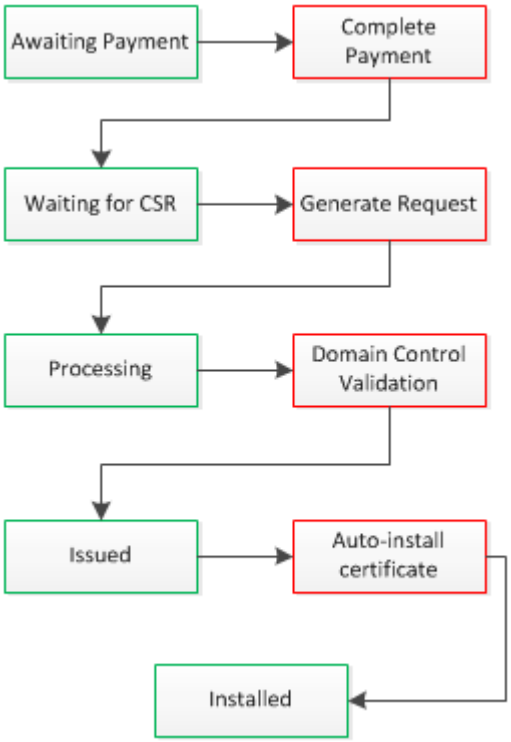
Save Certificate

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

Request Invoice

- Allows you to submit an invoice request to Comodo for the selected certificate. The invoice will be sent to your default email address and any other addresses that you add.

The following diagram illustrates the relationship between statuses and available actions:

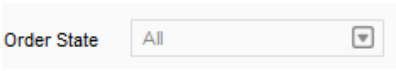


For clarification, the 'Auto-install certificate' option is always available after issuance so you can, for example, re-use the utility to install the same certificate on a different host. The 'Renew Certificate' option will appear when certificates with a status of 'Issued', 'Installed' are approaching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

The interface also contains the following items related to certificates:

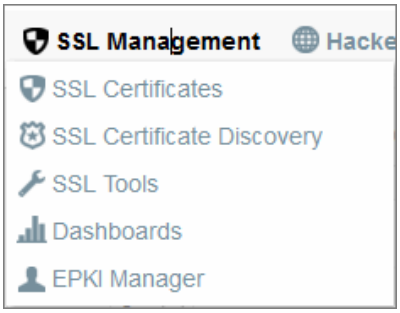
Refreshes the list of certificate orders or sites.

Starts the purchase process for a new Comodo certificate. This is covered in Buying a Certificate.



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

Allows you to speak directly to a Comodo support operative.



Switch between the SSL management screen (default), the certificate discovery interface, the SSL tools area, the dashboard and the EPKI Manager page.

3. Tutorial

This tutorial takes you through the processes of adding servers to S³ then the certificate ordering and installation processes. Please use the following links to go straight to the section that you need help with:

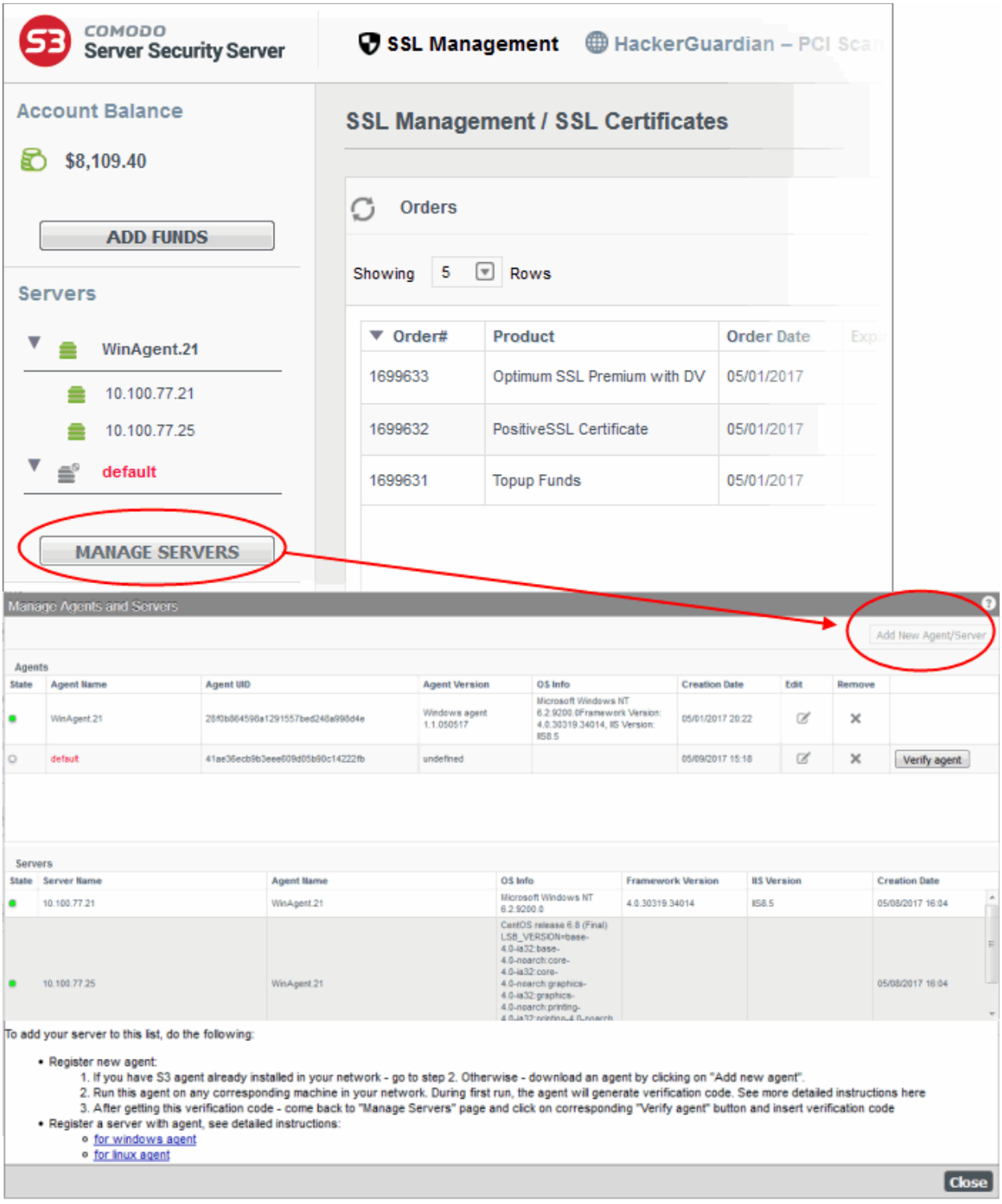
- **Adding your Servers**
- **Generate and Submit a CSR**
- **Complete Domain Control Validation**
- **Install or Save Issued Certificate**

3.1. Add your Servers

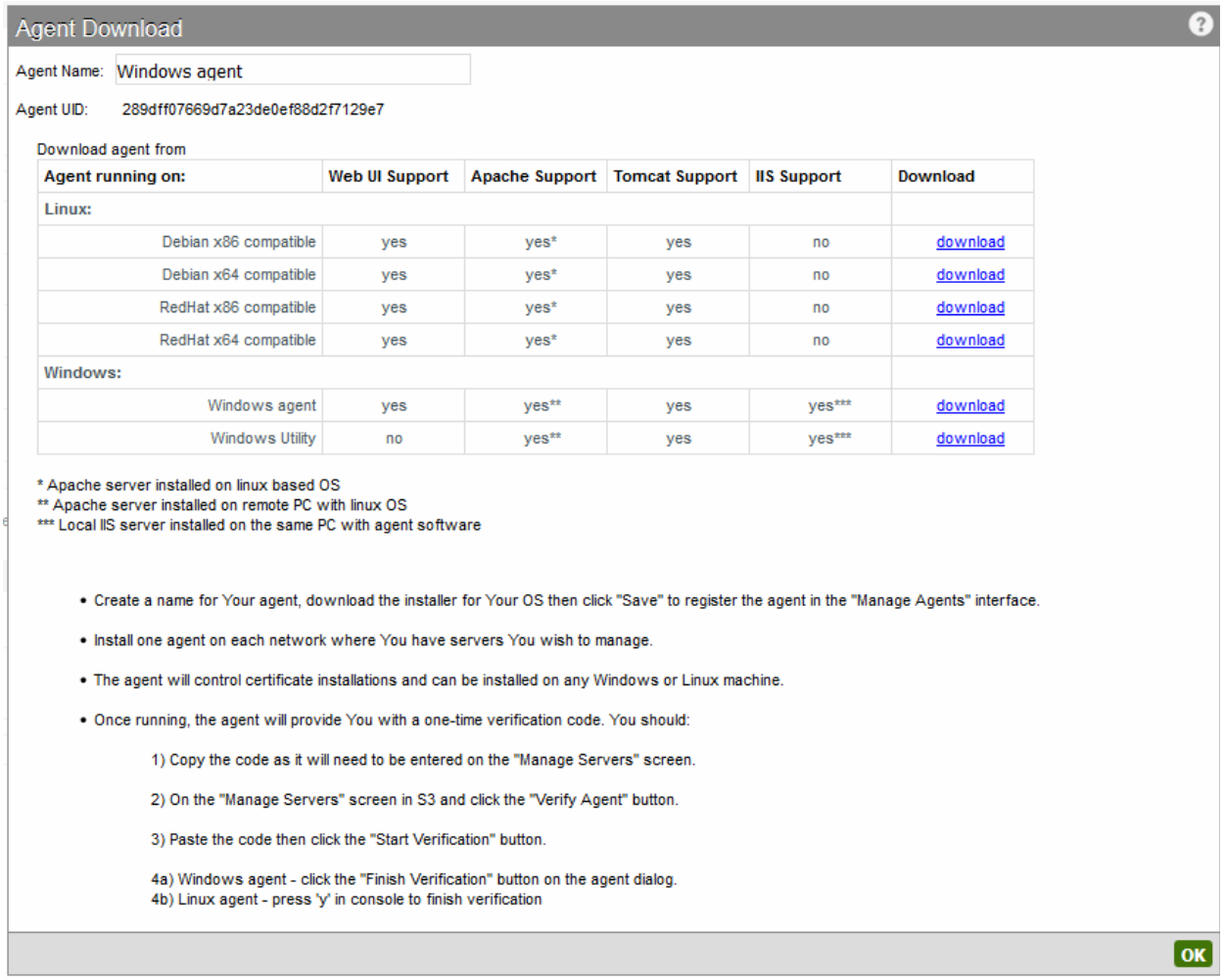
In order to establish communications between S³ and your servers, you first need to install the S³ agent on a Linux or Windows machine on your network. This machine will handle communications between the S³ web console and your web-servers. After installing the agent, you will be able to add multiple servers. After adding your servers, you will be able to run certificate discovery scans on them and will be able to track, manage and install certificates on them.

To add agents:

- Click the 'Manage Servers' button then 'Add New Agent/Server' button:



- This will open the agent download screen.
- Type a name to identify the agent in the 'Agent Name' field
- Select a 'Linux' or 'Windows' agent download link depending on the OS of the machine on which you are going to install the agent



Click the appropriate 'download' link to open a .zip file containing the agent setup files. Extract all files to the user's home directory on the machine you wish to use to run the agent. For example:

Linux – `/home/user/Agent`

Windows – `C:\Users\username\Agent`

- Click 'OK' to register the agent in the 'Manage Agents' interface. You can edit or download other versions of the agent at any time.

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

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

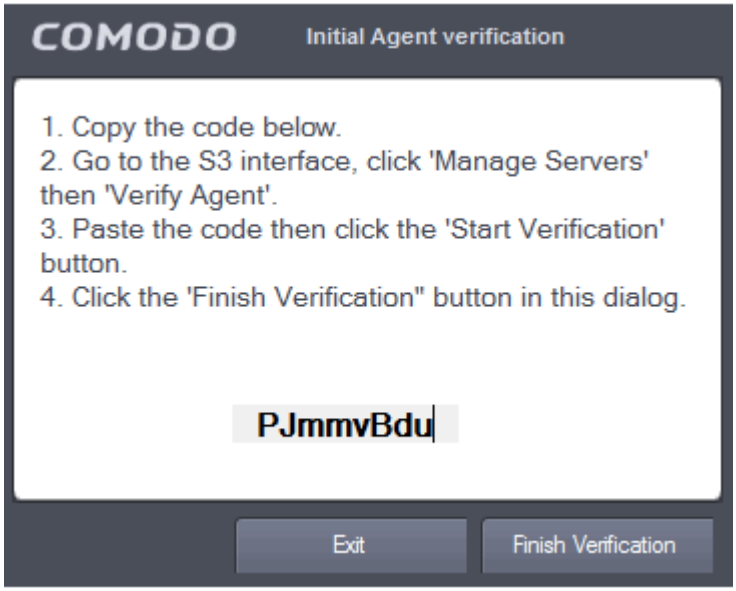
Managing agents and servers

Install the agent on a Windows machine

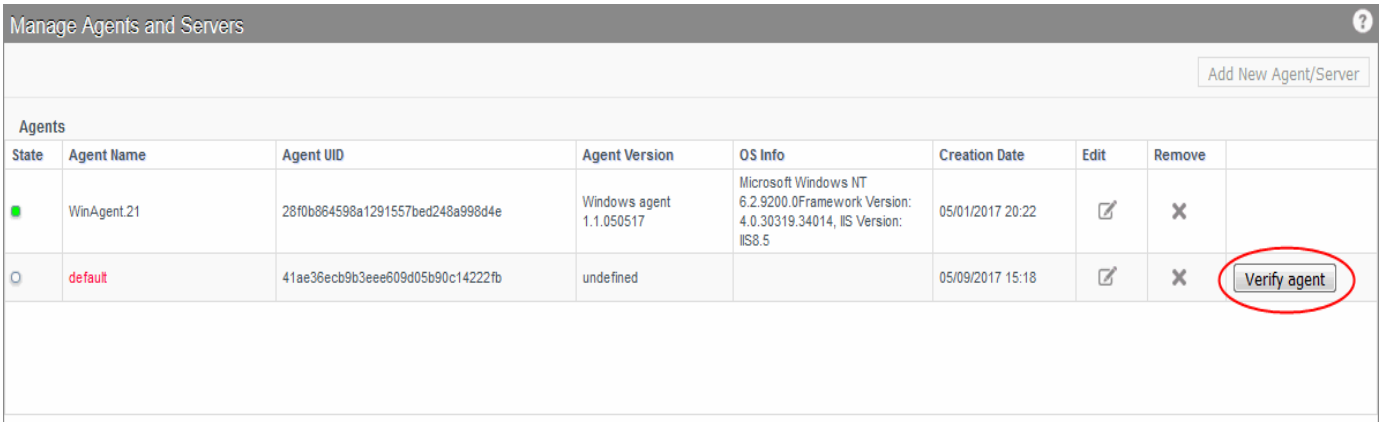
Note: Please ensure you have admin privileges to run the application.

- Extract the contents of the zip file to the Windows machine you wish to use to control your servers

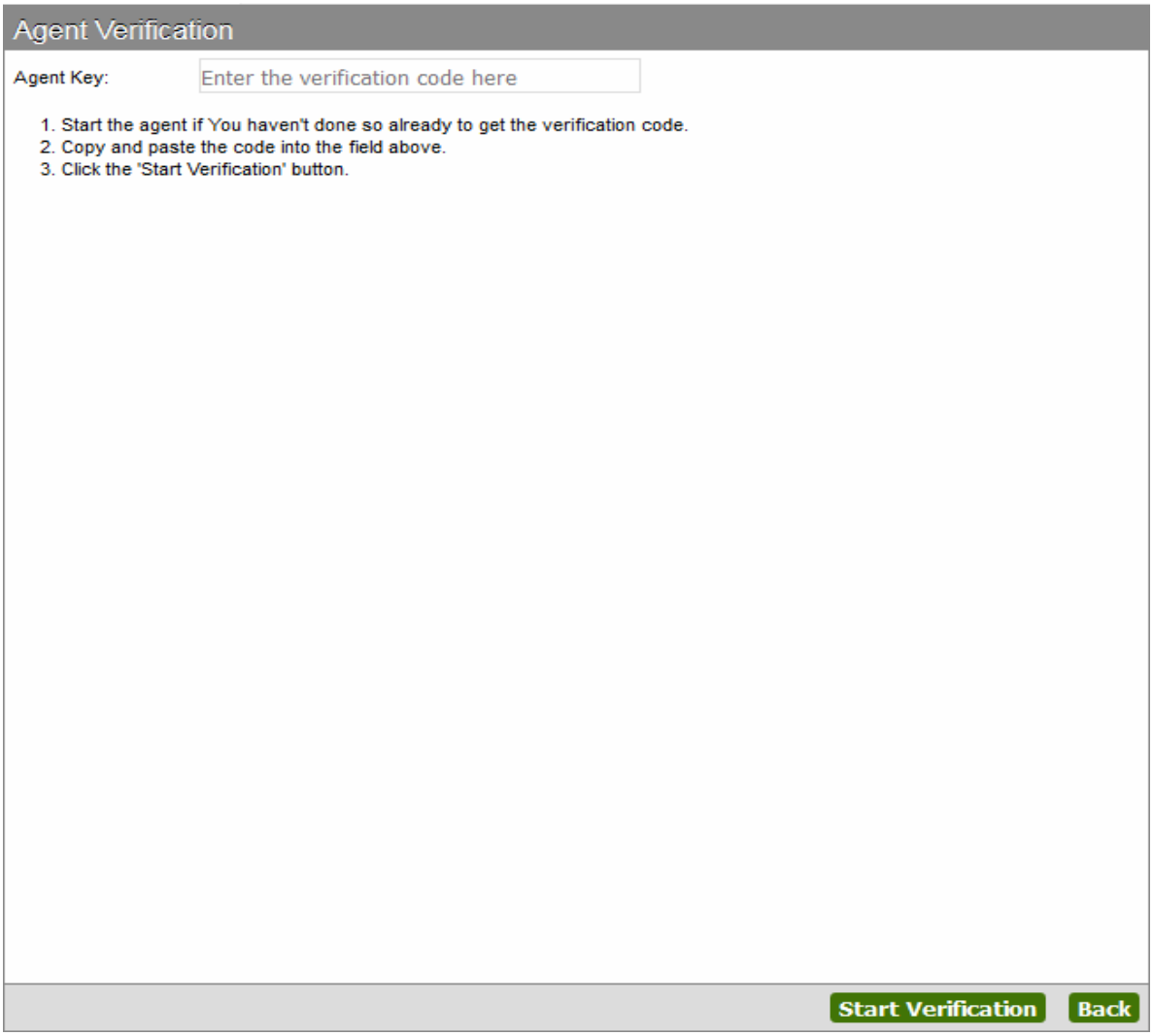
- Open 'ComodoS3Agent.exe' to start the installation process.



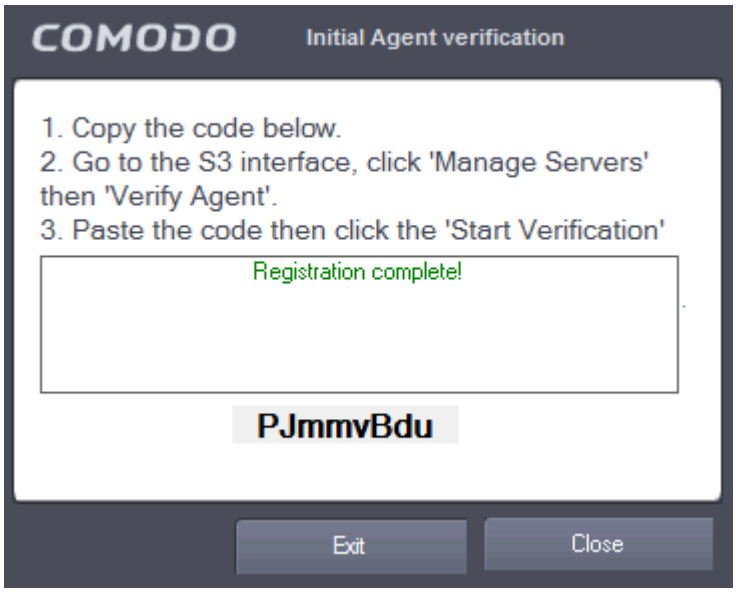
- To synchronize the agent with S³:
  - Copy the unique code from the 'Initial Agent verification' dialog
  - Login to the S³ web interface and click the 'Manage Servers' button
  - Locate the agent you have just installed and click the 'Verify agent' button:



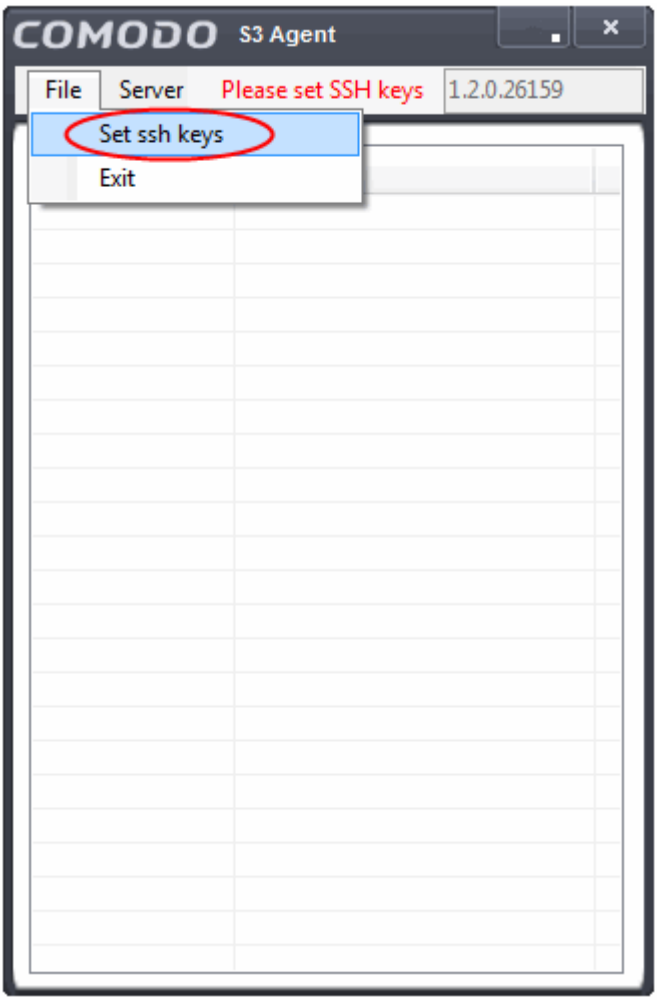
  - Paste the verification code into the 'Agent Key' text box then click the 'Start Verification' button:



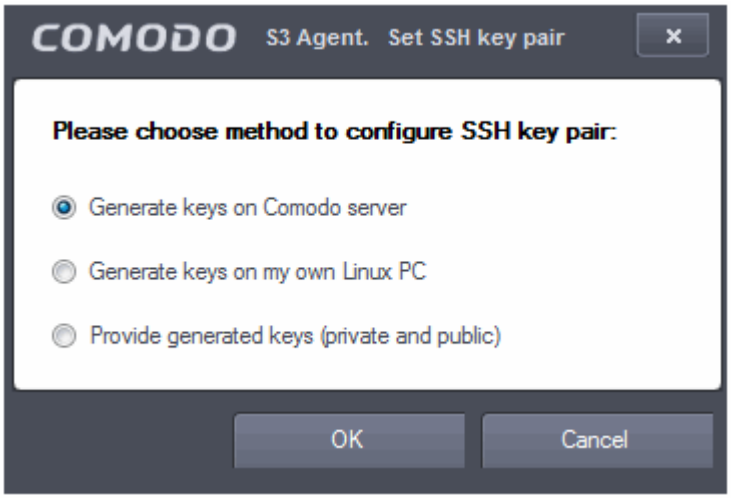
- Next, go back to the agent verification dialog on your Windows machine and click 'Finish Verification'. The verification dialog will confirm whether your registration was successful:



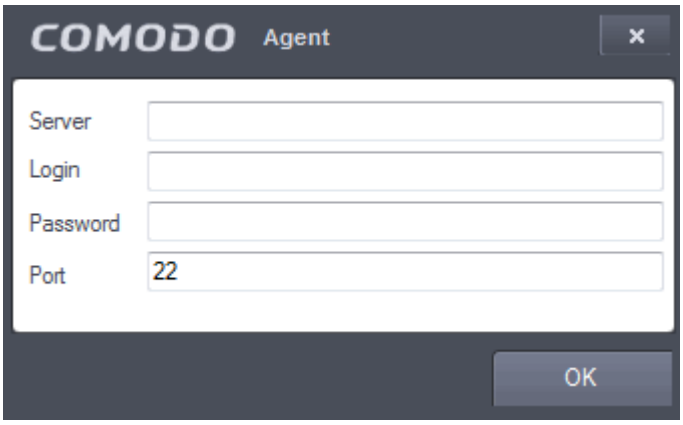
- Click 'Close'. The S³ Agent dialog will open
- Select 'Set ssh keys' from the 'File' menu or choose 'Please set SSH keys'



You can configure the SSH key pair in three ways:

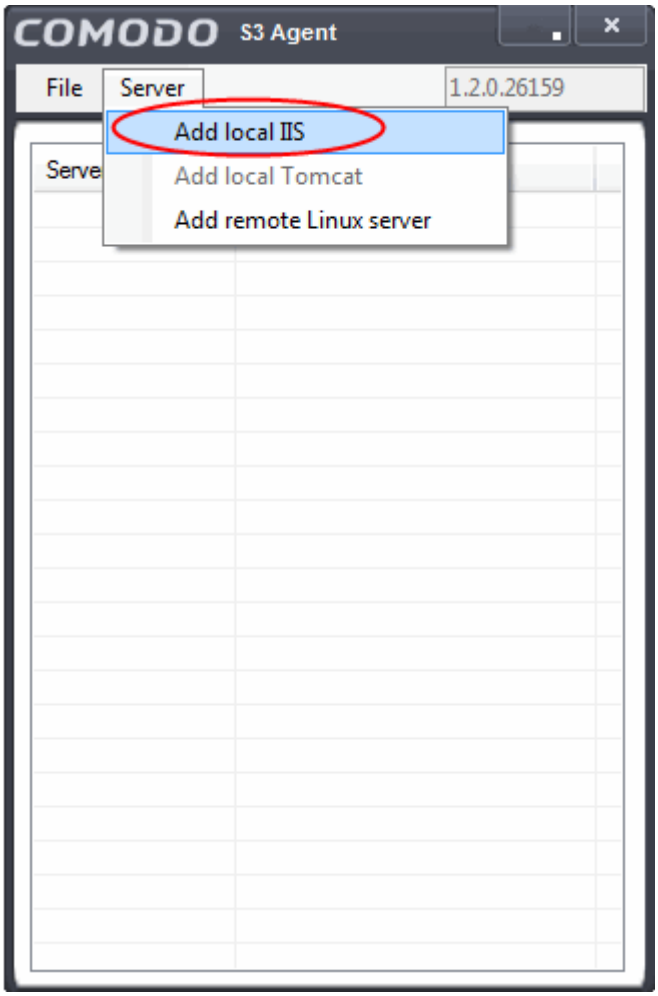


- Generate keys on Comodo server – Automatically generate the SSH key pair on Comodo's servers
- Generate keys on my own Linux PC – Generate keys by entering Linux credentials (server address, login, password and port):



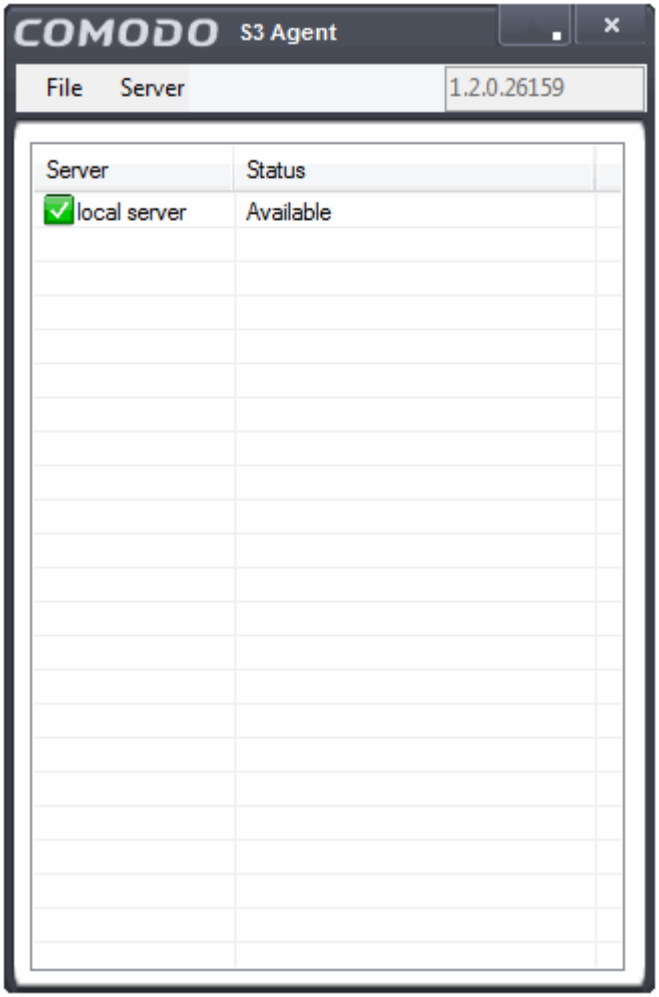
- Provide generated keys (private and public) - Select your SSH keys from file saved on your local computer

- 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



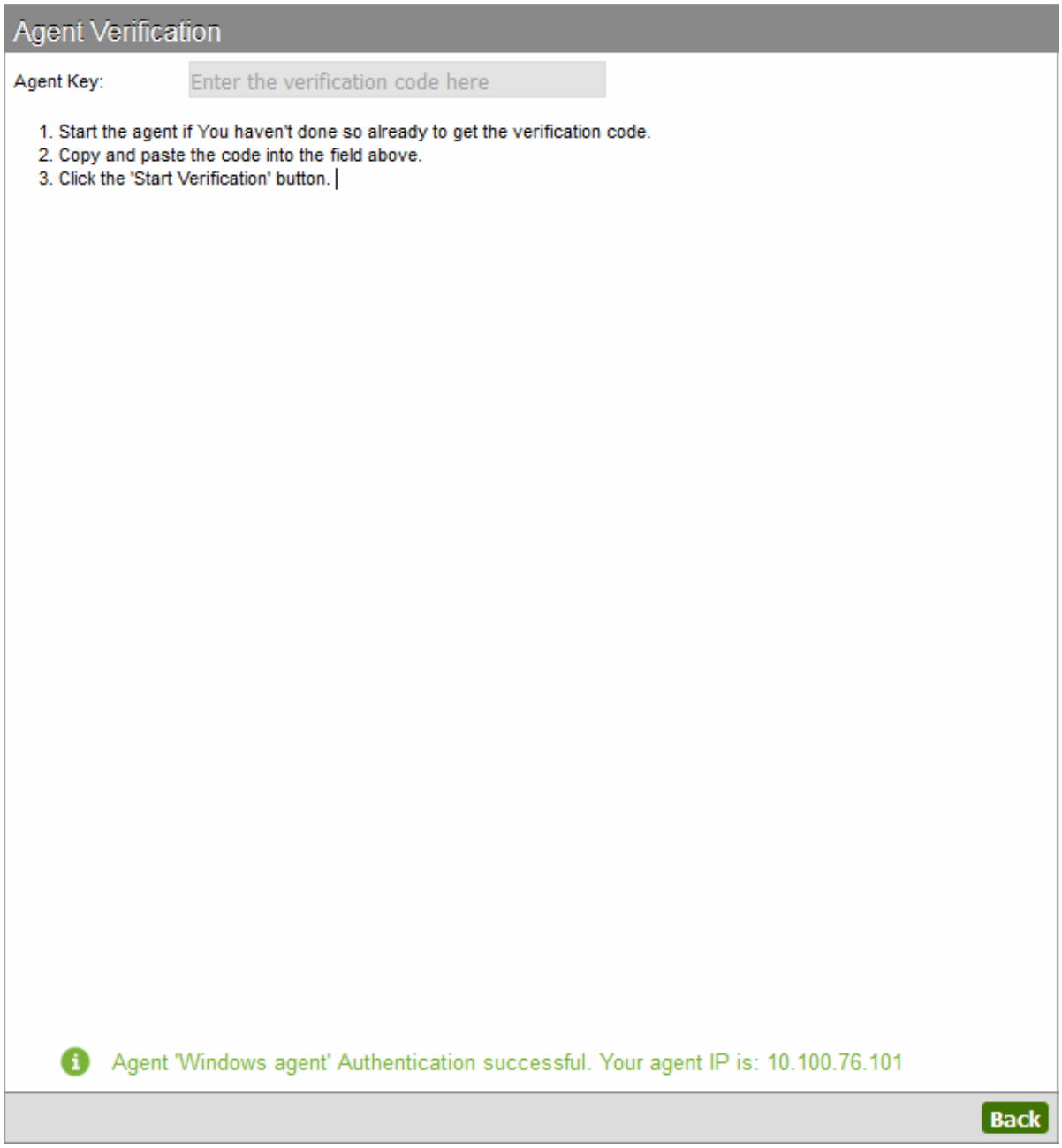
- 'Add Remote Linux server' opens the 'Add Linux server' dialog to provide SSH Key-Based Authentication on a Linux server (server address, login, password and port). This allows the agent to connect to the server for authentication

- 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

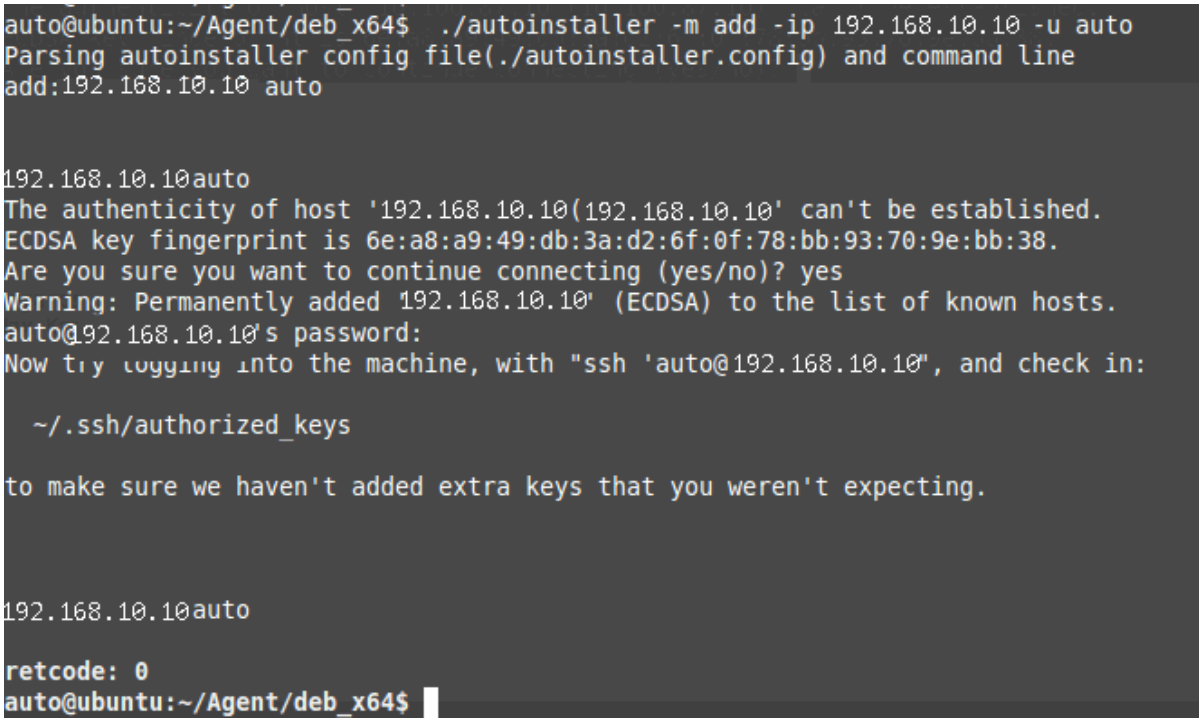


- After the file is verified, you can add servers by entering the following line at the command line interface:

  ./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.

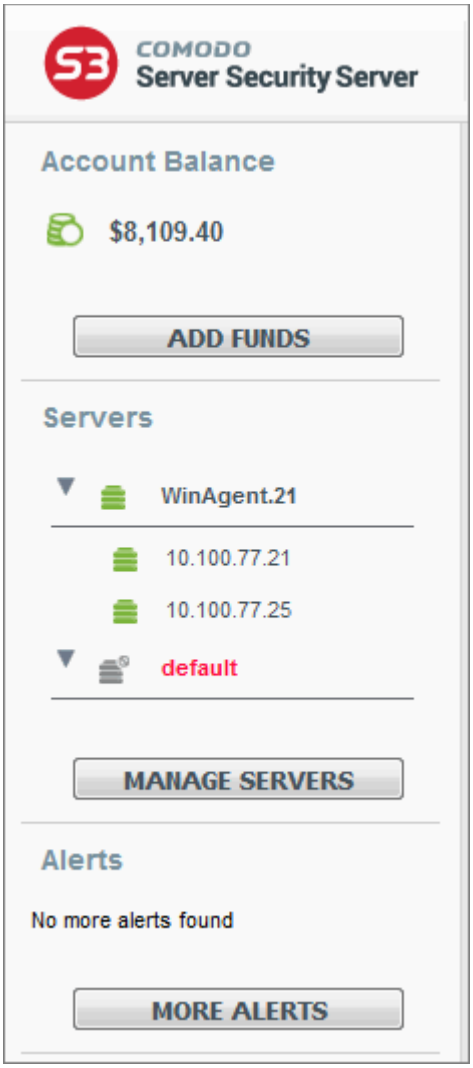


Note: Your agent must be activated before adding the server

- 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:



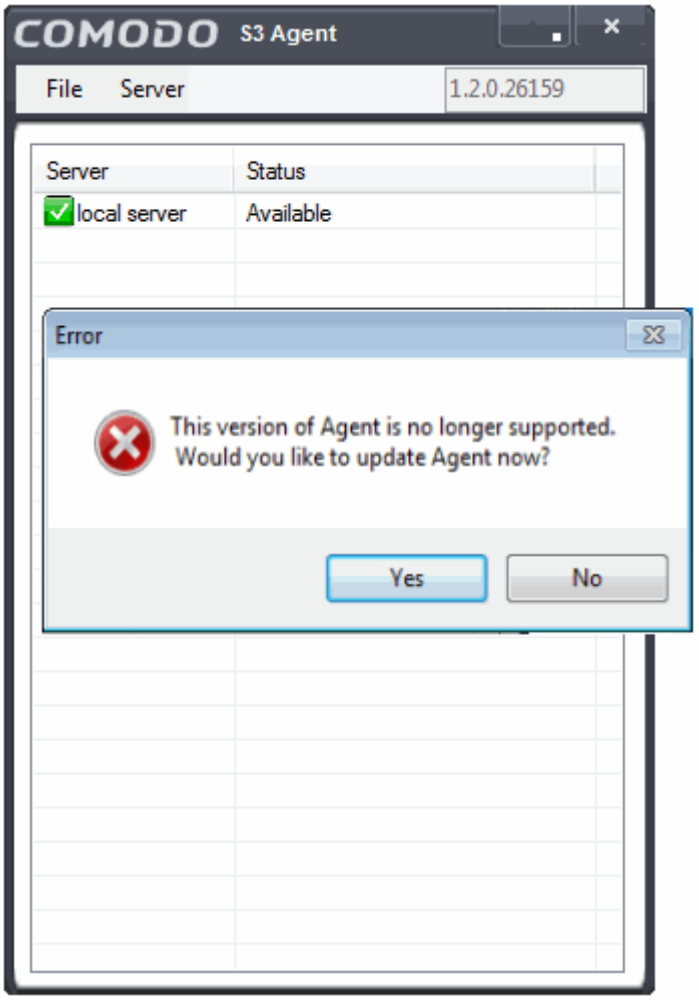
Server statuses:

- 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**

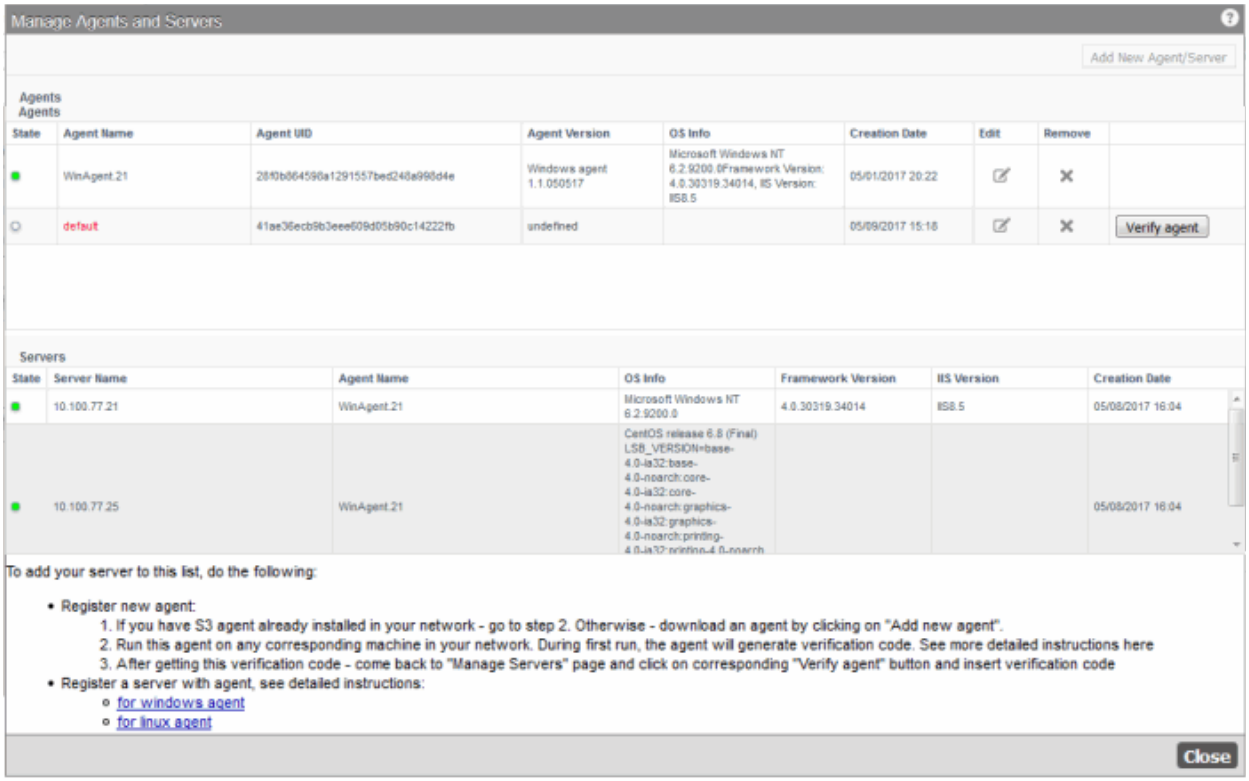
To update an agent,

- 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:



- The 'Manage Agents and Servers' dialog allows you to view server and agent availability, edit the agent name and re-download the agent if required:



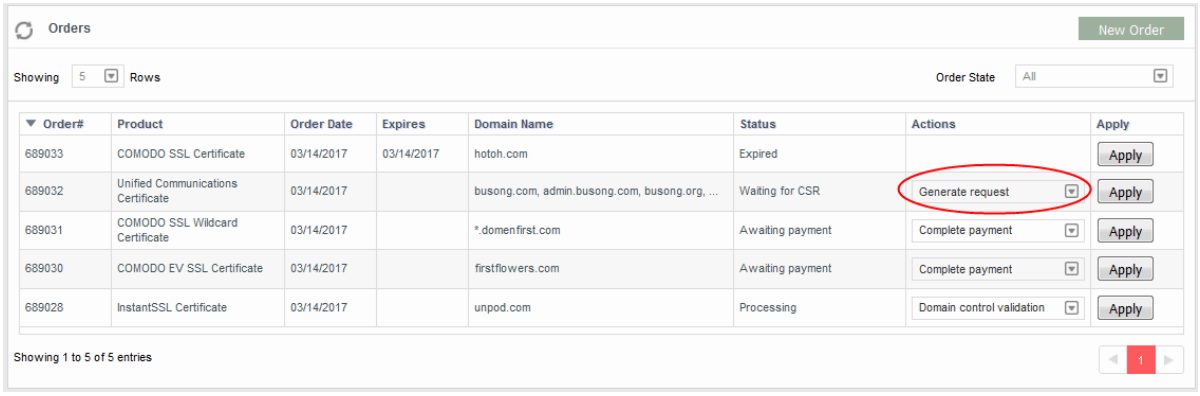
- Agents are shown in the top half of the window, while all servers added via those agents are listed at the bottom
- Both agent and server must be active (green icon) for S³ to carry out actions such as installing certificates.

3.2. Generate and Submit a CSR

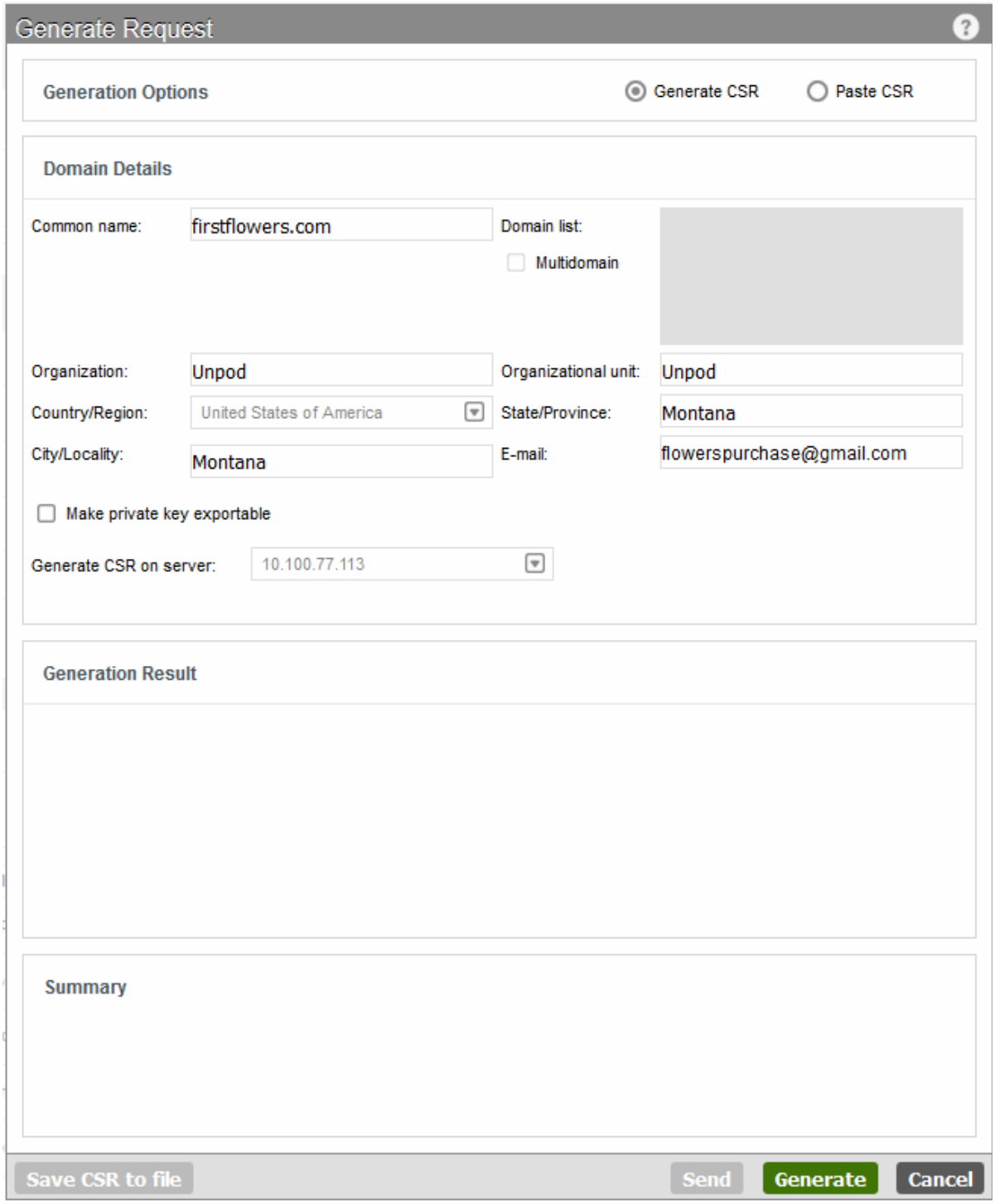
- This step deals with orders that have the status 'Waiting for CSR'.
- If your order has a status of 'Processing', then **skip to Complete Domain Control Validation**
- If your order has a status of 'Issued', then **skip to Install a certificate**.
- If your order has a status of 'Awaiting Payment'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

To generate and submit a CSR:

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

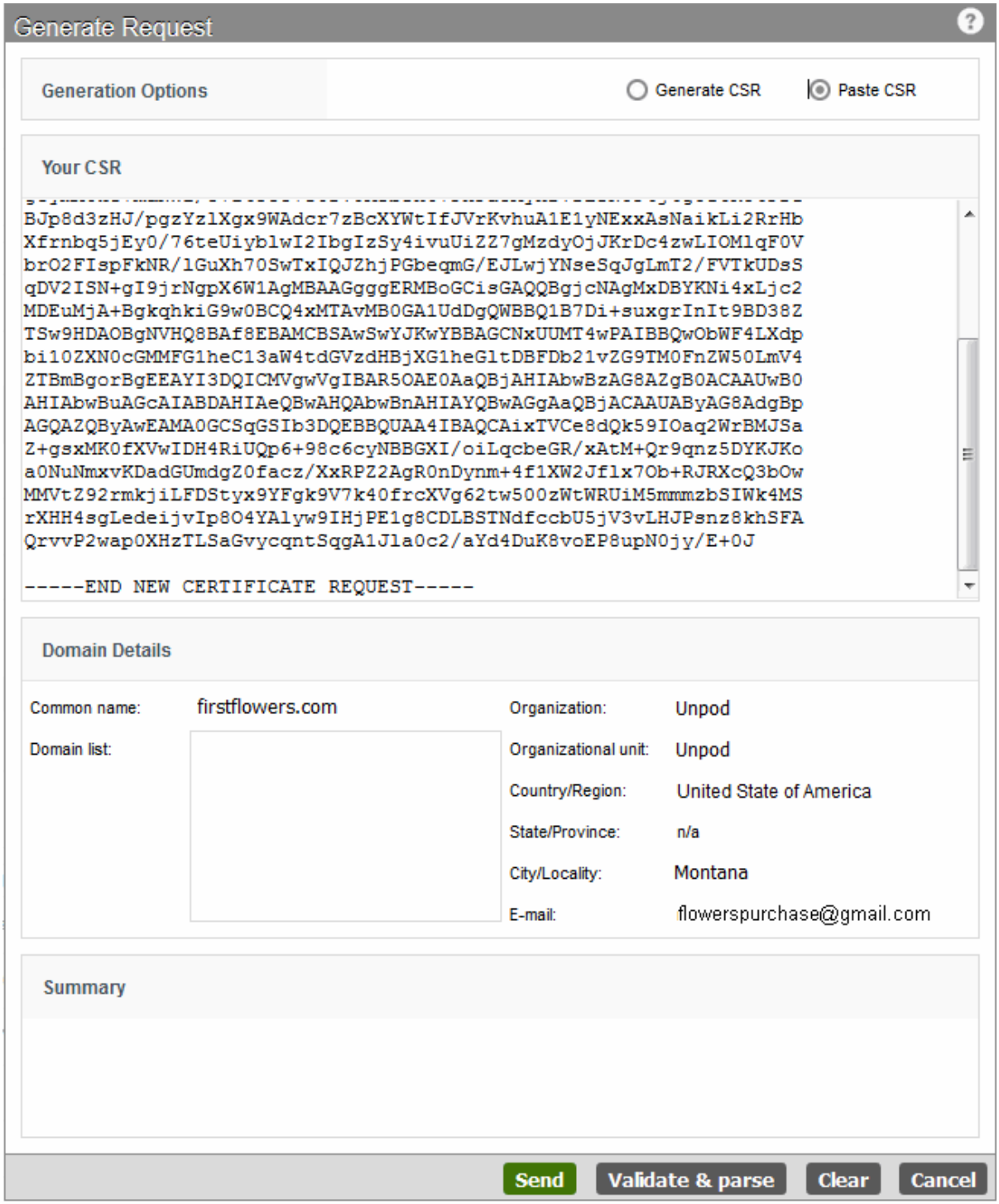


The 'Generate Request' form will open:



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 can generate it using S³ (please note that this requires software agent to be installed and run) and complete all fields. Most are self-explanatory, but for those with little experience of certificates:

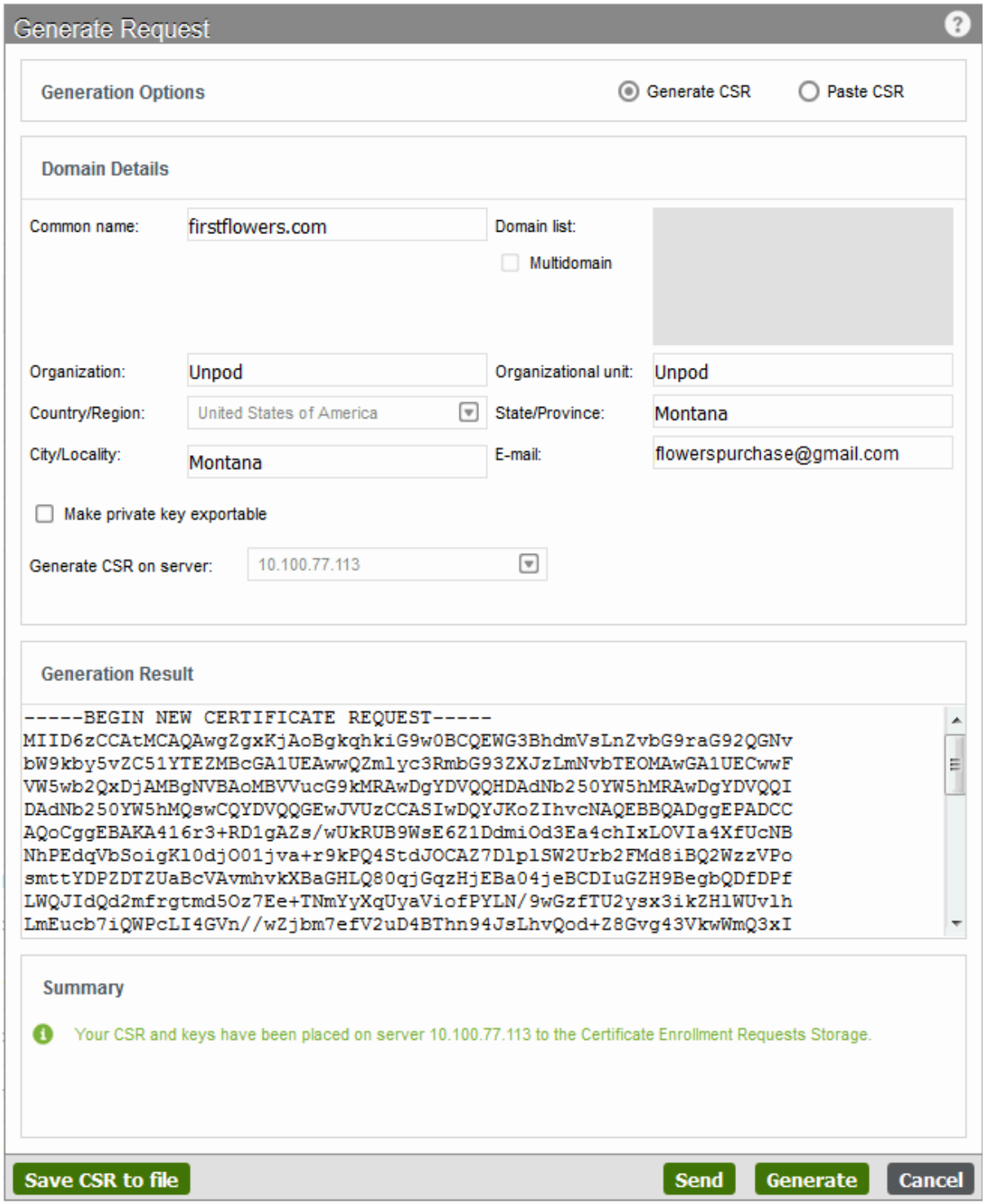
Domain Details

- 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.

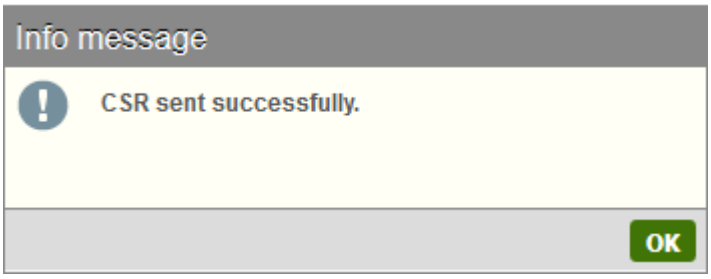
After the CSR form is complete:

- 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 window will appear:



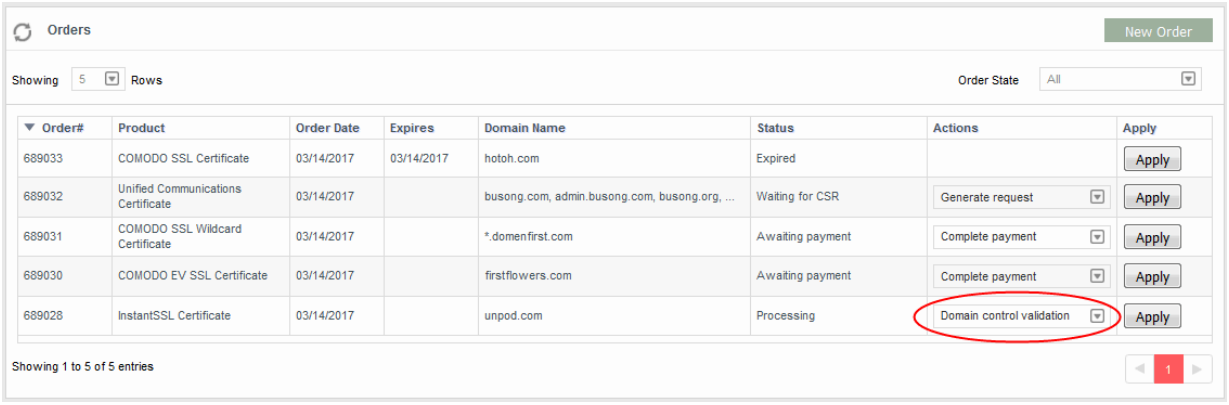
The certificate status will change to 'Processing' and 'Actions' for this certificate will now contain three options – "Replace CSR", "Domain control validation" and "Request Invoice".

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.

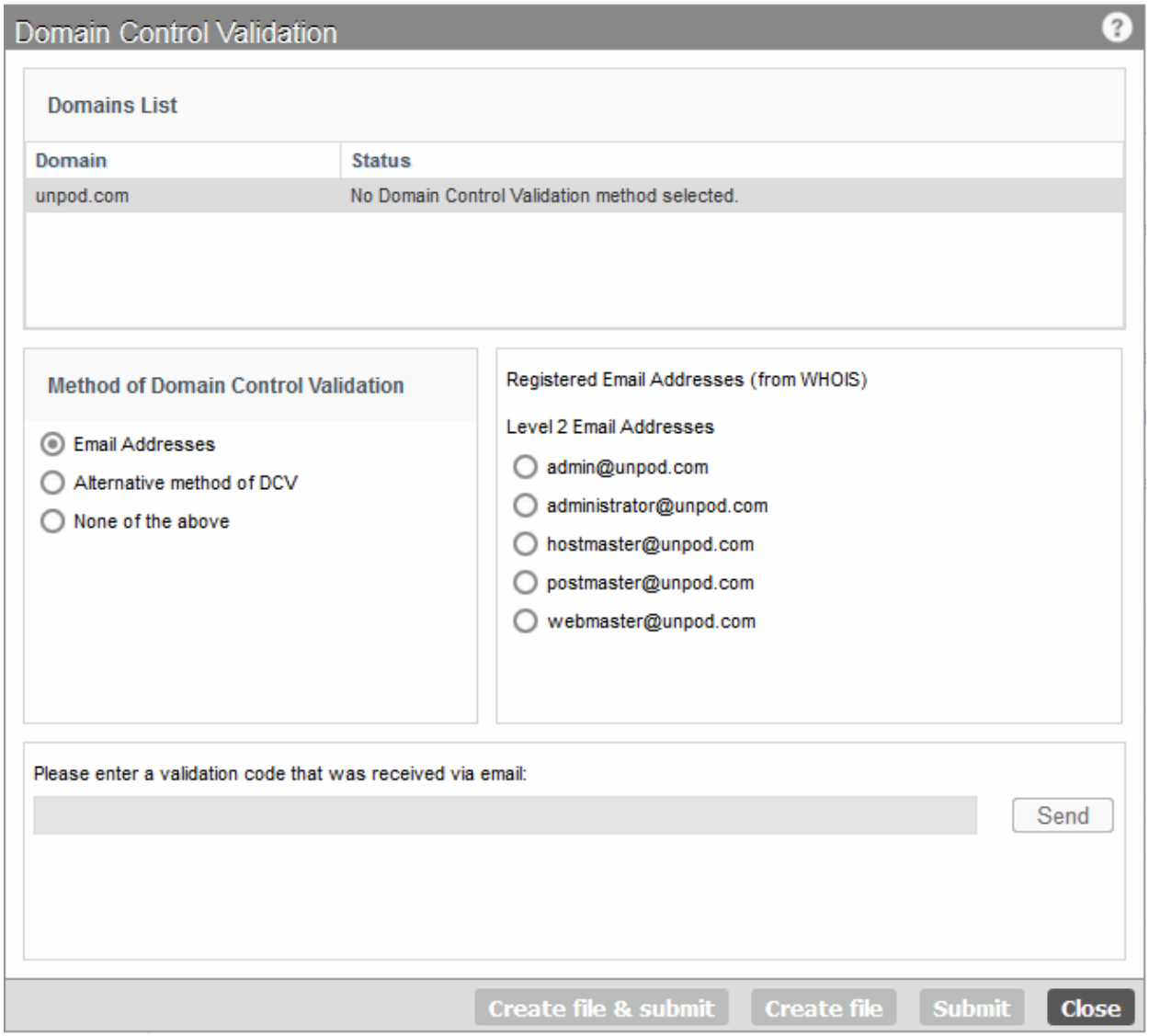
While this is in progress you should complete Domain Control Validation (DCV).

3.3. Complete Domain Control Validation

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 'Actions' drop-down and click 'Apply':



This will open the DCV configuration interface:



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

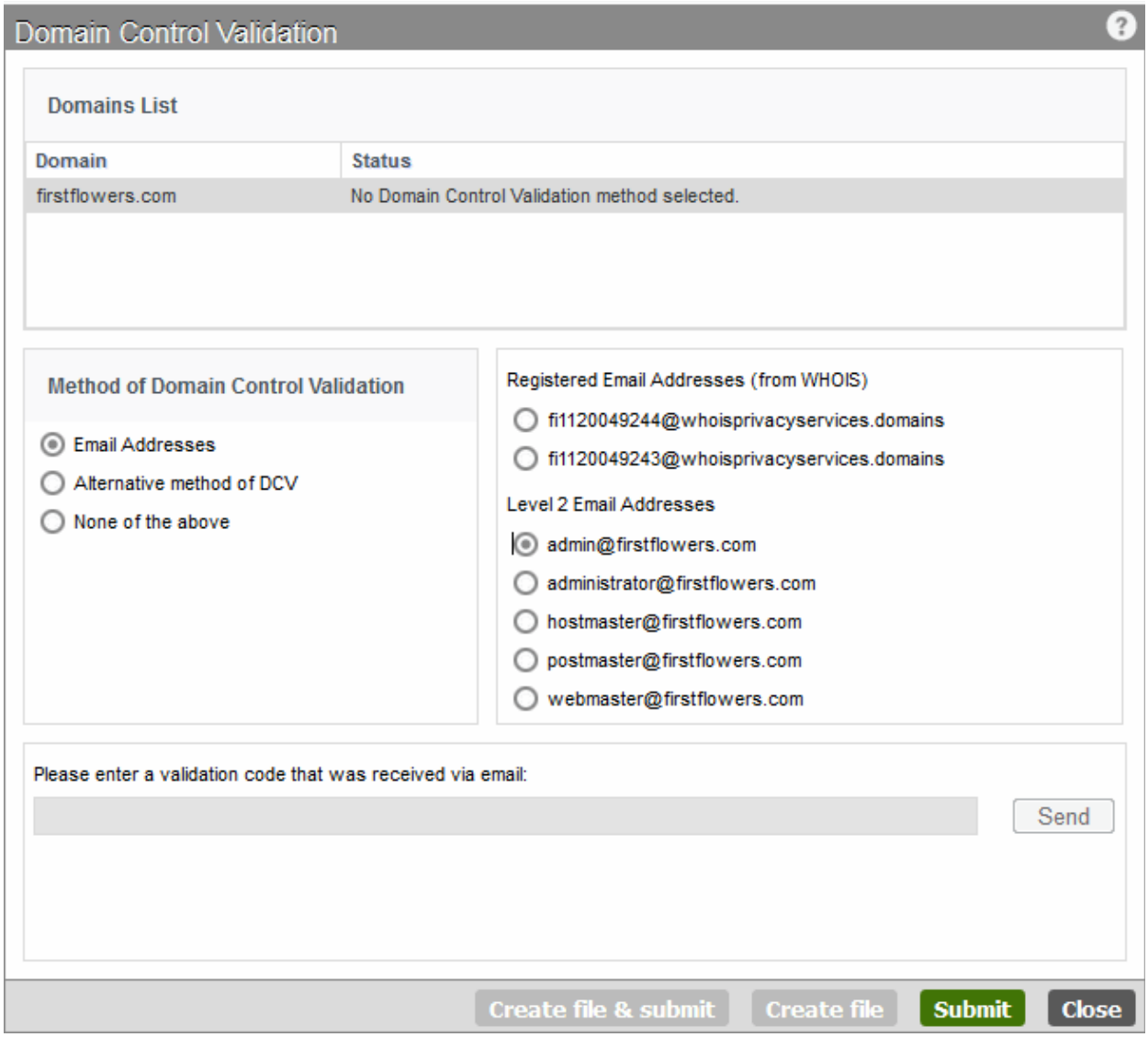
- **Validation by alternative methods of DCV** – There are currently 3 alternative methods you can pick from. The first two involve uploading a .txt file containing hashes of your CSR to your web server. The third involves adding the hash of your CSR as a DNS CNAME for your domain. In all cases, Comodo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

  OR

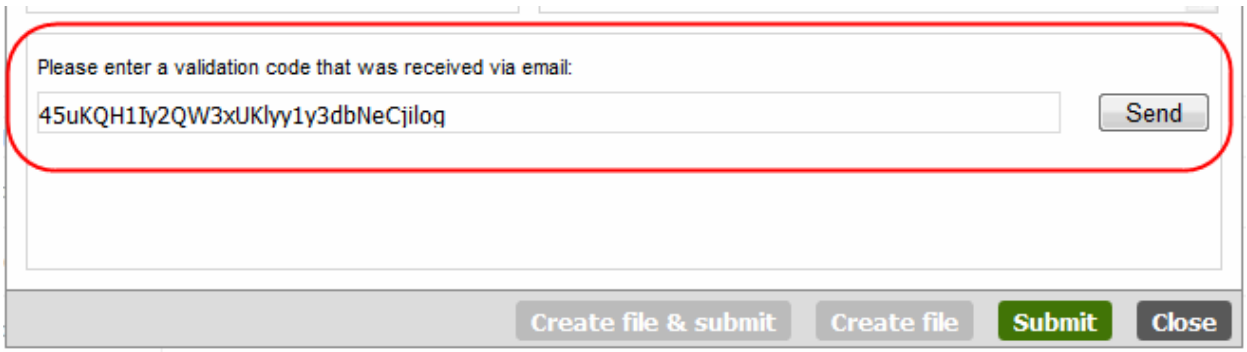
- None of the above – Choose this if you have already arranged an alternative way of completing DCV with Comodo. If you choose this option, please remember to click 'Submit' to register this choice with Comodo issuance systems and to cancel any DCV method you may have selected previously.

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.



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 as shown below:

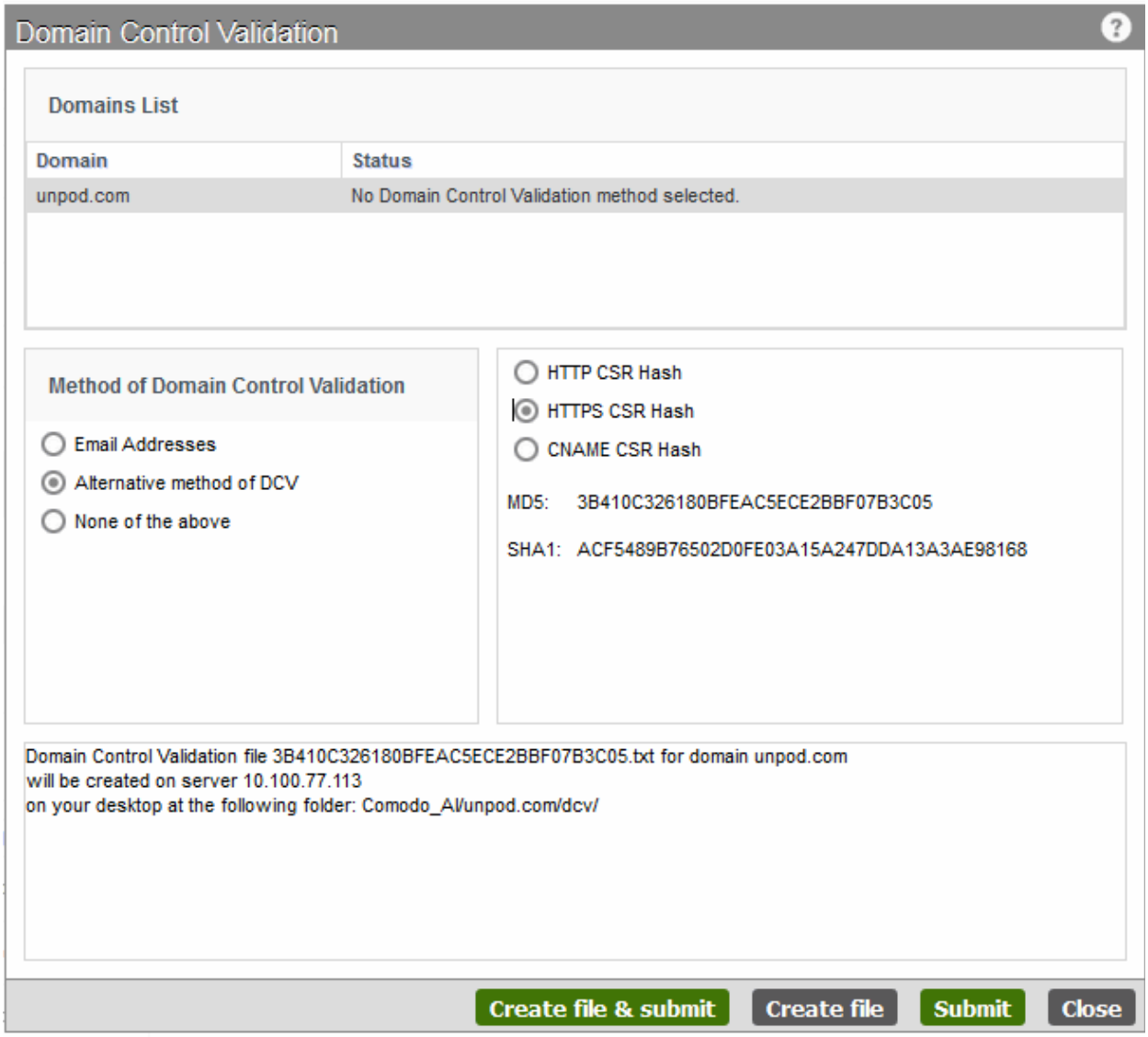


- Click 'Send' to submit the code for verification

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?/comodo/Knowledgebase/Article/View/791/0/

In short, you need to create a plain-text (.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 **/.**well-known**/**pki-validation**/** 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

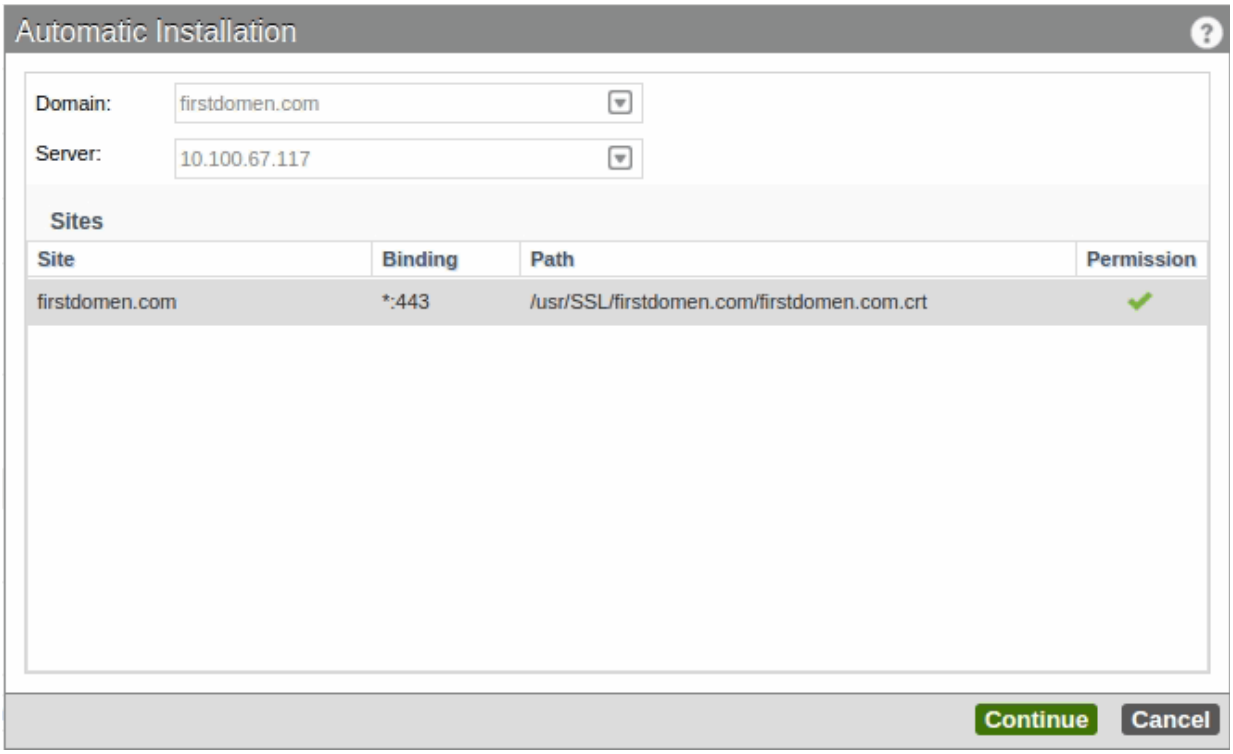
Make sure to include the trailing periods as the check will fail without them.

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

3.4. Install or Save Issued Certificate

If your certificate has a status of 'Issued' then the next action you should choose is 'Autoinstall' certificate.

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

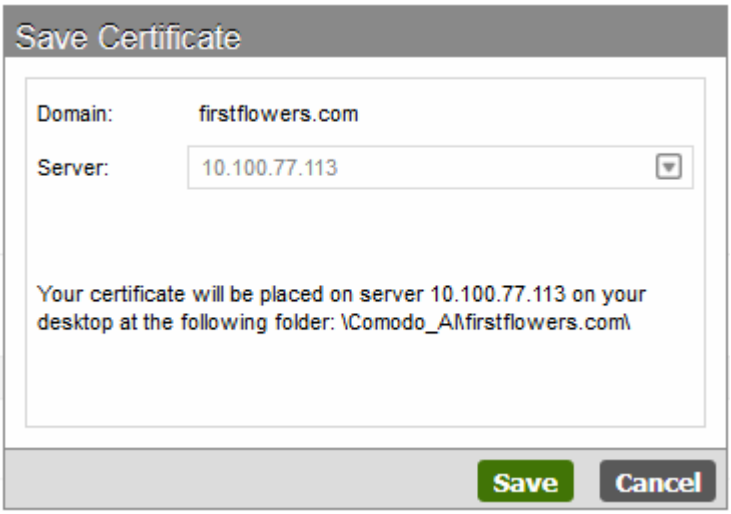


- Select the domain on which the certificate should be installed from the 'Domain' drop-down
- Select the target server from the 'Server' drop-down
- Click 'Continue'

You will see a confirmation message when your certificate is installed.

To save a certificate

- Select a certificate with 'Issued' status
- In the 'Actions' drop-drown, choose 'Save certificate' and click 'Apply'
- Define the target server in the 'Server' drop-box



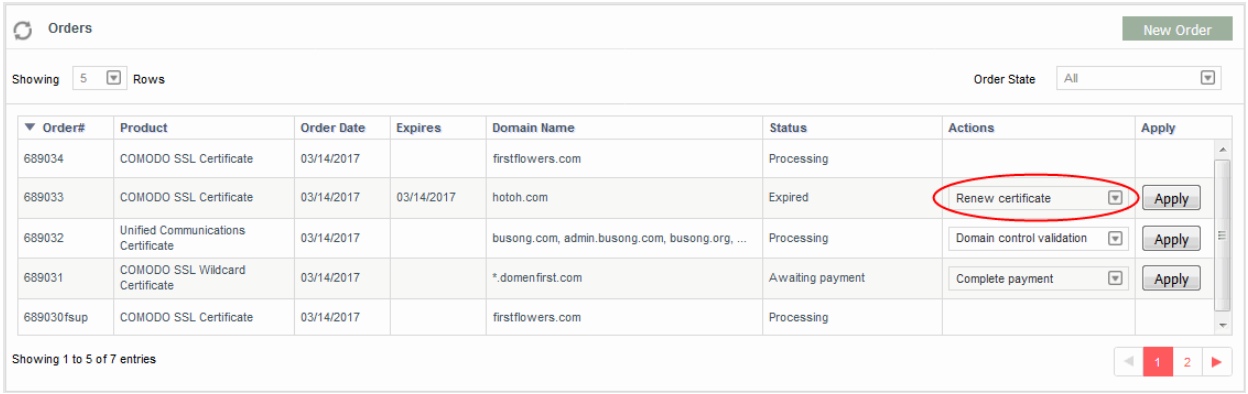
- Click 'Save'

- You will see a confirmation message when your certificate is saved. Click 'OK'

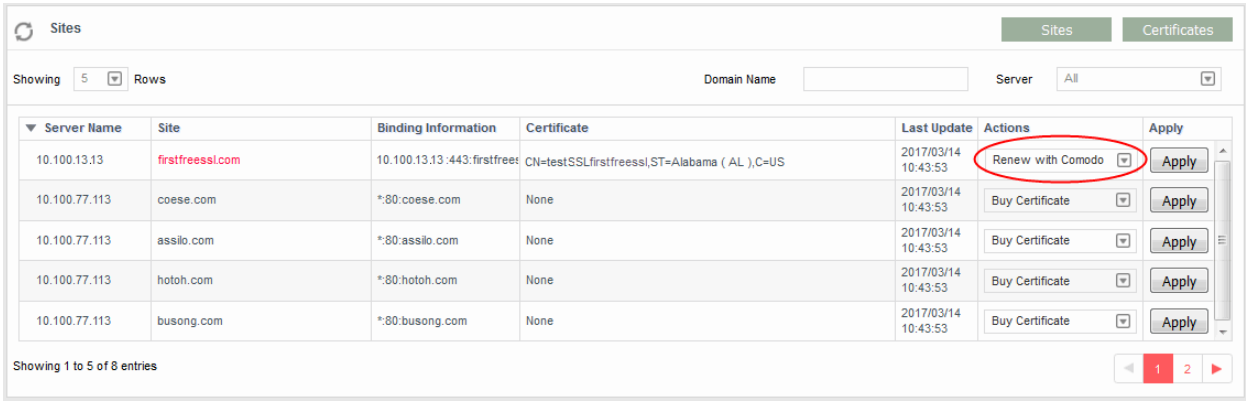
4. Renew a Certificate

S³ provides three ways to renew certificates:

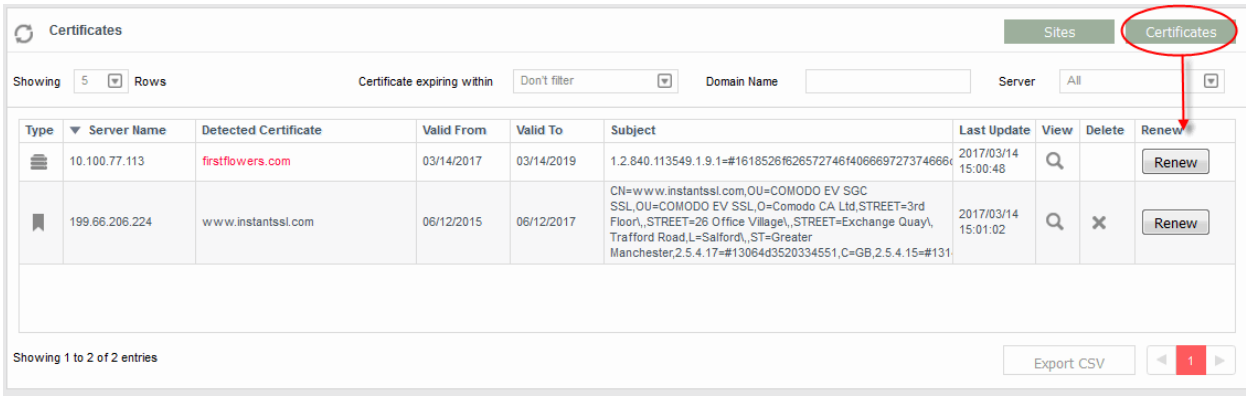
- To renew one of your Comodo certificate orders, use the 'Renew certificate' option in the 'Actions' drop-down'



- To renew non-Comodo discovered certificates orders, locate the certificate in the 'Sites' list and select 'Renew with Comodo' from the drop-down box



- Alternatively, click the 'Certificates' button, locate the certificate in question and click the 'Renew' button:



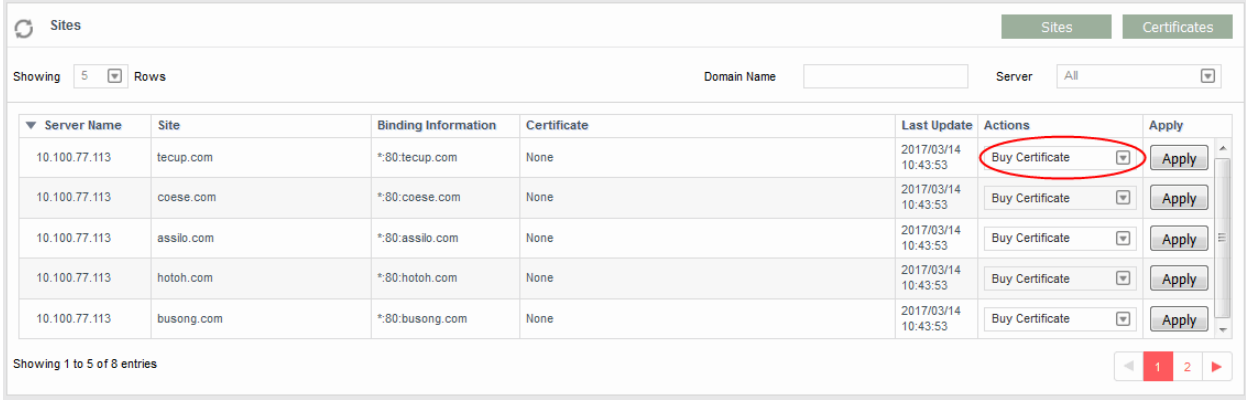
After clicking the 'Certificates' button, you can locate a specific certificate by using the search filters along the top. You can search by time-to-expiry, domain name and server IP.

After choosing a certificate to renew, you will move onto the next step, **Completing Your Order**

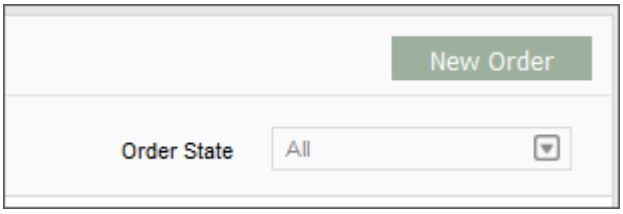
5. Buy a Certificate

There are a couple of ways to buy a new certificate in S³:

- Select 'Buy Certificate' on the 'Sites' menu. This allows you to purchase a certificate for domains that were detected on your servers



- Click the 'New Order' button at the right of the 'Orders' panel:

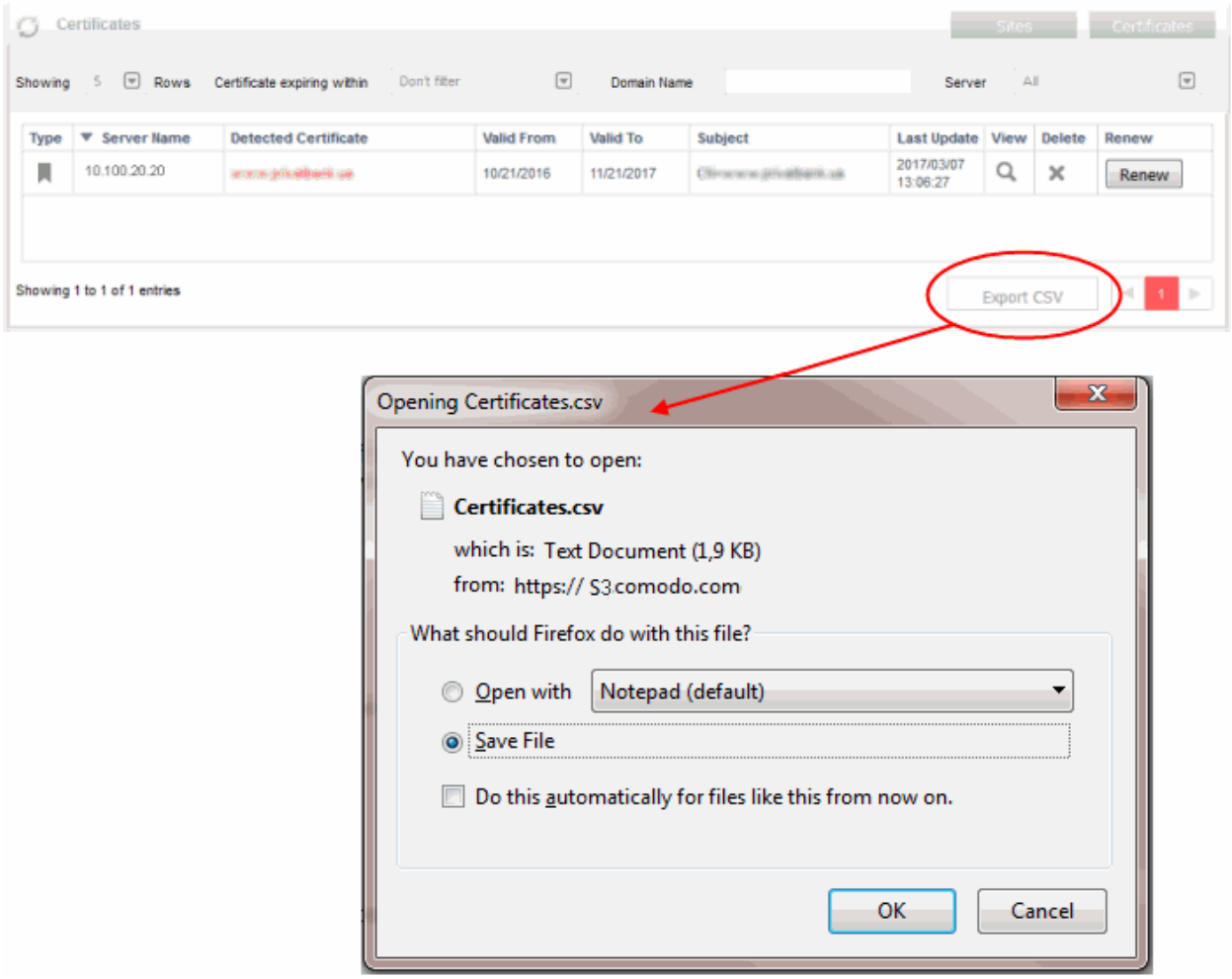


In either case, the 'Create new order' form will open. Refer to **Completing your Order** to move onto the next step.

Administrators can save all detected certificates by exporting them as a CSV file.

To export the list of certificates

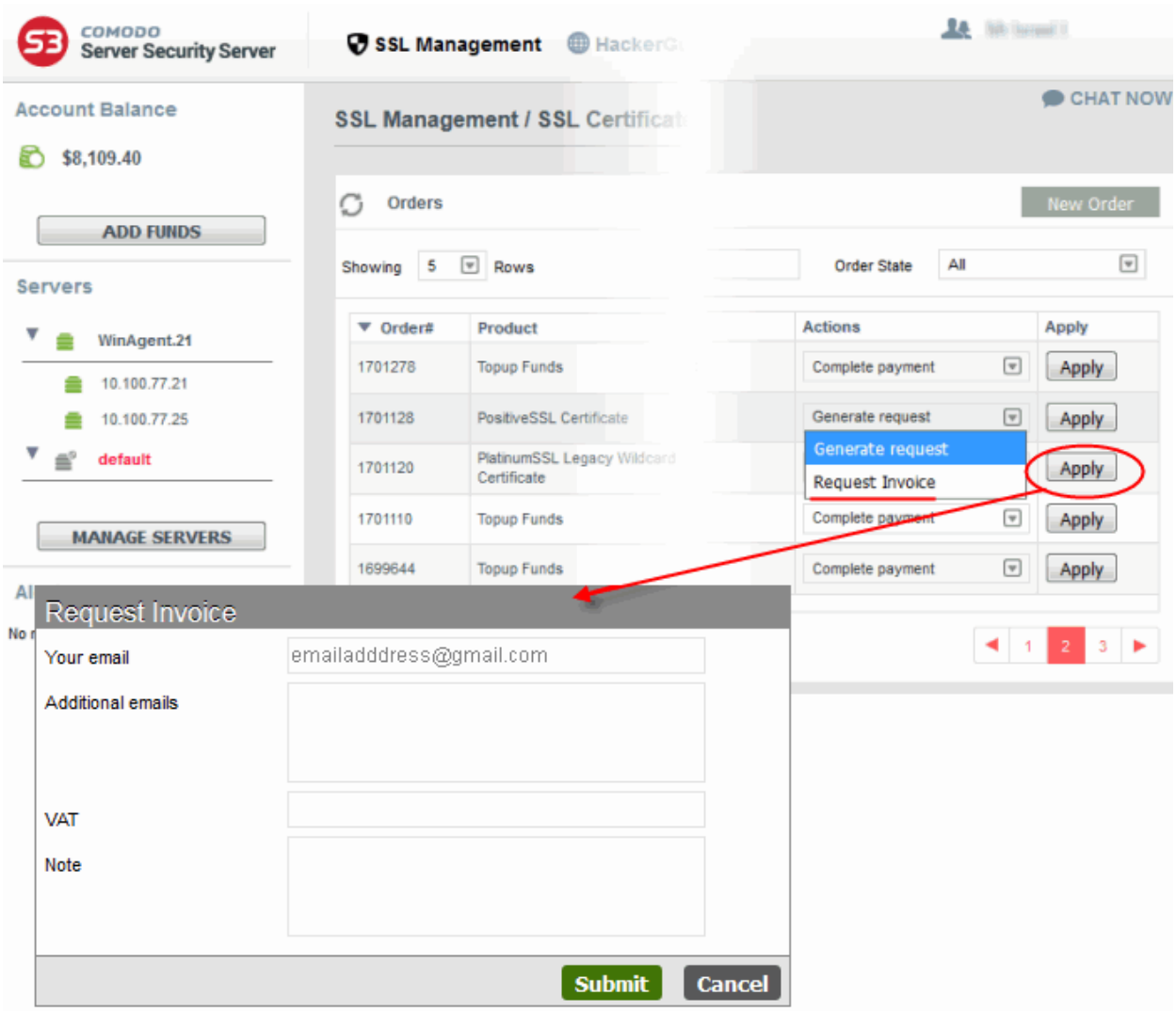
- Click 'Export CSV' button at the bottom of the 'Certificates' pane
- The export dialog will open:



- Click 'OK' and navigate to the location in your computer to save the file.

You can request an invoice to acknowledge your certificate purchase:

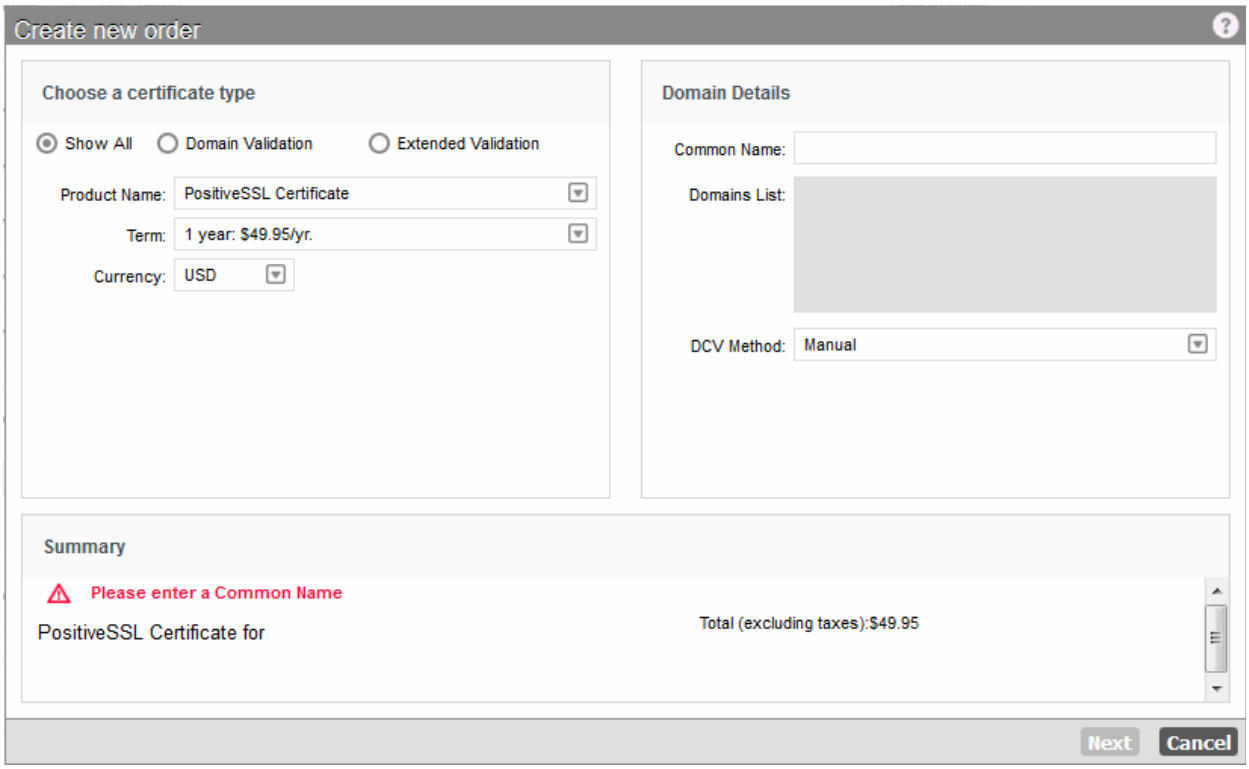
- Select 'Request Invoice' in the 'Actions' drop-down then click 'Apply'
- In the 'Request Invoice' dialog, complete the required information then click 'Submit



You will receive an email notification.

6. 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 Name: Choose between Extended Validation or Domain Validation certificate categories
  - EPKI users - Select the 'Domain Validation' category to see a list of all non-EV certificates in your account (including OV certs)
- Select the certificate type you wish to purchase
- Select the term of your certificate from the 'term' drop-down
- Currency: Allows you to change your payment currency if required.

Domain Details

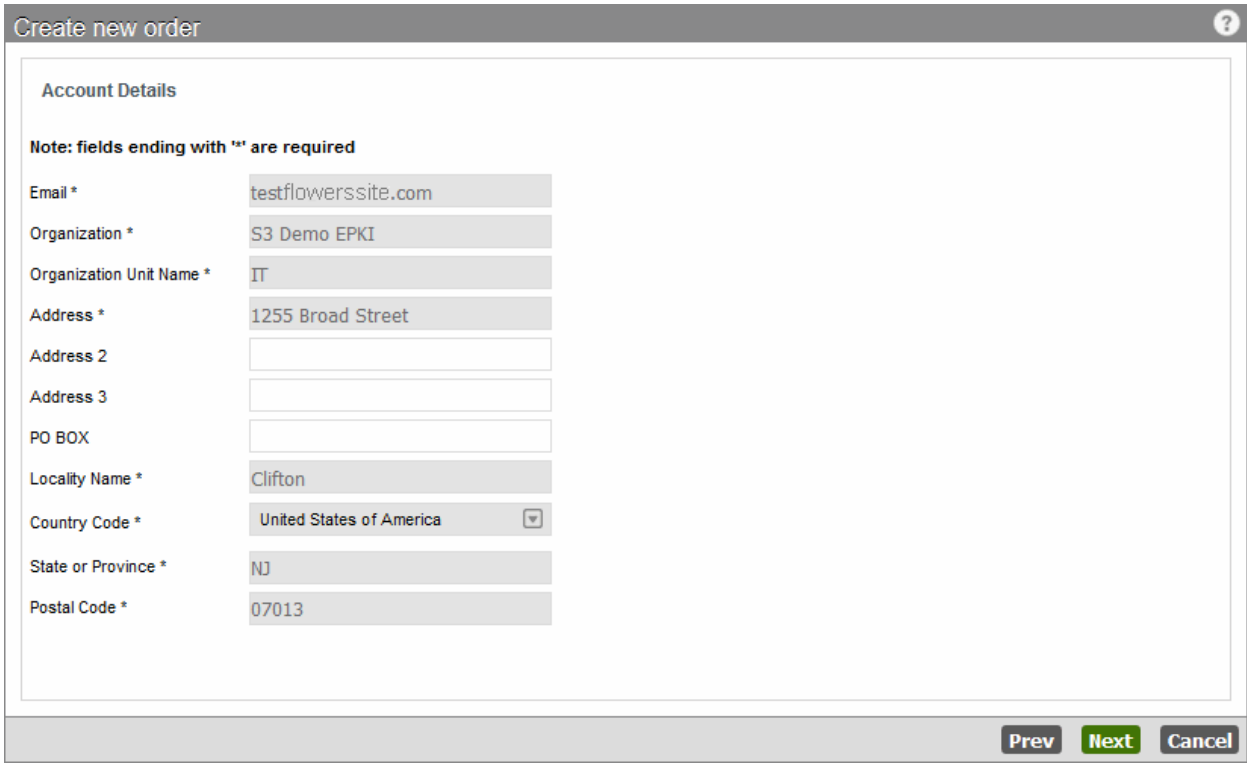
- Common Name: Fully Qualified Domain Name (for example, www.domain.com). This should be auto-populated if you are renewing a certificate.
- Domain List: Select the domain name form available in the the list.
- DCV Method: Select a method for completing Domain Control Validation.
  Note: 'HTTP CSR HASH' is the recommended options. The form will default to these options if we detect it is possible to complete validation this way on your server.

Summary

Displays the common certificate type and cost details.

- Click 'Next'.

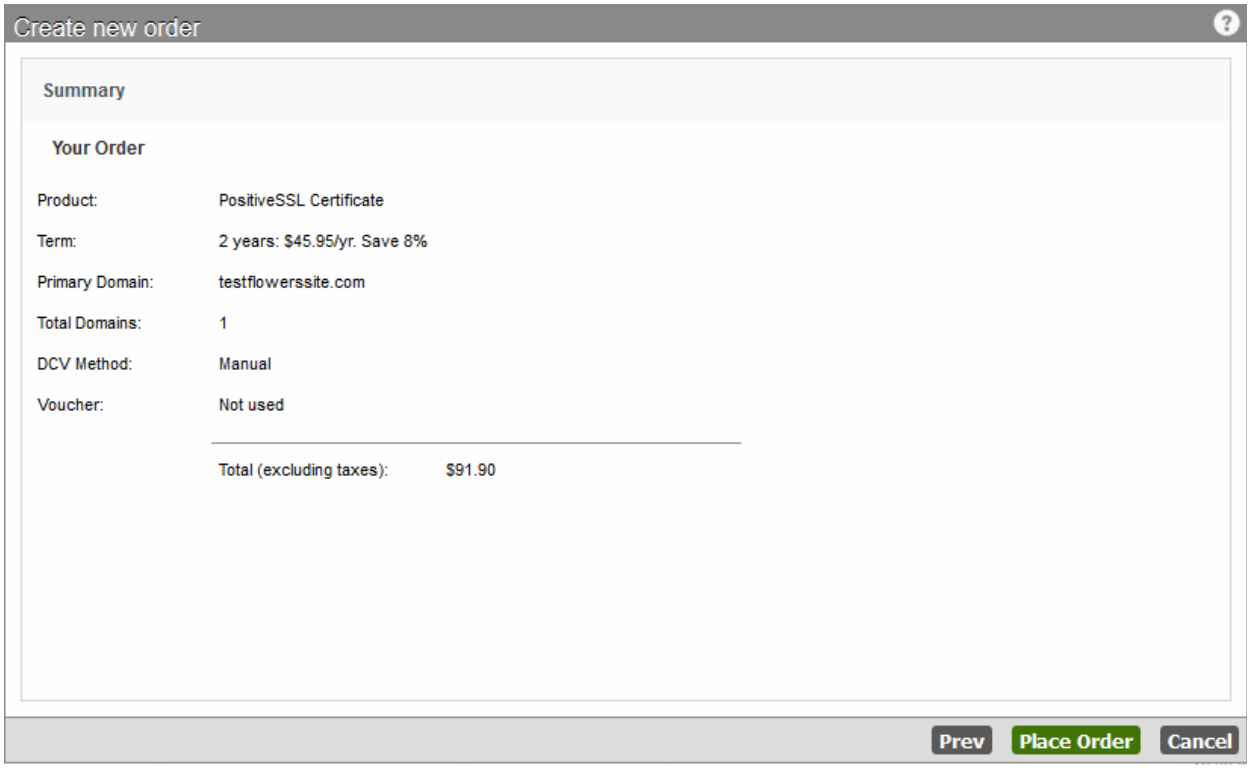
The next step is the account and contact details screen. Fields marked *are mandatory.



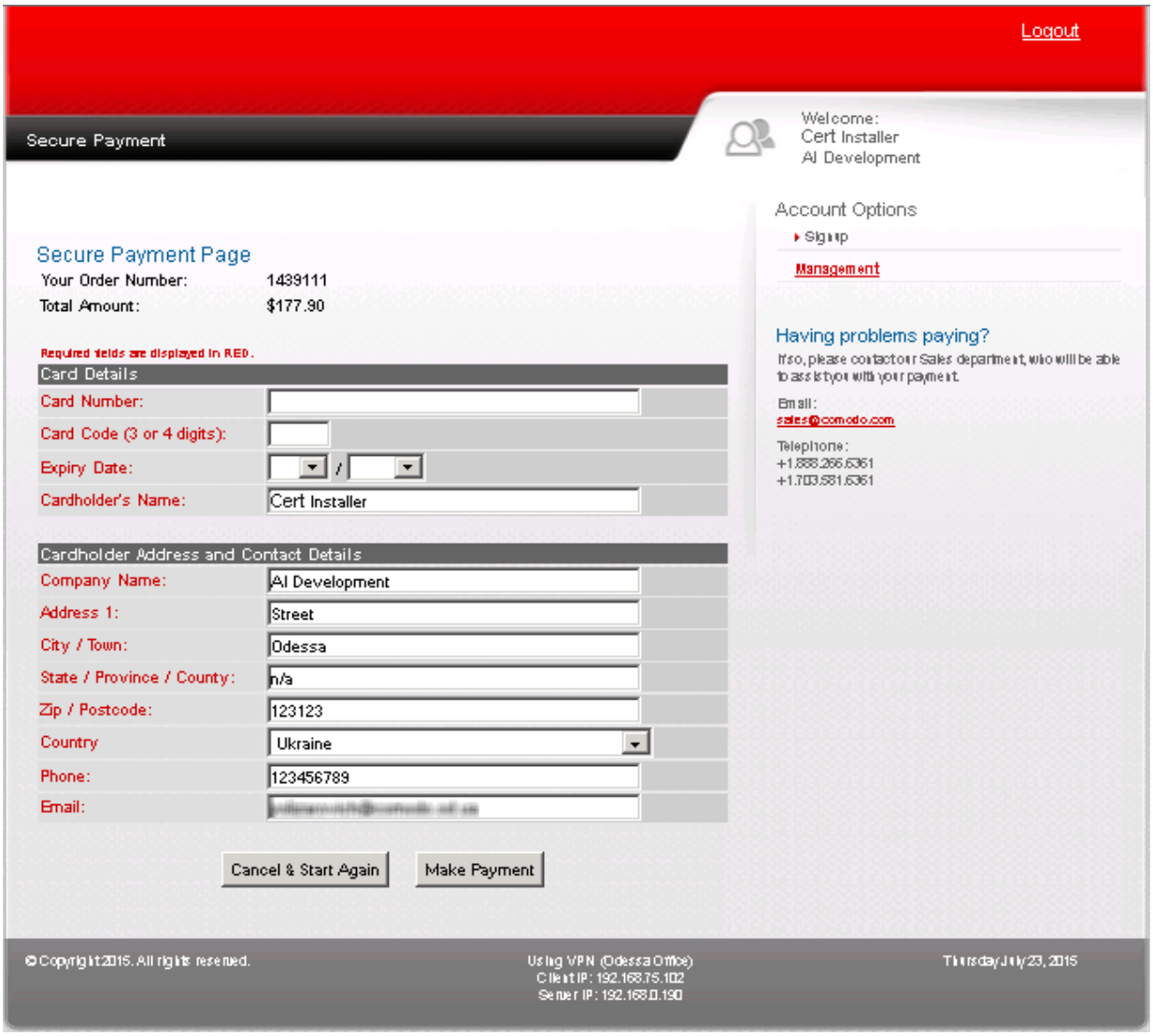
In many cases we will be able to draw all the company and contact details we need from our records, so you may not see this screen at all. In certain cases, however, we may need you to submit additional information. For example, an EV certificate application requires additional information that you might 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:



- Click 'Place Order' to continue.
- 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'
- Click 'Complete Payment' to open the Comodo order form:



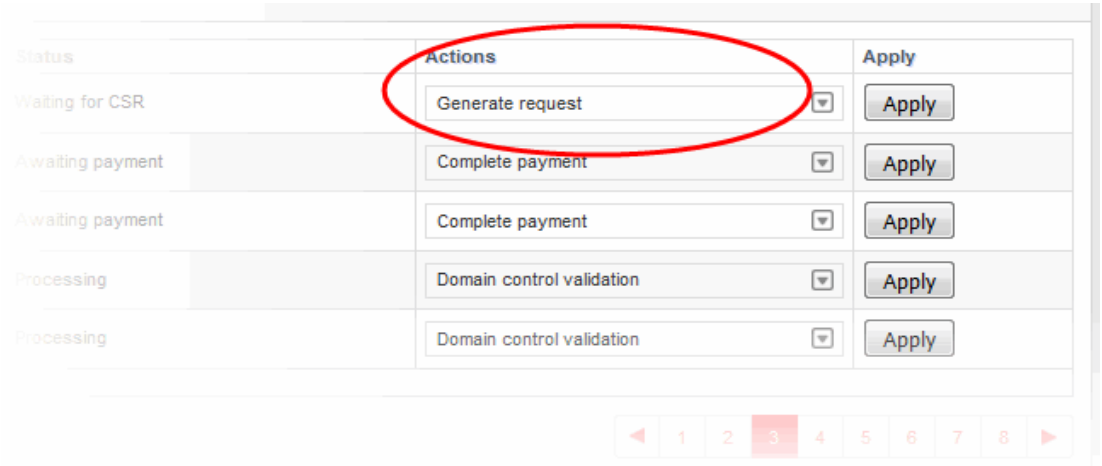
Complete the required card payment details then click 'Make Payment'. Once payment is complete, your new certificate will appear in the SSL management interface as a new order with 'Waiting for CSR' status. Refer to **Generate and Submit CSR** section for more information.

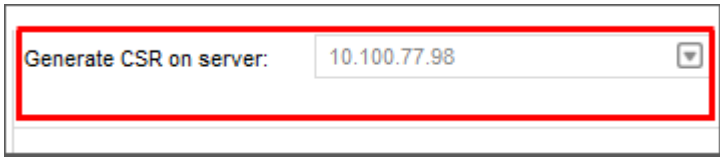
7. Generate a CSR

If your certificate order has a status of 'Waiting for CSR' then select 'Generate Request' and click the 'Apply' button.

This will start a wizard to help you create and submit a CSR for the domain listed in the 'Domain Name' column.

Make sure to specify the server which hosts the target domain in the 'Generate CSR on server' box:





Click here for more detailed help on generating a CSR.

8. SSL Certificate Discovery Tool

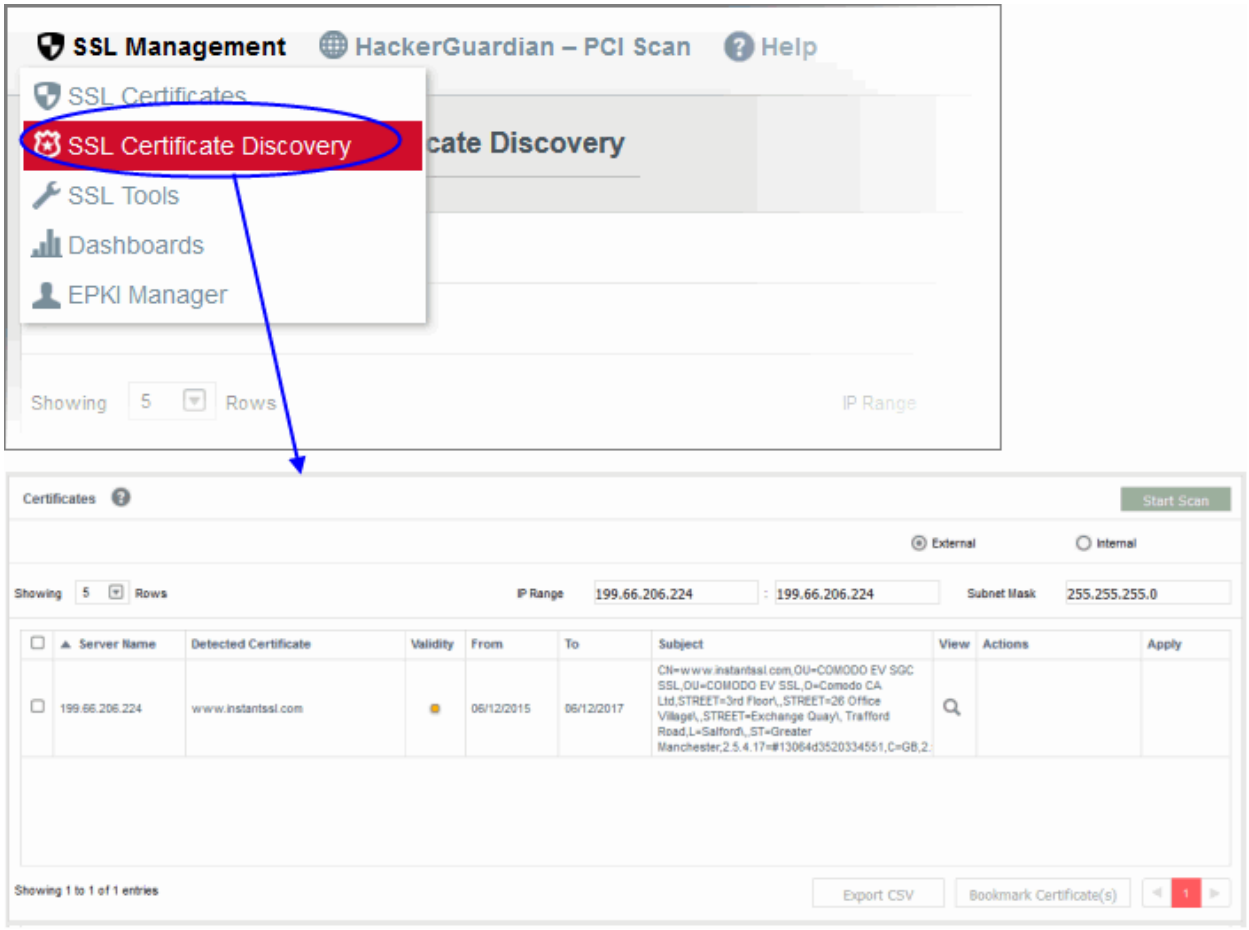
The 'SSL Certificate Discovery' tool allows you to scan for certificates on IP addresses associated with your S³ account. The scan will find public-facing certificates and internal certificates, regardless of issuing certificate authority. You can renew discovered certificates from the lower pane of the 'SSL Management' interface.

Note – for internal scans you must have installed and run the agent on your network to use the discovery tool.

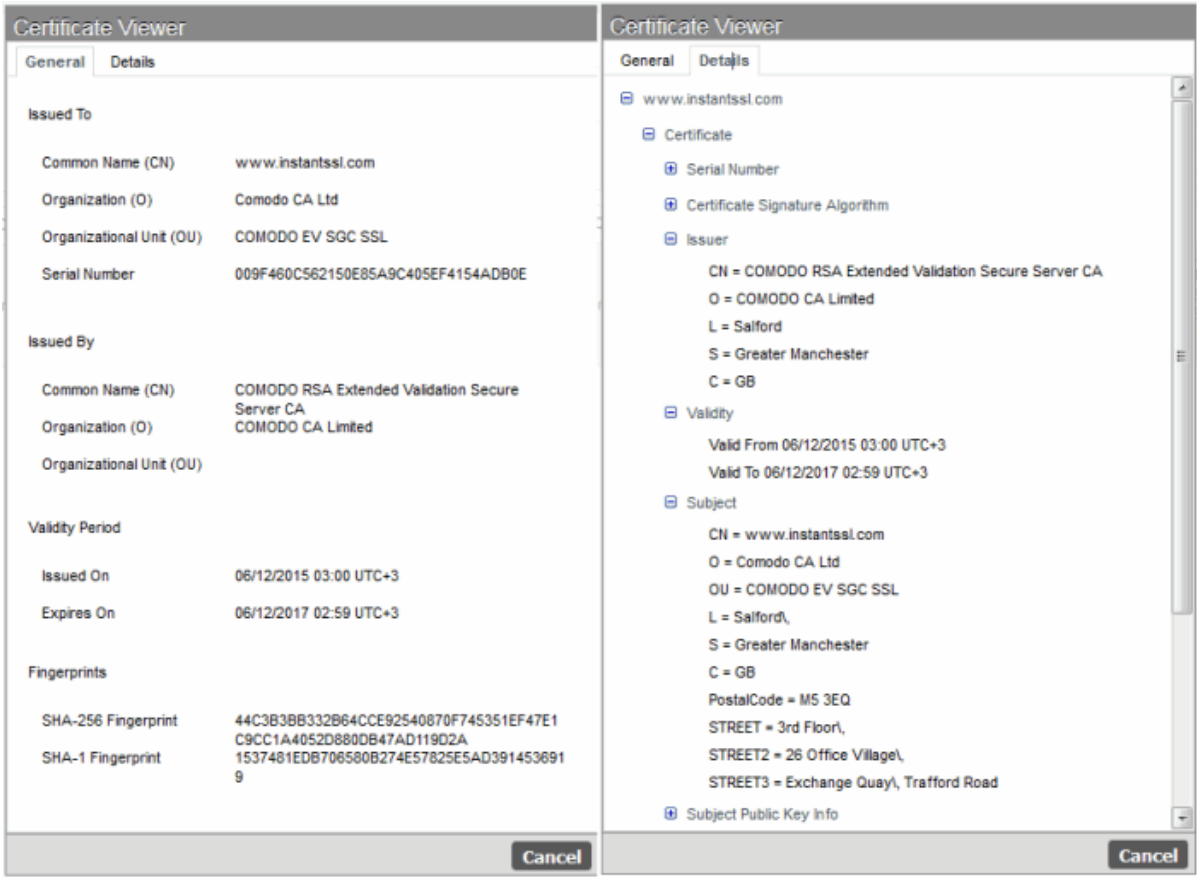
- On the file menu, click 'SSL Management' then 'SSL Certificate Discovery' to open the discovery interface

To discover certificates

- Choose 'External' or 'Internal' discovery as required
- For internal scans you will need to select an agent from the drop-down
- Enter your IP range and subnet mask in the boxes provided
- Click the 'Start Scan' button at the top-right
- The results table will show all certificates currently deployed on the IP addresses you specified:



- The 'View' icon next to a certificate opens the 'Certificate Viewer' which contains general and detailed certificate information:



- Click 'Cancel' to close the viewer

- To renew discovered certificates that are issued by CAs other than Comodo, click 'Renew with Comodo' then click 'Apply'
- To save certificates information in CSV format, click the 'Export CSV' on the bottom
- To import a certificate to S³ management console, check the certificate box then click 'Bookmark Certificate(s)' on the bottom.

Importing important certificates is useful if you have many certificates to manage, or if you wish to mark a particular certificate for attention in the future.

- Click 'OK' to confirm your selection. Imported certificate(s) will be seen in the lower pane in the 'SSL Management' interface and marked with flag icon.

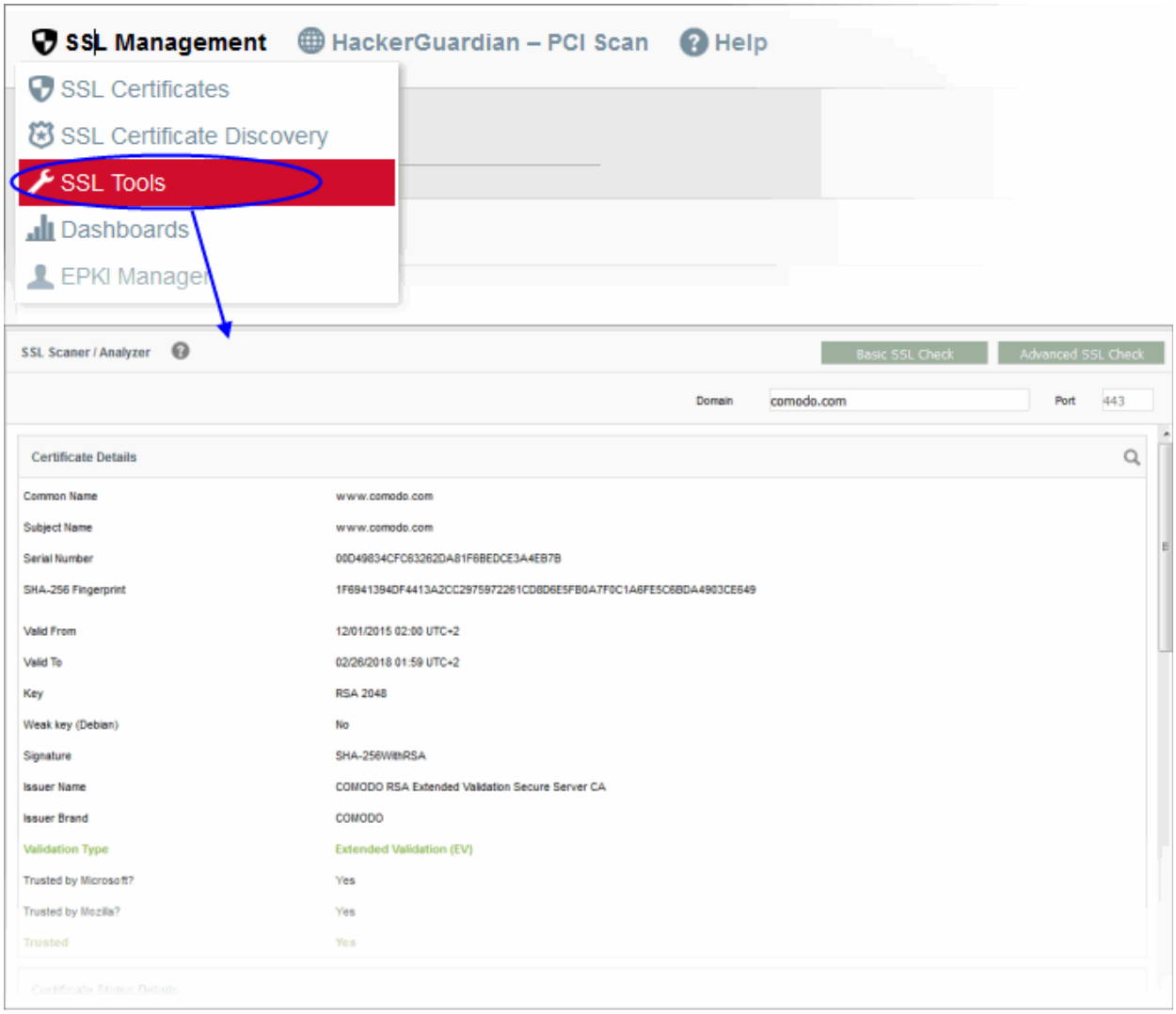
9. SSL Tools

The 'SSL Tools' section contains a certificate analysis utility which checks whether a certificate on a particular domain is installed correctly. The tool shows basic certificate information such as key size, common name, SAN names and organization info. It also identifies any issues with your web-server configuration, such as supported protocols, available cipher suites and web-server features.

- Open the 'SSL Tools' area by choosing 'SSL Management' > 'SSL Tools' from the drop-down at the the top left

To run the analyzer

- Enter common name SSL was issued for in the 'Domain' box (for example, *comodo.com*)
- Specify port. (*Default=443*). If you do not have custom settings on your server, leave it at the default.
- Click 'Basic SSL Check' or 'Advanced SSL Check' button at the top-right.



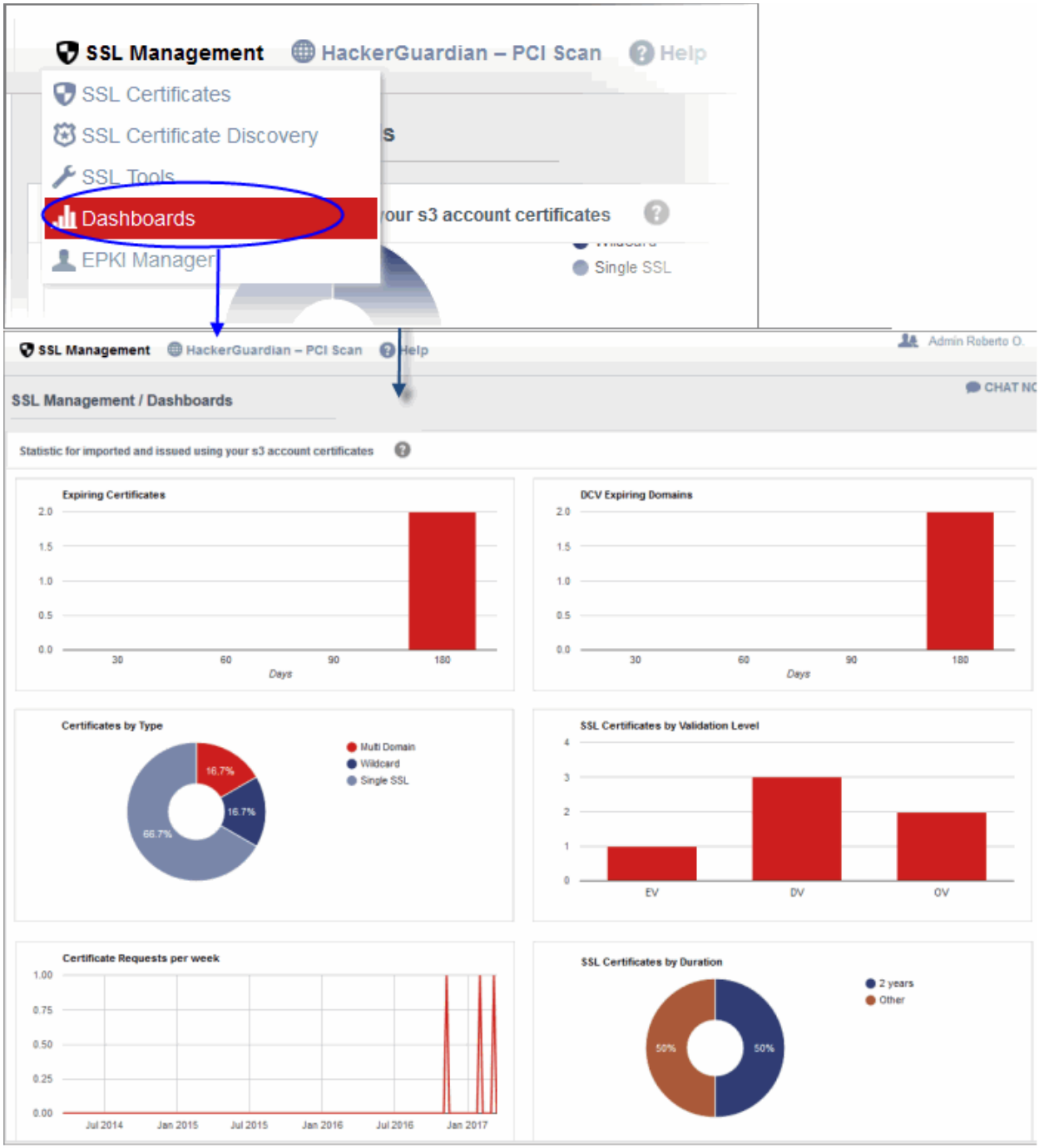
- 'Basic SSL Check' provides basic certificate information and is useful for quickly identifying the validity, type and issuer of the certificate.
- 'Advanced SSL Check' shows the basic information plus details about web-server configuration, including any protocol problems and whether the web server has the correct cipher suites.

10. S³ Dashboards

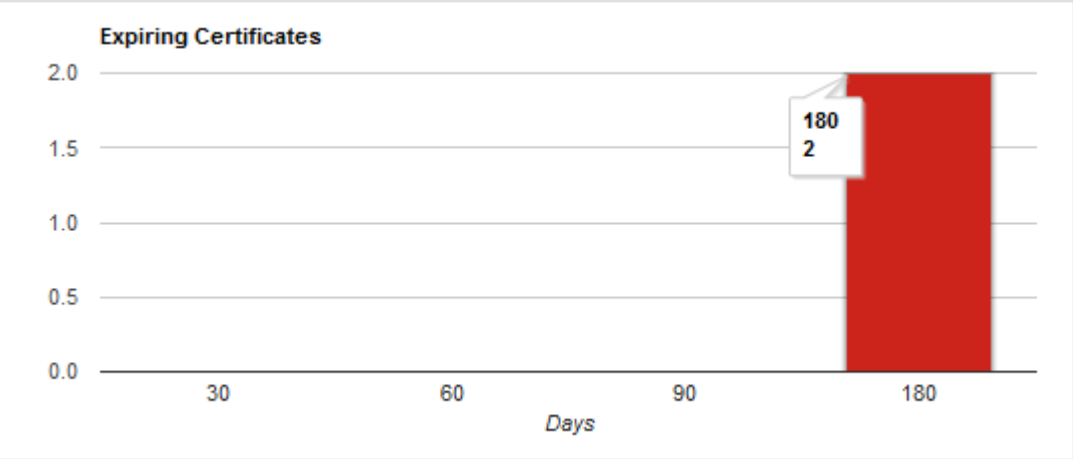
The dashboard is an informative heads-up-display which shows an overview of your Comodo certificate orders and certificates imported from your network.

- Open the 'Dashboards' area by choosing 'SSL Management' > 'Dashboards' from the drop-down at top left.

Chart data is updated in real-time, so any modifications should be reflected in the dashboard near-instantly.

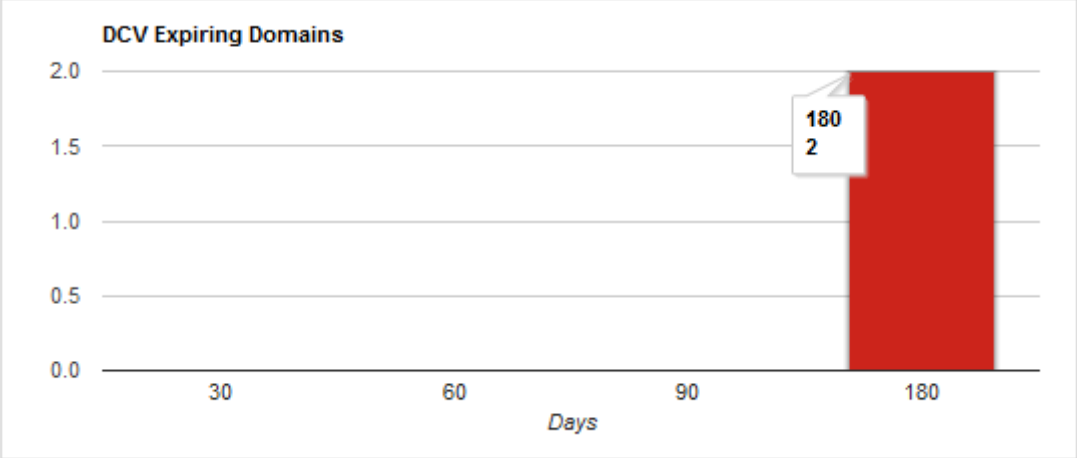


- **Expiring Certificates** – Comodo, self-signed and 'Other Trusted' certificates expiring within 180 days



The 'Expiring Certificates' bar graph shows the number of certificates expiring within the next 30, 60, 90 and 180 days. Hovering the mouse cursor over a legend or bar displays the number of certificates in each category.

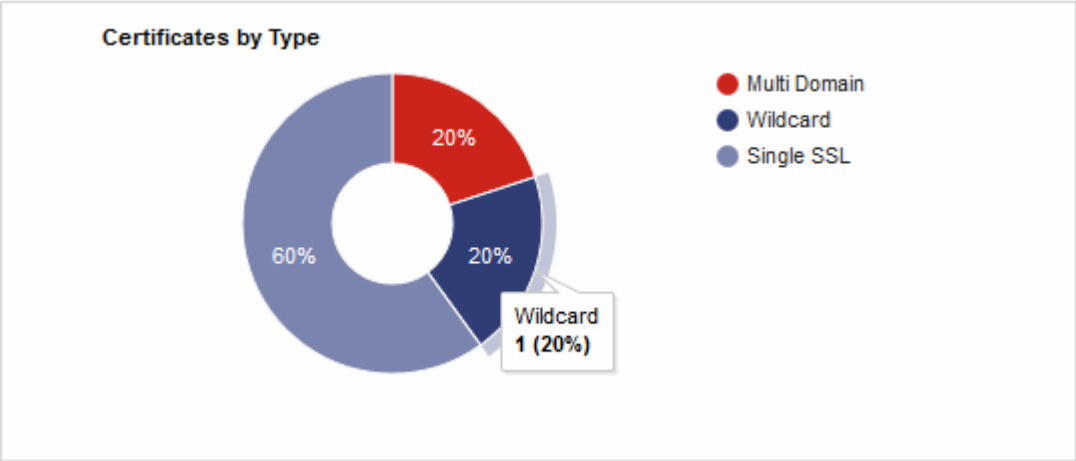
- **DCV Expiring Domains** – Domains for which Domain Control Validation will expire within 180 days



Indicates how many of your domains are within 30, 60, 90 and 180 days of DCV (domain control validation) expiry. DCV validity lasts for one year so It is possible DCV might be approaching expiry even though your certificate is not. If DCV is allowed to expire, it will not mean your certificate becomes invalid/stops functioning. However, your next application for that domain will need to pass DCV again.

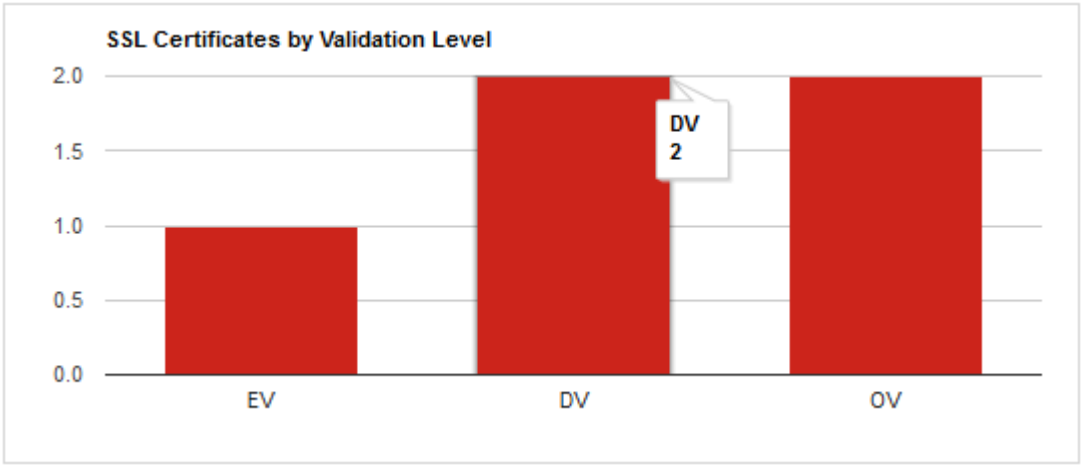
Placing the mouse cursor over a legend or bar displays a tool-tip showing the number of domains within that time-frame.

- **Certificates by Type** - Single Domain, Wildcard, Multi-Domain, UCC etc.



The 'Certificate by Type' chart shows the composition of your certificate portfolio by type (single domain, wildcard, multi-domain). Hovering your mouse cursor over a segment displays additional details such as the actual quantity of certificates of that type.

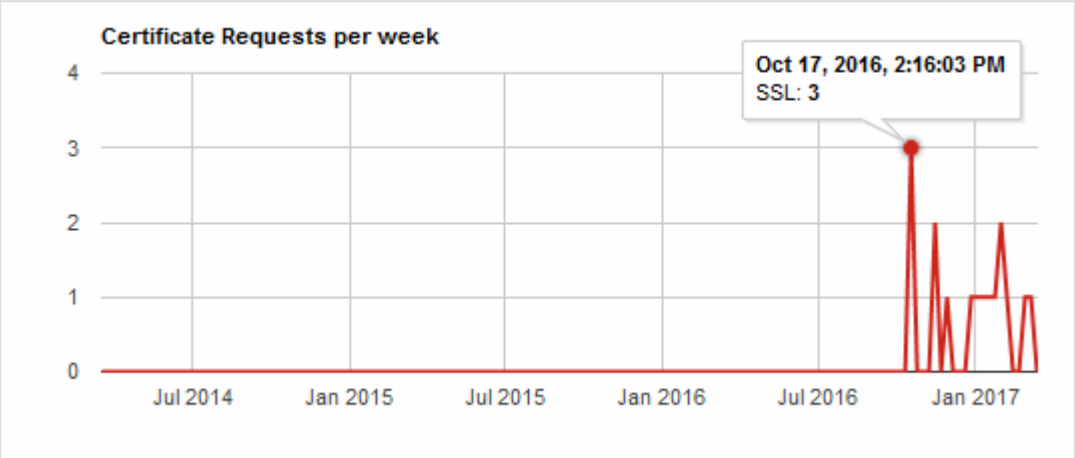
- **SSL Certificates by Validation Level** – EV, DV, OV



Displays the composition of your certificate portfolio according to certificate validation level. This includes the number of Domain Validated, Organization Validated and Extended Validation certificates on your network.

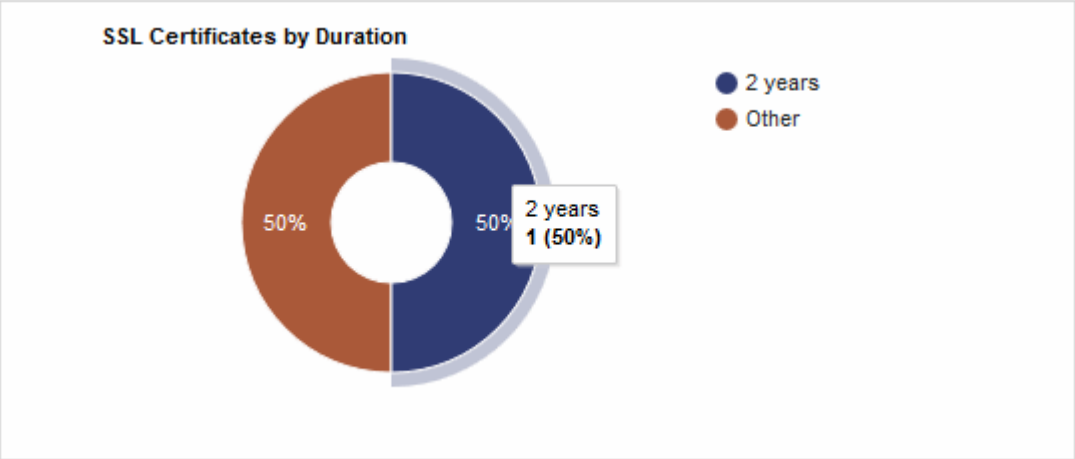
Hovering your mouse cursor over a bar displays the exact number of certificates in that category.

- **Certificate Requests per week** - The 'Certificates Requests' graph displays the number of SSL orders you have placed per week over time.



Place your mouse cursor over a section of the graph to see the exact number of certificates that were requested.

- **SSL Certificates by Duration** – How many of your certificates are 1 year, 2 year, 3 year etc.



The 'Certificates by Duration' pie chart is a break-down of your certificates by term length.

Hover your mouse cursor over a section to view the exact number of certificates with that term length and their percentage of the total.

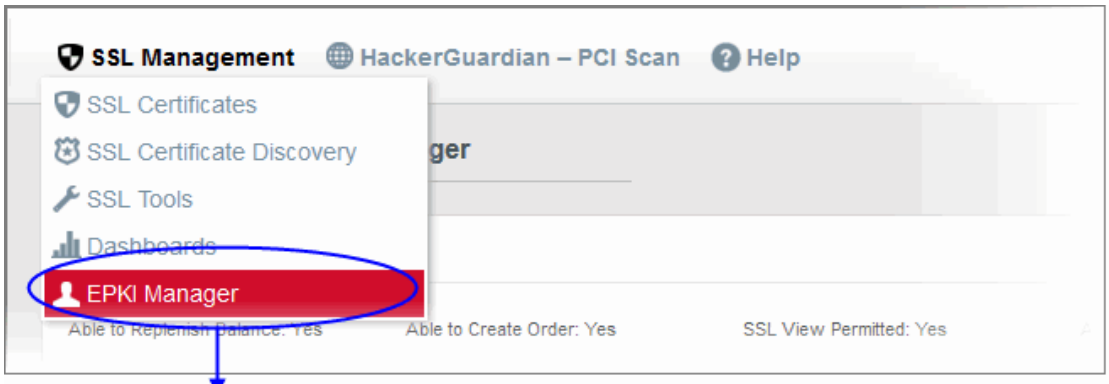
11. EPKI Manager

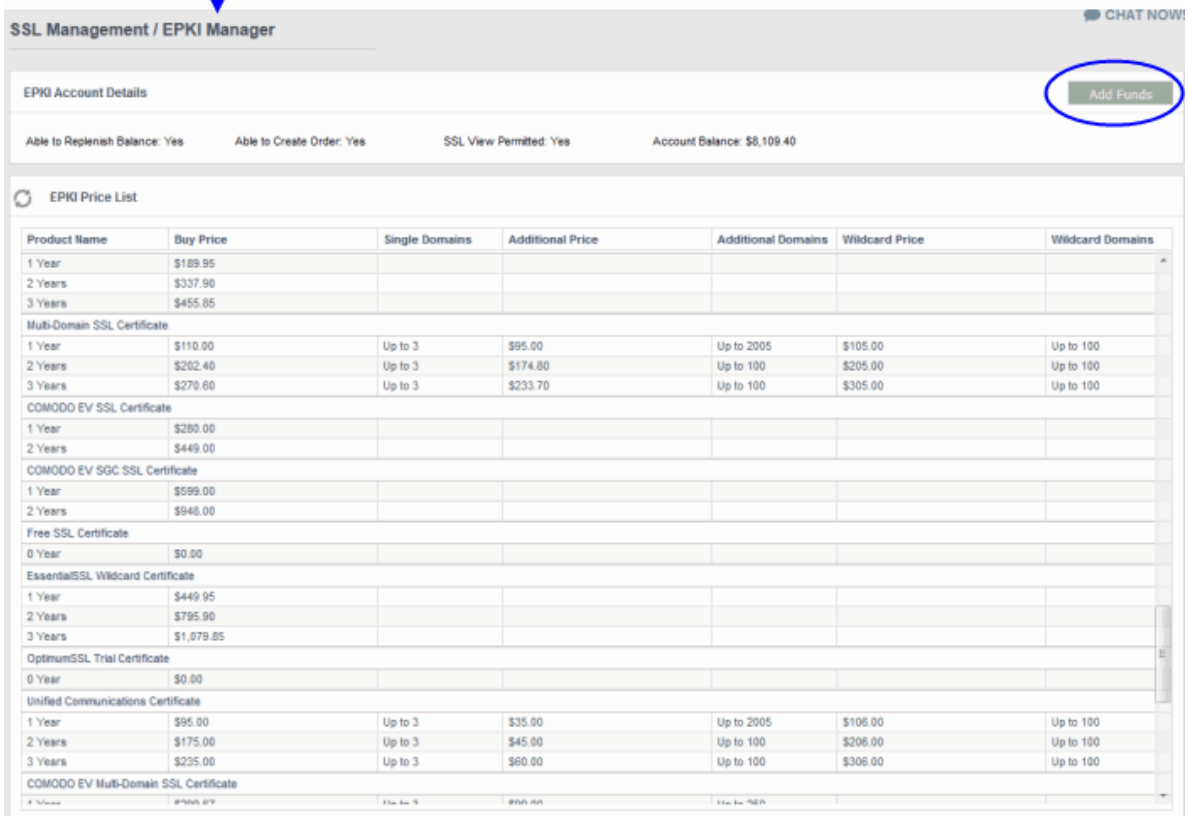
Comodo EPKI accounts allow enterprises to order large volumes of web server and SMIME certificates at discounted prices. **Click here** to read more about the EPKI manager program.

- The 'EPKI Manager' page in S^3 allows EPKI users to view their account balance, view their certificate buy prices and add funds to their account.
- EPKI manager users can log in to S^3 using their existing username, password and one of their order numbers.
- All purchases made in S^3 by EPKI customers will be drawn from available account funds.
- EPKI users can deposit funds by clicking 'SSL Management' > 'EPKI Manager' > 'Add Funds'
- All users that have been added to your EPKI account will also be able to login to S^3. All user permissions will also apply in S^3.

To deposit additional funds

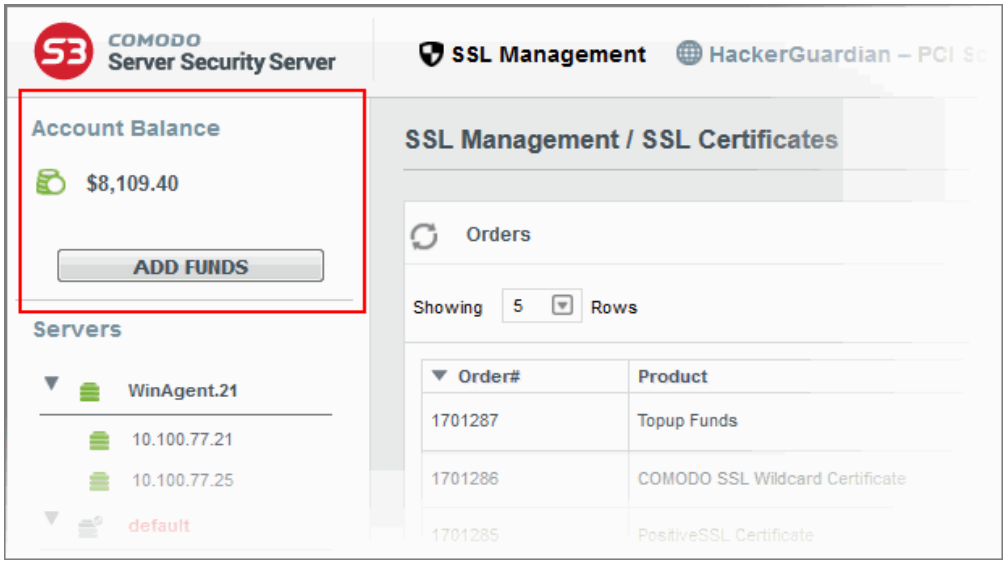
- Click 'SSL Management' > 'EPKI Manager'
- Click the 'Add Funds' button at the top right of the page



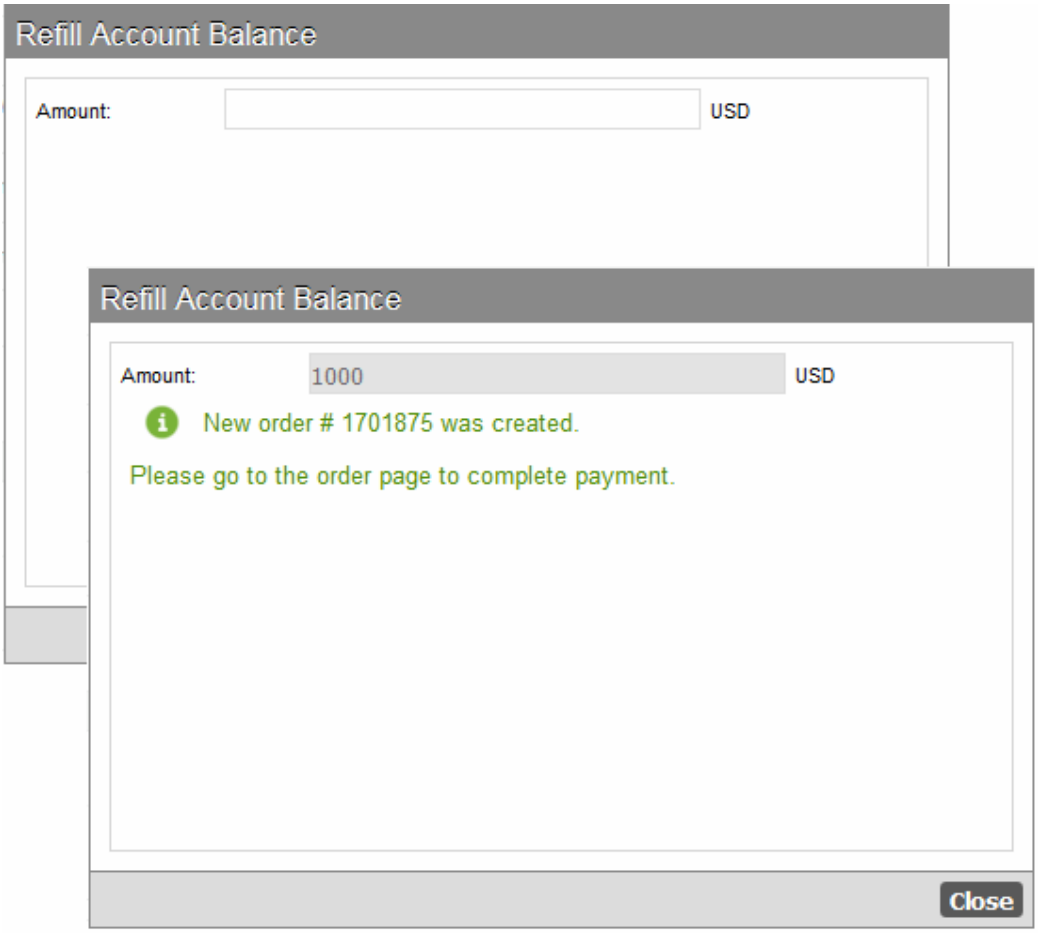


OR

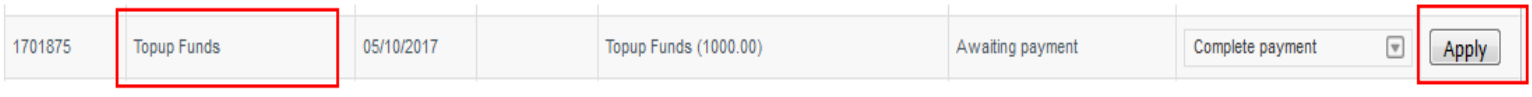
- Click the 'Add Funds' button on the left:



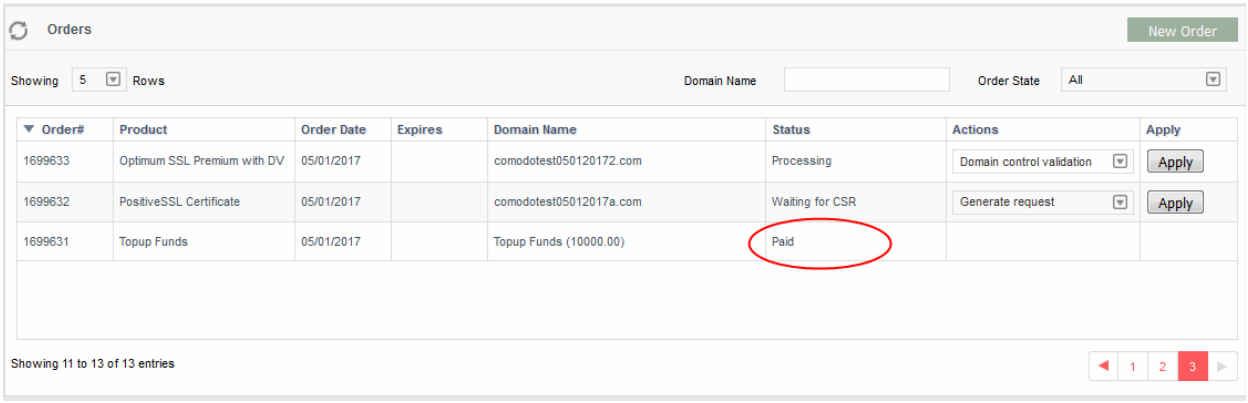
- Type the amount you wish to add in the 'Refill Account Balance' dialog then click 'OK':



- This will create a 'Topup Funds' order in the SSL certificates area with a status of 'Awaiting Payment':
- Go to 'SSL Management' > 'SSL Certificates', locate the 'Topup Funds' order and click the 'Apply' button to complete payment:



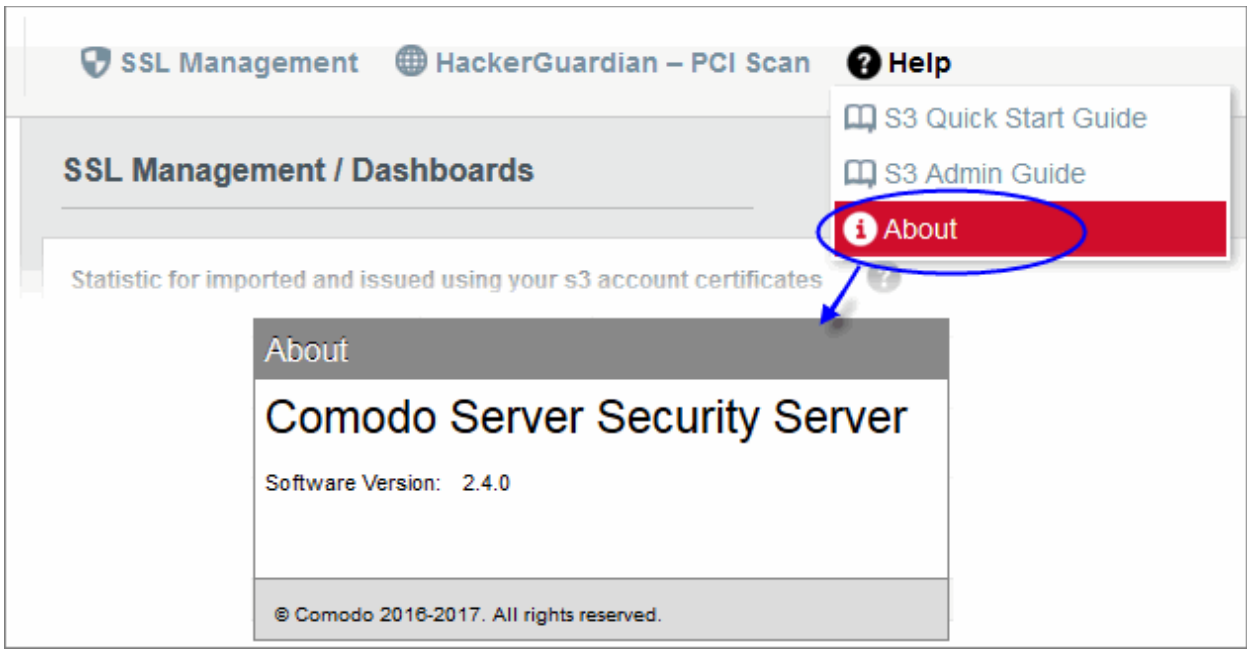
- After payment is complete, the funds will be added to your account. The deposit will be shown as a completed order in the SSL management interface with a status of 'Paid':



12. About S³ and Support Details

The 'Help' menu at the top right of the S³ main interface enables you to access the online help guide and to view the 'About' dialog of the console.

- Click the 'About' from the 'Help' menu to view the S³ version number



About Comodo Security Solutions

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