

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	3
1.1.Login into the Console.....	4
2. The Main Interface / Actions and Statuses	10
3. Tutorial	14
3.1.Add your Servers	14
3.2.Generate and Submit a CSR.....	26
3.3.Complete Domain Control Validation.....	32
3.4.Install or Save Issued Certificate	37
4. Renew a Certificate	39
5. Buy a Certificate	40
6. Complete your Order	43
7. Generate a CSR	47
8. SSL Certificate Discovery Tool	47
9. SSL Tools	50
10. S³ Dashboards	51
11. EPKI Manager	55
12. About S³ and Support Details	57
About Comodo Security Solutions	58

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.

The screenshot displays the Comodo Server Security Server (S³) dashboard. The top navigation bar includes 'SSL Management', 'HackerGuardian - PCI Scan', and 'Help'. The main content area is divided into two sections: 'Orders' and 'Sites'.

Orders Section: This section shows a table of SSL orders. The table has columns for Order#, Product, Order Date, Expires, Domain Name, Status, and Actions. The 'Actions' column includes buttons for 'Complete payment' and 'Generate request'. The 'Status' column shows various states like 'Awaiting payment' and 'Waiting for CSR'.

Order#	Product	Order Date	Expires	Domain Name	Status	Actions
1761267	Topup Funds	05/09/2017		Topup Funds (500.00)	Awaiting payment	Complete payment
1761266	COMODO SSL Wildcard Certificate	05/09/2017		*.abc.com	Waiting for CSR	Generate request
1761265	PositiveSSL Certificate	05/09/2017		www.nuno2.com	Waiting for CSR	Generate request
1761279	PositiveSSL Certificate	05/09/2017		nuno.com	Waiting for CSR	Generate request
1761278	Topup Funds	05/09/2017		Topup Funds (500.00)	Awaiting payment	Complete payment

Sites Section: This section shows a table of SSL sites. The table has columns for Server Name, Site, Binding Information, Certificate, Last Update, and Actions. The 'Actions' column includes buttons for 'Buy Certificate' and 'Renew with Comodo'.

Server Name	Site	Binding Information	Certificate	Last Update	Actions
10.100.77.21	firstfree01.sasgw.in.comodo.od.us	10.100.77.21:80 firstfree01	None	2017/05/08 19:39:03	Buy Certificate
10.100.77.21	Default	*.443:	None	2017/05/08 19:39:03	Buy Certificate
10.100.77.21	asd1gh.sasgw.in.comodo.od.us	10.100.77.21:80 asd1gh.sas	None	2017/05/08 19:39:03	Buy Certificate
10.100.77.21	qafest2.sasgw.in.comodo.od.us	*.4431:	None	2017/05/08 19:39:03	Buy Certificate
10.100.77.21	test123.sasgw.in.comodo.od.us	10.100.77.21:443 test123.s	DN=test123.sasgw.in.comodo.od.us,ST=Alabama (AL),C=US	2017/05/08 19:39:03	Renew with Comodo

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**

- **Login into the Console**
- **The Main Interface / Actions and Statuses**
- **Tutorial**
 - **Add your Servers**
 - **Generate and Submit a CSR**
 - **Complete Domain Control Validation**
 - **Install or Save Issued Certificate**
- **Renew a Certificate**
- **Buy a Certificate**
- **Complete your Order**
- **Generate a CSR**
- **SSL Certificate Discovery Tool**
- **SSL Tools**
- **S³ Dashboard**
- **EPKI Manager**
- **About S³ and Support Details**

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:

Create New' and a red 'Submit' button." data-bbox="216 604 819 886"/>

Comodo S3

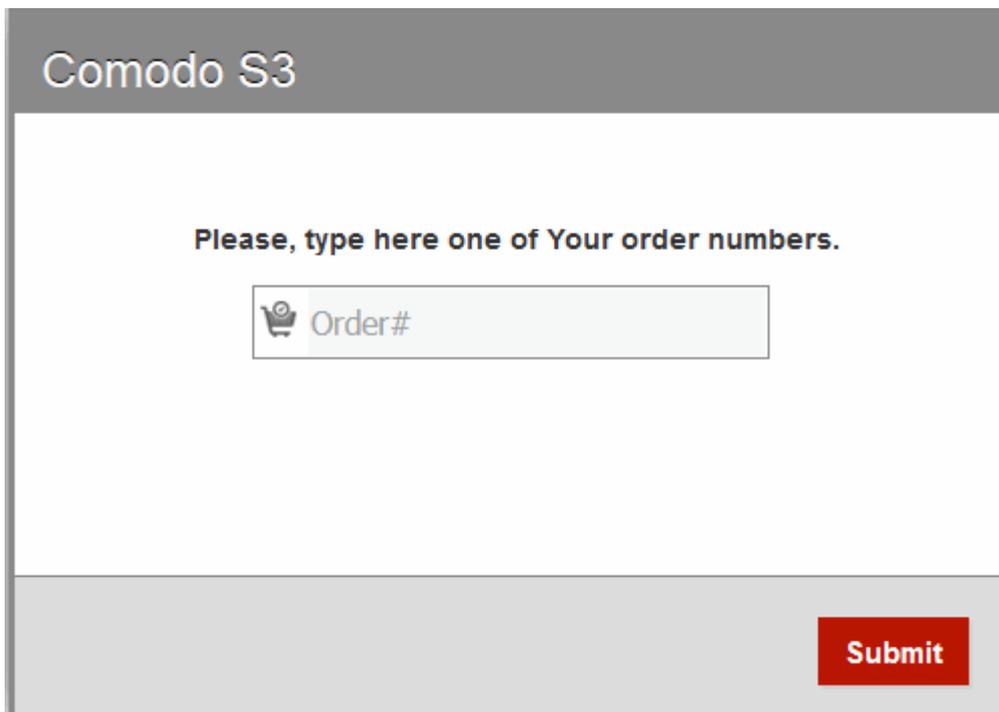
Login

Password

Don't have account? [Create New](#)

Submit

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

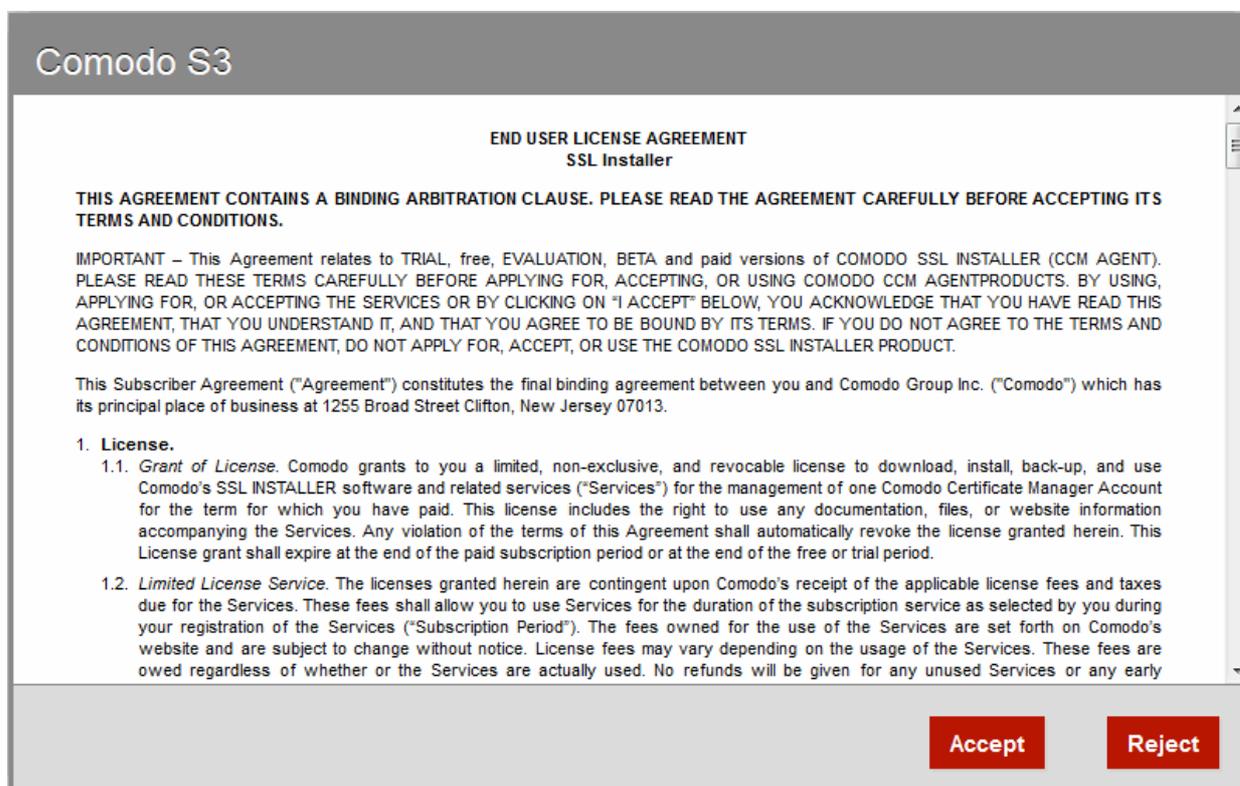


Comodo S3

Please, type here one of Your order numbers.

Submit

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



Comodo S3

END USER LICENSE AGREEMENT
SSL Installer

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.

IMPORTANT – This Agreement relates to TRIAL, free, EVALUATION, BETA and paid versions of COMODO SSL INSTALLER (CCM AGENT). PLEASE READ THESE TERMS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING COMODO CCM AGENTPRODUCTS. BY USING, APPLYING FOR, OR ACCEPTING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE COMODO SSL INSTALLER PRODUCT.

This Subscriber Agreement ("Agreement") constitutes the final binding agreement between you and Comodo Group Inc. ("Comodo") which has its principal place of business at 1255 Broad Street Clifton, New Jersey 07013.

1. License.

1.1. *Grant of License.* Comodo grants to you a limited, non-exclusive, and revocable license to download, install, back-up, and use Comodo's SSL INSTALLER software and related services ("Services") for the management of one Comodo Certificate Manager Account for the term for which you have paid. This license includes the right to use any documentation, files, or website information accompanying the Services. Any violation of the terms of this Agreement shall automatically revoke the license granted herein. This License grant shall expire at the end of the paid subscription period or at the end of the free or trial period.

1.2. *Limited License Service.* The licenses granted herein are contingent upon Comodo's receipt of the applicable license fees and taxes due for the Services. These fees shall allow you to use Services for the duration of the subscription service as selected by you during your registration of the Services ("Subscription Period"). The fees owed for the use of the Services are set forth on Comodo's website and are subject to change without notice. License fees may vary depending on the usage of the Services. These fees are owed regardless of whether or the Services are actually used. No refunds will be given for any unused Services or any early

Accept Reject

- 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 S³ console:

SSL Management / SSL Certificates

Orders

Order#	Product	Order Date	Expires	Domain Name	Status	Actions	Apply
1701287	Topup Funds	05/09/2017		Topup Funds (500.00)	Awaiting payment	Complete payment	Apply
1701286	COMODO SSL Wildcard Certificate	05/09/2017		*.abc.com	Waiting for CSR	Generate request	Apply
1701285	PositiveSSL Certificate	05/09/2017		www.nuno2.com	Waiting for CSR	Generate request	Apply
1701279	PositiveSSL Certificate	05/09/2017		nuno.com	Waiting for CSR	Generate request	Apply
1701278	Topup Funds	05/09/2017		Topup Funds (500.00)	Awaiting payment	Complete payment	Apply

Showing 1 to 5 of 12 entries

Sites

Server Name	Site	Binding Information	Certificate	Last Update	Actions	Apply
10.100.77.21	firstfreessl.saspwin.comodo.od.ua	10.100.77.21:80:firstfreest	None	2017/05/08 19:39:03	Buy Certificate	Apply
10.100.77.21	Default	*.443:	None	2017/05/08 19:39:03	Buy Certificate	Apply
10.100.77.21	asdfgh.saspwin.comodo.od.ua	10.100.77.21:80:asdfgh.sa	None	2017/05/08 19:39:03	Buy Certificate	Apply
10.100.77.21	qatest2.saspwin.comodo.od.ua	*.4431:	None	2017/05/08 19:39:03	Buy Certificate	Apply
10.100.77.21	test123.saspwin.comodo.od.ua	10.100.77.21:443:test123.4	CN=test123.saspwin.comodo.od.ua,ST=Alabama (AL),C=US	2017/05/08 19:39:03	Renew with Comodo	Apply

Showing 1 to 5 of 19 entries

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:



Signup

Company details - These must be your Registered Address

Company Name	<input type="text"/>	
Department	<input type="text"/>	(optional)
Address 1	<input type="text"/>	
Address 2	<input type="text"/>	(optional)
Address 3	<input type="text"/>	(optional)
Zip / Postcode	<input type="text"/>	
Country	<input type="text" value="Select country..."/>	<input type="checkbox"/>
State / Province / Country	<input type="text"/>	
City / Town	<input type="text"/>	
PO Box	<input type="text"/>	(optional)
Company Number	<input type="text"/>	(optional)
DUNS Number	<input type="text"/>	(optional)

Your Contact Details

Title	<input type="text"/>	
First Name	<input type="text"/>	
Last Name	<input type="text"/>	
Email Address	<input type="text"/>	
Telephone Number	<input type="text"/>	
Fax Number	<input type="text"/>	(optional)

Admin Address(Optional)

Next ►

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

Agreement

End User License Agreement

**END USER LICENSE AGREEMENT
SSL Installer**

THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.

IMPORTANT – This Agreement relates to TRIAL, free, EVALUATION, BETA and paid versions of COMODO SSL INSTALLER (CCM AGENT). PLEASE READ THESE TERMS CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING COMODO CCM AGENTPRODUCTS. BY USING, APPLYING FOR, OR ACCEPTING THE SERVICES OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE COMODO SSL INSTALLER PRODUCT.

This Subscriber Agreement ("Agreement") constitutes the final binding agreement between you and Comodo Group Inc. ("Comodo") which has its principal place of business at 1255 Broad Street

I Accept

Next ►

Comodo Certificate Subscriber Agreement

COMODO CERTIFICATE SUBSCRIBER AGREEMENT

IMPORTANT - PLEASE READ THIS CERTIFICATE SUBSCRIBER AGREEMENT CAREFULLY BEFORE APPLYING FOR, ACCEPTING, OR USING A COMODO CERTIFICATE. BY USING, APPLYING FOR, OR ACCEPTING A COMODO CERTIFICATE OR BY CLICKING ON "I AGREE", YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO ITS TERMS. IF YOU DO NOT ACCEPT THIS AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE A COMODO CERTIFICATE AND DO NOT CLICK "I AGREE".

This agreement is between you ("Subscriber") and Comodo CA Limited ("Comodo"), a United Kingdom company. The agreement governs your application for and use of an SSL Certificate issued from Comodo. You and Comodo agree as follows:

1. Subscription Service.

1.1. Issuance. Upon Comodo's acceptance of Subscriber's application for a Certificate, Comodo shall attempt to validate the application information in accordance with the Comodo CPS and, for EV

I Agree

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

Summary

Admin Credentials

Login	<input type="text"/>	<p>All passwords must contain at least 8 characters. Password cannot have a space as the first character. Three out of the following five requirements must be met: At least one uppercase alpha character. At least one lowercase alpha character. At least one numeric character. At least one punctuation character. At least one non-ASCII character.</p>
Password	<input type="password"/>	
Confirm Password	<input type="password"/>	

Company Details

Company Name	LA Oldfashion Cuisine
Address 1	8400 Santa Monica Blvd, West Hollywood
Zip / Postcode	90069
Country	United States of America
State / Province / Country	CA
City / Town	Los Angeles

Your Contact Details

Title	Mr
First Name	Peter
Last Name	Johnson
Email Address	johnson.peter38@gmail.com
Telephone Number	(323)012-3456

Submit

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

Signup completed

Congratulations!

Your S³ account has been created successfully!

Your order number is **1701926**

You can now login at <https://s3.comodo.com/web> with your username, password and the order number mentioned above.

Click OK to automatic login into S3

OK

- **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.
- 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' then 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 S³ 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 screenshot shows the 'SSL Management' interface. Callout boxes provide the following information:

- Order large volumes of web server and SMIME certificates, deposit additional funds:** Points to the 'Account Balance' section on the left.
- Click 'Manage Servers' to download the agent required to set up new servers:** Points to the 'MANAGE SERVERS' button.
- All your Comodo certificate orders appear in the upper pane:** Points to the 'Orders' table.
- 'Status' tells you where your certificate is in the ordering and installation processes:** Points to the 'Status' column in the 'Orders' table.
- The actions you can take depend on the certificate status:** Points to the 'Actions' column in the 'Orders' table.
- Chat with Comodo support:** Points to the 'CHAT NOW' button.
- Important notifications, e.g. certificate expiry, are shown on the left:** Points to the 'Alerts' section.
- Click to switch between SSL Management, Certificate Discovery, SSL tools, the Dashboard and the EPKI Manager:** Points to the navigation tabs at the top.
- The lower pane shows all web-sites and certificates discovered and bookmarked on your servers. Certificates issued by CAs other than Comodo are shown in red:** Points to the 'Sites' table.
- These actions allow you to replace and renew discovered certificates:** Points to the 'Actions' column in the 'Sites' table.

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
<p>Awaiting Payment</p> <p>Your order has been placed with Comodo, but payment has not yet been received.</p> <p>Please complete payment for order processing to continue.</p>	Complete Payment
<p>Waiting for CSR</p> <p>A certificate order has been created but a corresponding CSR has not been imported to the auto-installer nor submitted to Comodo CA. You must submit a CSR for your domain to start the certificate application and issuance processes.</p>	Generate request Request Invoice
<p>Processing</p> <p>CSR has been submitted and received. Comodo CA is now processing the order and validating the application. Note – you must next complete Domain Control</p>	Domain Control Validation Replace CSR

Certificate Status	Available Actions
<p>Validation (DCV) before your certificate can be issued.</p> <p>Note - If your status is 'Processing' but you have completed the CSR and domain validation (DCV) processes, it is usually because Comodo are still completing organization validation. Please check the interface regularly to see if your certificate has been issued. Please allow up to 1 week for EV certs and 2 days for OV certs.</p>	Request Invoice
<p>Issued</p> <p>Certificate has been issued by Comodo CA and is awaiting further actions. Certificate status will change to 'Issued' if your CSR has been accepted AND the DCV check is successful.</p>	Auto-install certificate Save Certificate Renew Certificate Installation Check Request Invoice
<p>Installed</p> <p>Certificate has been successfully installed.</p>	Auto-install certificate Save Certificate Renew Certificate Request Invoice
<p>Paid</p> <p>Only relevant to EPKI users. Indicates that funds have been successfully added to your account.</p>	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.

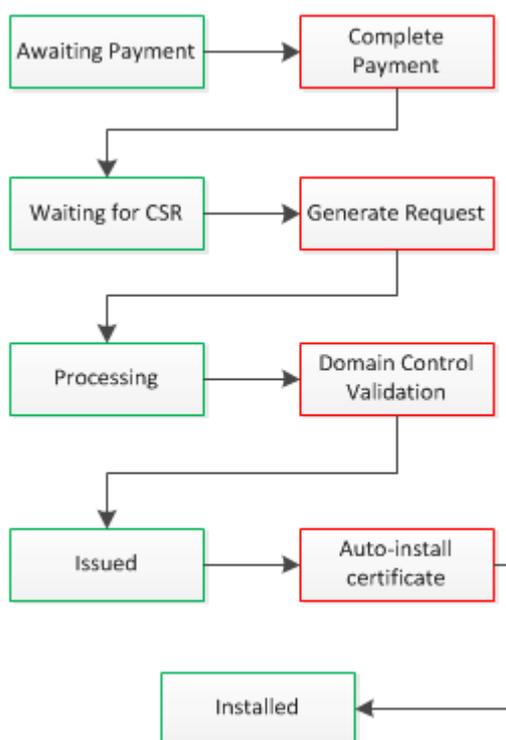
Save Certificate

- 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:

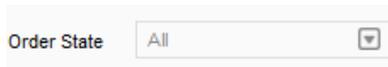


Refreshes the list of certificate orders or sites.



New Order

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



Order State All

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



CHAT NOW!

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:

The screenshot shows the Comodo Server Security Server interface. On the left, there's a sidebar with 'Account Balance' (\$8,109.40), 'Servers' (listing WinAgent.21 and default), and a 'MANAGE SERVERS' button circled in red. The main area shows 'SSL Management / SSL Certificates' with an 'Orders' table containing three rows: 1699633 (Optimum SSL Premium with DV), 1699632 (PositiveSSL Certificate), and 1699631 (Topup Funds). Below this is a 'Manage Agents and Servers' modal window. In this modal, the 'Add New Agent/Server' button is circled in red, with a red arrow pointing from the 'MANAGE SERVERS' button. The modal contains two tables: 'Agents' and 'Servers'. The 'Agents' table has columns for State, Agent Name, Agent UID, Agent Version, OS Info, Creation Date, Edit, and Remove. It lists 'WinAgent.21' and 'default'. The 'Servers' table has columns for State, Server Name, Agent Name, OS Info, Framework Version, IIS Version, and Creation Date. It lists two servers: 10.100.77.21 and 10.100.77.25. Below the tables, there are instructions on how to add a server to the list, including steps for registering a new agent and registering a server with an agent. A 'Close' button is at the bottom right of the modal.

- 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

Agent Download ?

Agent Name:

Agent UID: 289dff07669d7a23de0ef88d2f7129e7

Download agent from

Agent running on:	Web UI Support	Apache Support	Tomcat Support	IIS Support	Download
Linux:					
Debian x86 compatible	yes	yes*	yes	no	download
Debian x64 compatible	yes	yes*	yes	no	download
RedHat x86 compatible	yes	yes*	yes	no	download
RedHat x64 compatible	yes	yes*	yes	no	download
Windows:					
Windows agent	yes	yes**	yes	yes***	download
Windows Utility	no	yes**	yes	yes***	download

* Apache server installed on linux based OS
** Apache server installed on remote PC with linux OS
*** Local IIS server installed on the same PC with agent software

- Create a name for Your agent, download the installer for Your OS then click "Save" to register the agent in the "Manage Agents" interface.
- Install one agent on each network where You have servers You wish to manage.
- The agent will control certificate installations and can be installed on any Windows or Linux machine.
- Once running, the agent will provide You with a one-time verification code. You should:
 - 1) Copy the code as it will need to be entered on the "Manage Servers" screen.
 - 2) On the "Manage Servers" screen in S3 and click the "Verify Agent" button.
 - 3) Paste the code then click the "Start Verification" button.
 - 4a) Windows agent - click the "Finish Verification" button on the agent dialog.
 - 4b) Linux agent - press 'y' in console to finish verification

OK

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

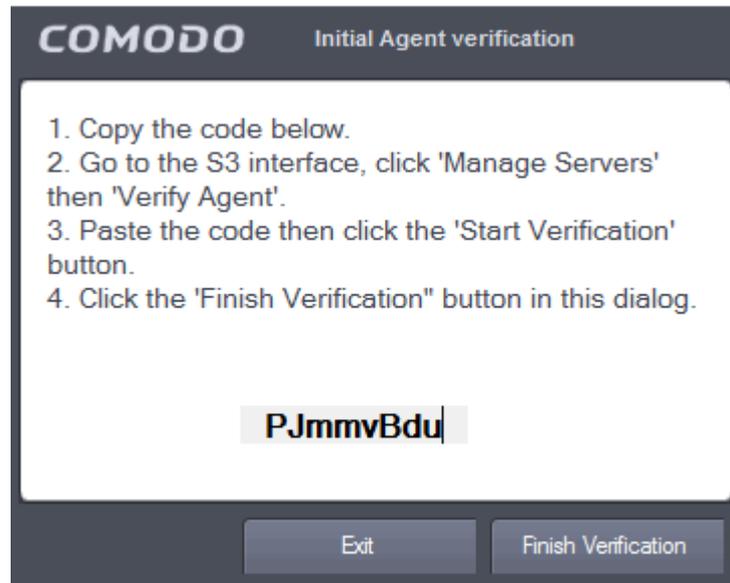
Managing agents and servers

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:

Manage Agents and Servers								
Add New Agent/Server								
Agents								
State	Agent Name	Agent UID	Agent Version	OS Info	Creation Date	Edit	Remove	
■	WinAgent.21	28f0b864598a1291557bed248a998d4e	Windows agent 1.1.050517	Microsoft Windows NT 6.2.9200.0Framework Version: 4.0.30319.34014, IIS Version: IIS8.5	05/01/2017 20:22			
○	default	41ae36ecb9b3eee609d05b90c14222fb	undefined		05/09/2017 15:18			Verify agent

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

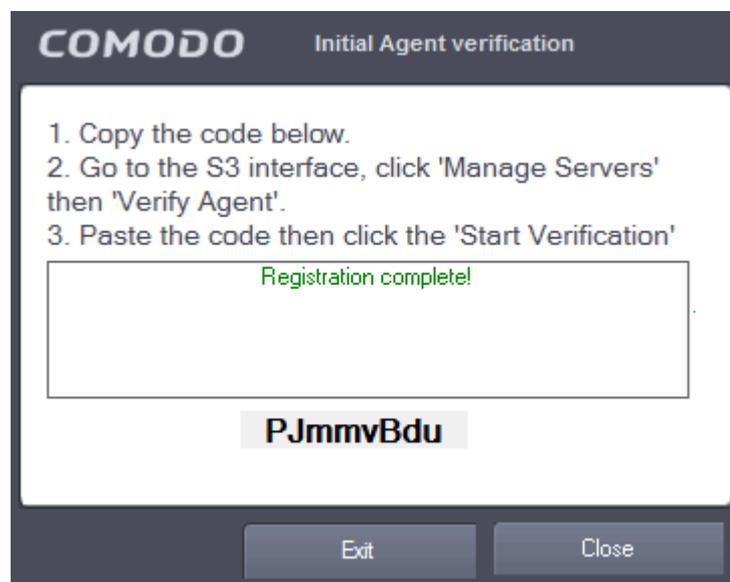
Agent Verification

Agent Key:

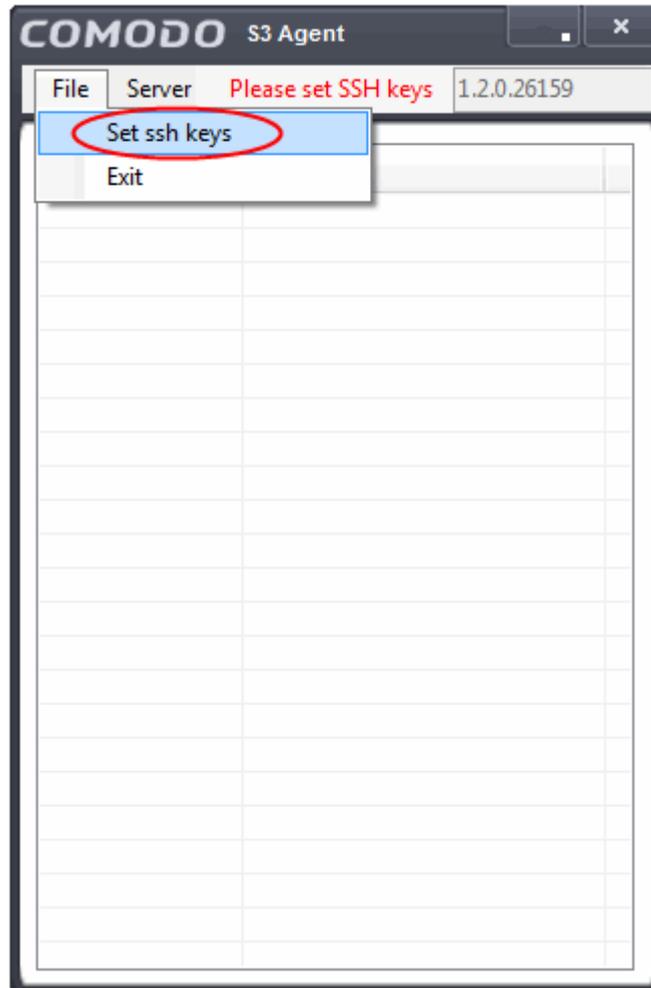
1. Start the agent if You haven't done so already to get the verification code.
2. Copy and paste the code into the field above.
3. Click the 'Start Verification' button.

Start Verification **Back**

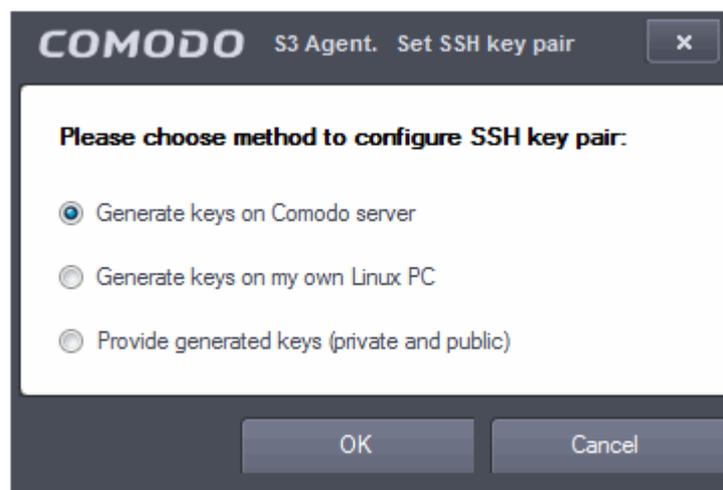
- Next, go back to the agent verification dialog on your Windows machine and click 'Finish Verification'. The verification dialog will confirm whether your registration was successful:



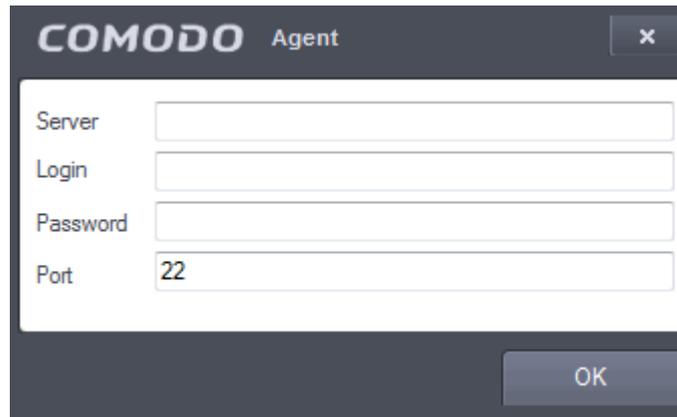
- Click 'Close'. The S³ Agent dialog will open
- Select 'Set ssh keys' from the 'File' menu or choose 'Please set SSH keys'



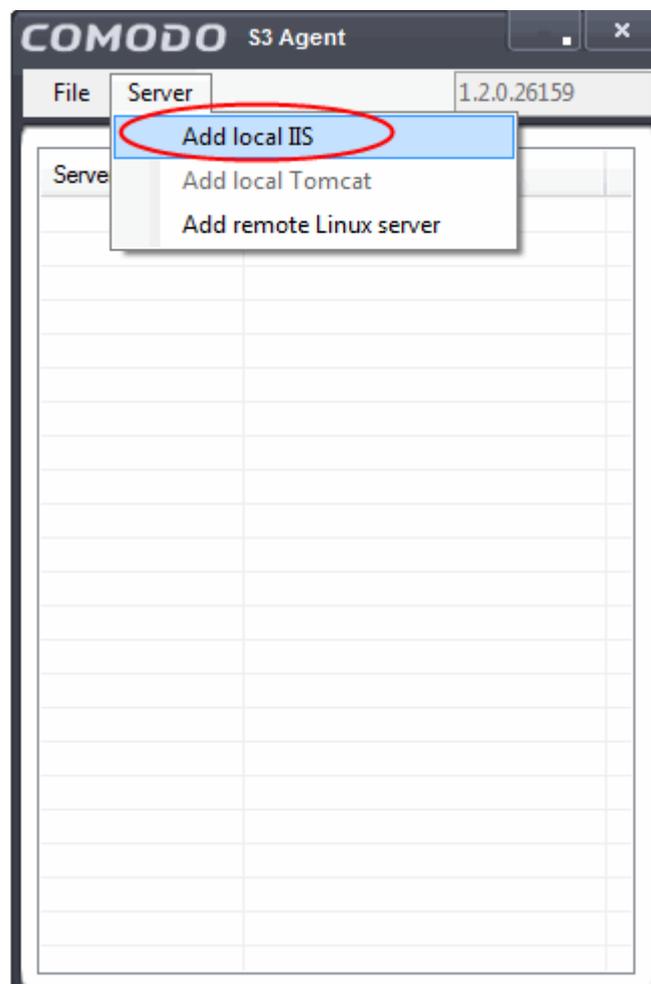
You can configure the SSH key pair in three ways:



- 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



Agent Verification

Agent Key:

1. Start the agent if You haven't done so already to get the verification code.
2. Copy and paste the code into the field above.
3. Click the 'Start Verification' button. |

 Agent 'Windows agent' Authentication successful. Your agent IP is: 10.100.76.101

[Back](#)

- 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:

COMODO Server Security Server

Account Balance

\$8,109.40

ADD FUNDS

Servers

- WinAgent.21
 - 10.100.77.21
 - 10.100.77.25
- default

MANAGE SERVERS

Alerts

No more alerts found

MORE ALERTS

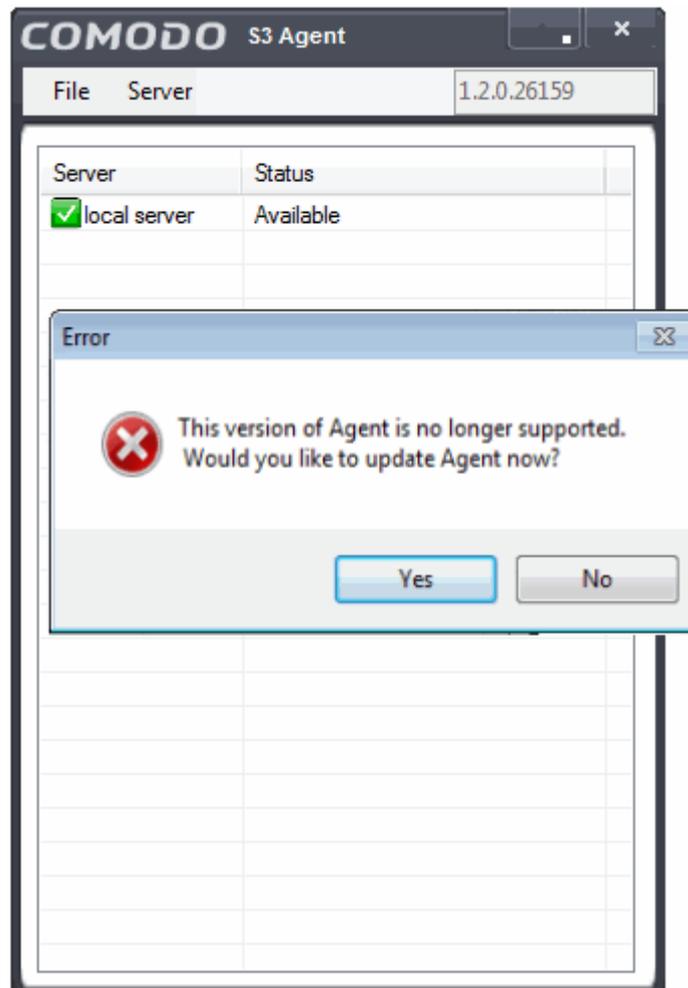
Server statuses:

- 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:

Manage Agents and Servers Add New Agent/Server

Agents

State	Agent Name	Agent UID	Agent Version	OS Info	Creation Date	Edit	Remove
●	WinAgent.21	28f0b064596a1291557bed246a96d4e	Windows agent 1.1.050517	Microsoft Windows NT 6.2.9200 (Framework Version: 4.0.30319.34014, IIS Version: IIS8.5	05/01/2017 20:22		
○	default	41ae36ecb9b3ee608d05b90c14222fb	undefined		05/09/2017 15:18		

[Verify agent](#)

Servers

State	Server Name	Agent Name	OS Info	Framework Version	IIS Version	Creation Date
●	10.100.77.21	WinAgent.21	Microsoft Windows NT 6.2.9200.0	4.0.30319.34014	IIS8.5	05/08/2017 16:04
●	10.100.77.25	WinAgent.21	CentOS release 6.8 (Final) LSB_VERSION=base- 4.0-ia32:base- 4.0-noarch:core- 4.0-ia32:core- 4.0-noarch:graphics- 4.0-ia32:graphics- 4.0-noarch:printing- 4.0-ia32:x11font-4.0-noarch			05/08/2017 16:04

To add your server to this list, do the following:

- Register new agent:
 1. If you have S3 agent already installed in your network - go to step 2. Otherwise - download an agent by clicking on "Add new agent".
 2. Run this agent on any corresponding machine in your network. During first run, the agent will generate verification code. See more detailed instructions here
 3. After getting this verification code - come back to "Manage Servers" page and click on corresponding "Verify agent" button and insert verification code
- Register a server with agent, see detailed instructions:
 - [for windows agent](#)
 - [for linux agent](#)

[Close](#)

- 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'

Orders New Order

Showing 5 Rows Order State: All

Order#	Product	Order Date	Expires	Domain Name	Status	Actions	Apply
689033	COMODO SSL Certificate	03/14/2017	03/14/2017	hotoh.com	Expired		Apply
689032	Unified Communications Certificate	03/14/2017		busong.com, admin.busong.com, busong.org, ...	Waiting for CSR	Generate request	Apply
689031	COMODO SSL Wildcard Certificate	03/14/2017		*.domenfirst.com	Awaiting payment	Complete payment	Apply
689030	COMODO EV SSL Certificate	03/14/2017		firstflowers.com	Awaiting payment	Complete payment	Apply
689028	InstantSSL Certificate	03/14/2017		unpod.com	Processing	Domain control validation	Apply

Showing 1 to 5 of 5 entries 1

The 'Generate Request' form will open:

Generate Request ?

Generation Options Generate CSR Paste CSR

Domain Details

Common name: Domain list:
 Multidomain

Organization: Organizational unit:
Country/Region: State/Province:
City/Locality: E-mail:

Make private key exportable

Generate CSR on server:

Generation Result

Summary

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.

?
Generate Request

Generation Options

 Generate CSR
 Paste CSR

Your CSR

```
-----BEGIN CERTIFICATE REQUEST-----
BJp8d3zHJ/pgzYz1Xgx9WAdcr7zBcXYWtIfJVrKvhuA1E1yNExxAsNaikLi2RrHb
Xfrnbq5jEy0/76teUiyblwI2IbgIzSy4ivuUiZZ7gMzdyOjJKrDc4zwLIOMlqF0V
brO2FIspFkNR/1GuXh70SwTxIQJZzhjPGbeqmG/EJLwjYNseSqJgLmT2/FVTkUDsS
qDV2ISN+gI9jrNgpX6W1AgMBAAAggggERMBogCisGAQQBgjcNAgMxDBYKNi4xLjc2
MDEuMjA+BgkqhkiG9w0BCQ4xMTAvMB0GA1UdDgQWBQB1B7Di+suxgrInIt9BD38Z
TSw9HDAOBgNVHQ8BAf8EBAMCBSAwSwYJKwYBBAAGCNxUUMT4wPAIBBQwObWF4LXdP
bi10ZXN0cGMMFG1heC13aW4tdGVzdHBjXG1heGltDBFDb21vZG9TM0FnZW50LmV4
ZTBmBgorBgEEAYI3DQICMVgwVgIBAR5OAE0AaQBjAHIAbwBzAG8AZgB0ACAAUwB0
AHIAbwBuAGcAIABDAHIAeQBwAHQAAbwBnAHIAIYQBWAGGAaQBjACAAUABYAG8AdgBp
AGQAZQByAwEAMA0GCsqGS1b3DQEBBQUAA4IBAQAixTVCe8dQk59IOaq2WrBMJSa
Z+gsxMK0fXVwIDH4RiUQp6+98c6cyNBBGXl/oiLqcbegr/xAtM+Qr9qnz5DYKJKo
a0NuNmXvKDadGUmDgZ0facz/XxRP22AgR0nDym+4f1XW2Jf1x7Ob+RJRxcQ3bOw
MMVtZ92rmkjilFDStyx9YFgk9V7k40frcXVg62tw500zWtWRUIM5mmzbsSIWk4MS
rXHH4sgLedeijvIp804YAlYw9IHjPE1g8CDLBSSTNdfccbU5jV3vLHJPsnz8khSFA
QrvvP2wap0XHzTLsAGvycqntSggA1Jla0c2/aYd4DuK8voEP8upN0jy/E+0J
-----END NEW CERTIFICATE REQUEST-----
```

Domain Details

Common name:	firstflowers.com	Organization:	Unpod
Domain list:	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	Organizational unit:	Unpod
		Country/Region:	United State of America
		State/Province:	n/a
		City/Locality:	Montana
		E-mail:	flowerspurchase@gmail.com

Summary

Send
Validate & parse
Clear
Cancel

- 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:

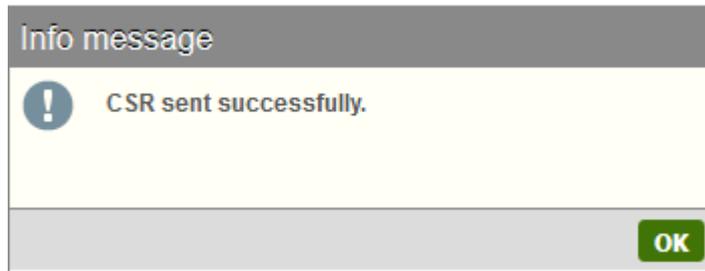
Domain Details

- 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



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':

The screenshot shows the "Orders" management interface. It features a table with columns for Order#, Product, Order Date, Expires, Domain Name, Status, Actions, and Apply. The "Domain control validation" option in the Actions column for the "InstantSSL Certificate" row is circled in red.

Order#	Product	Order Date	Expires	Domain Name	Status	Actions	Apply
689033	COMODO SSL Certificate	03/14/2017	03/14/2017	hotoh.com	Expired		Apply
689032	Unified Communications Certificate	03/14/2017		busong.com, admin.busong.com, busong.org, ...	Waiting for CSR	Generate request	Apply
689031	COMODO SSL Wildcard Certificate	03/14/2017		*.domenfirst.com	Awaiting payment	Complete payment	Apply
689030	COMODO EV SSL Certificate	03/14/2017		firstflowers.com	Awaiting payment	Complete payment	Apply
689028	InstantSSL Certificate	03/14/2017		unpod.com	Processing	Domain control validation	Apply

This will open the DCV configuration interface:

Domain Control Validation

Domains List

Domain	Status
unpod.com	No Domain Control Validation method selected.

Method of Domain Control Validation

Email Addresses
 Alternative method of DCV
 None of the above

Registered Email Addresses (from WHOIS)

Level 2 Email Addresses

admin@unpod.com
 administrator@unpod.com
 hostmaster@unpod.com
 postmaster@unpod.com
 webmaster@unpod.com

Please enter a validation code that was received via email:

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.

Domain Control Validation ?

Domains List

Domain	Status
firstflowers.com	No Domain Control Validation method selected.

Method of Domain Control Validation

Email Addresses

Alternative method of DCV

None of the above

Registered Email Addresses (from WHOIS)

fi1120049244@whoisprivacyservices.domains

fi1120049243@whoisprivacyservices.domains

Level 2 Email Addresses

admin@firstflowers.com

administrator@firstflowers.com

hostmaster@firstflowers.com

postmaster@firstflowers.com

webmaster@firstflowers.com

Please enter a validation code that was received via email:

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:

Please enter a validation code that was received via email:

45uKQH1Iy2QW3xUKlly1y3dbNeCjilog

- 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:

Domain Control Validation

Domains List

Domain	Status
unpod.com	No Domain Control Validation method selected.

Method of Domain Control Validation

Email Addresses

Alternative method of DCV

None of the above

HTTP CSR Hash

HTTPS CSR Hash

CNAME CSR Hash

MD5: 3B410C326180BFEAC5ECE2BBF07B3C05

SHA1: ACF5489B76502D0FE03A15A247DDA13A3AE98168

Domain Control Validation file 3B410C326180BFEAC5ECE2BBF07B3C05.txt for domain unpod.com will be created on server 10.100.77.113 on your desktop at the following folder: Comodo_AI/unpod.com/dcv/

Create file & submit **Create file** **Submit** **Close**

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	<p>Location: <a href="http[s]://<Authorization Domain Name>/.well-known/pki-validation/<MD5 hash>.txt">http[s]://<Authorization Domain Name>/.well-known/pki-validation/<MD5 hash>.txt</p> <p>.txt file name: <md5 hash>.text</p> <p>.txt file contents: SHA-256 hash comodoca.com Unique value</p> <p>Note – The 'Unique value' is optional and can be omitted if not supplied.</p>
Example	<p>http[s]://example.com/.well-known/pki-validation/C7FBC2039E400C8EF74129EC7DB1842C.txt</p> <p>Text file contents</p> <p>c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f comodoca.com 10af9db9tu</p>

- 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

Automatic Installation ?

Domain: ▼

Server: ▼

Sites

Site	Binding	Path	Permission
firstdomen.com	*:443	/usr/SSL/firstdomen.com/firstdomen.com.crt	✓

Continue **Cancel**

- 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-down, choose 'Save certificate' and click 'Apply'
- Define the target server in the 'Server' drop-box

Save Certificate

Domain: firstflowers.com

Server:

Your certificate will be placed on server 10.100.77.113 on your desktop at the following folder: \\Comodo_AIfirstflowers.com\

- Click 'Save'

Info message

! Certificate successfully saved on server 10.100.100.100 by path: ~/Comodo_AI/testnamewebsite1.com/testnamewebsite1.com_1631285.zip.

- 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'

Order#	Product	Order Date	Expires	Domain Name	Status	Actions	Apply
689034	COMODO SSL Certificate	03/14/2017		firstflowers.com	Processing		
689033	COMODO SSL Certificate	03/14/2017	03/14/2017	hotoh.com	Expired	Renew certificate	<input type="button" value="Apply"/>
689032	Unified Communications Certificate	03/14/2017		busong.com, admin.busong.com, busong.org, ...	Processing	Domain control validation	<input type="button" value="Apply"/>
689031	COMODO SSL Wildcard Certificate	03/14/2017		*.domenfirst.com	Awaiting payment	Complete payment	<input type="button" value="Apply"/>
689030fsup	COMODO SSL Certificate	03/14/2017		firstflowers.com	Processing		

Showing 1 to 5 of 7 entries

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

Server Name	Site	Binding Information	Certificate	Last Update	Actions	Apply
10.100.13.13	firstfreessl.com	10.100.13.13:443:firstfree	CN=testSSLfirstfreessl,ST=Alabama (AL),C=US	2017/03/14 10:43:53	Renew with Comodo	Apply
10.100.77.113	coese.com	*:80:coese.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	assilo.com	*:80:assilo.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	hotoh.com	*:80:hotoh.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	busong.com	*:80:busong.com	None	2017/03/14 10:43:53	Buy Certificate	Apply

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

Type	Server Name	Detected Certificate	Valid From	Valid To	Subject	Last Update	View	Delete	Renew
	10.100.77.113	firstflowers.com	03/14/2017	03/14/2019	1.2.840.113549.1.9.1=#1618526f626572746f4066697273746666	2017/03/14 15:00:48	Q		Renew
	199.66.206.224	www.instantssl.com	06/12/2015	06/12/2017	CN=www.instantssl.com,OU=COMODO EV SGC SSL,OU=COMODO EV SSL,O=Comodo CA Ltd,STREET=3rd Floor,STREET=26 Office Village,STREET=Exchange Quay, Trafford Road,L=Salford,ST=Greater Manchester,2.5.4.17=#13064d3520334551,C=GB,2.5.4.15=#131	2017/03/14 15:01:02	Q	X	Renew

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**

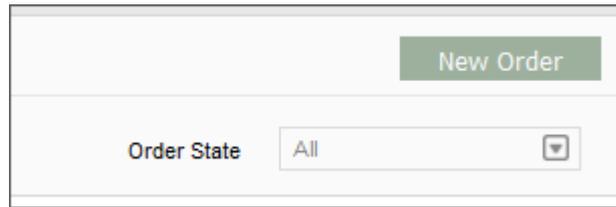
5. Buy a Certificate

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

Server Name	Site	Binding Information	Certificate	Last Update	Actions	Apply
10.100.77.113	tecup.com	*:80:tecup.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	coese.com	*:80:coese.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	assilo.com	*:80:assilo.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	hotoh.com	*:80:hotoh.com	None	2017/03/14 10:43:53	Buy Certificate	Apply
10.100.77.113	busong.com	*:80:busong.com	None	2017/03/14 10:43:53	Buy Certificate	Apply

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

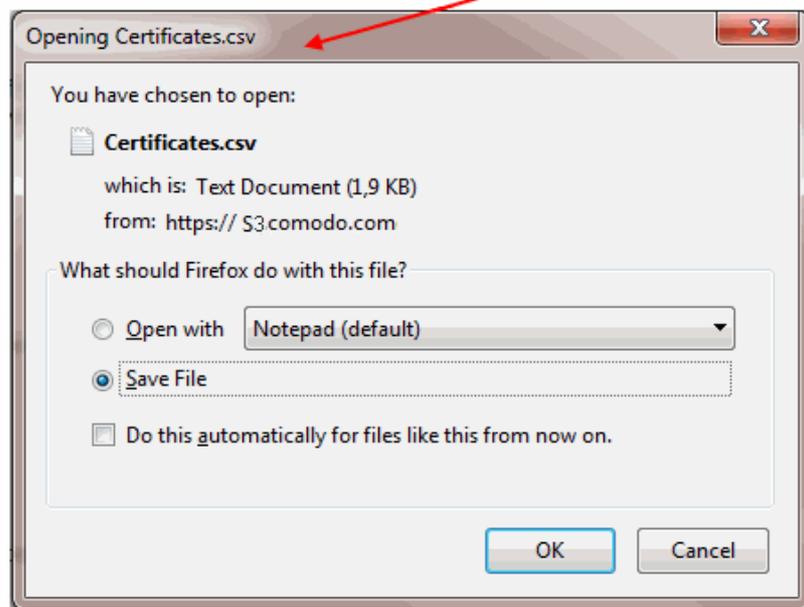
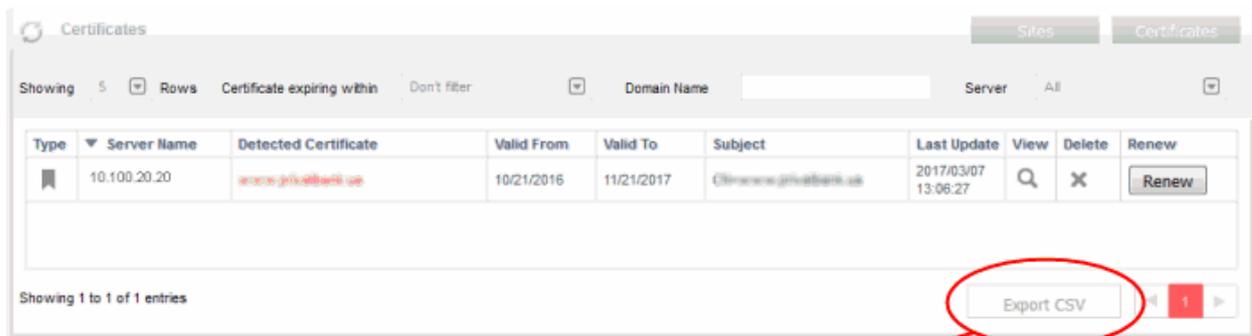


In either case, the 'Create new order' form will open. Refer to **Completing your Order** to move onto the next step.

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'

The screenshot displays the 'SSL Management / SSL Certificate' section of the Comodo Server Security Server interface. On the left, there is a sidebar with 'Account Balance' (\$8,109.40), 'Servers' (WinAgent.21, 10.100.77.21, 10.100.77.25, default), and 'ADD FUNDS' and 'MANAGE SERVERS' buttons. The main area shows an 'Orders' table with columns for Order#, Product, and Actions. The 'Request Invoice' action for order 1701120 is highlighted, and its 'Apply' button is circled in red. A modal form titled 'Request Invoice' is open, with a red arrow pointing to it from the circled button. The modal form contains fields for 'Your email' (pre-filled with 'emailaddress@gmail.com'), 'Additional emails', 'VAT', and 'Note', along with 'Submit' and 'Cancel' buttons.

Order#	Product	Actions	Apply
1701278	Topup Funds	Complete payment	Apply
1701128	PositiveSSL Certificate	Generate request	Apply
1701120	PlatinumSSL Legacy Wildcard Certificate	Generate request Request Invoice	Apply
1701110	Topup Funds	Complete payment	Apply
1699644	Topup Funds	Complete payment	Apply

Request Invoice

Your email:

Additional emails:

VAT:

Note:

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.

Create new order ?

Account Details

Note: fields ending with "*" are required

Email *	testflowerssite.com
Organization *	S3 Demo EPKI
Organization Unit Name *	IT
Address *	1255 Broad Street
Address 2	
Address 3	
PO BOX	
Locality Name *	Clifton
Country Code *	United States of America <input type="checkbox"/>
State or Province *	NJ
Postal Code *	07013

[Prev](#) [Next](#) [Cancel](#)

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:

Create new order ?

Summary

Your Order

Product: PositiveSSL Certificate

Term: 2 years: \$45.95/yr. Save 8%

Primary Domain: testflowerssite.com

Total Domains: 1

DCV Method: Manual

Voucher: Not used

Total (excluding taxes): \$91.90

[Prev](#) [Place Order](#) [Cancel](#)

- 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:

[Logout](#)

Secure Payment

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:

Welcome:
Cert Installer
AI Development

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

Telephone:
+1.888.266.6361
+1.703.681.6361

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

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:

Status	Actions	Apply
Waiting for CSR	Generate request	Apply
Awaiting payment	Complete payment	Apply
Awaiting payment	Complete payment	Apply
Processing	Domain control validation	Apply
Processing	Domain control validation	Apply

Navigation: < 1 2 3 4 5 6 7 8 >

Generate CSR on server:	10.100.77.98
-------------------------	--------------

[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

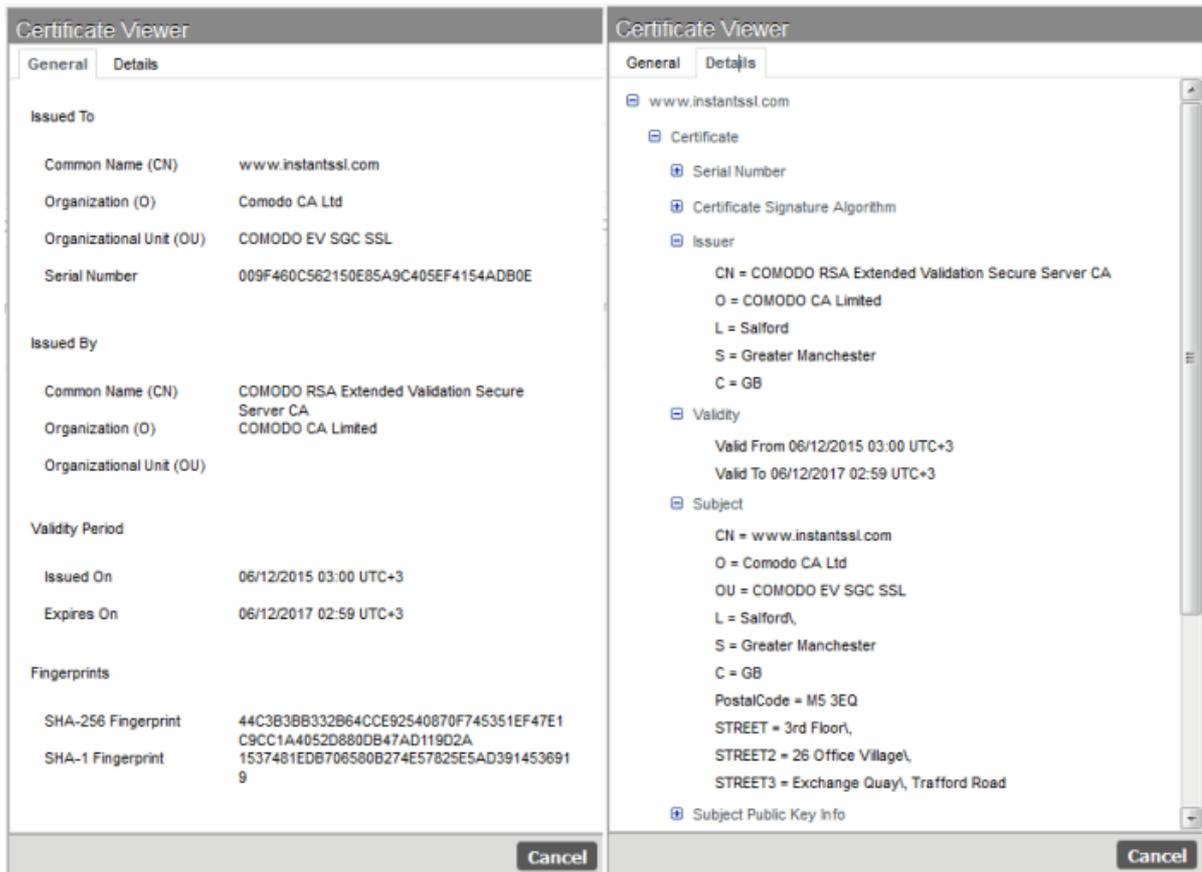
- Choose 'External' or 'Internal' discovery as required
- For internal scans you will need to select an agent from the drop-down
- Enter your IP range and subnet mask in the boxes provided
- Click the 'Start Scan' button at the top-right
- The results table will show all certificates currently deployed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

The screenshot shows the 'SSL Management' dashboard. A dropdown menu is open, with 'SSL Certificate Discovery' highlighted in red. A blue arrow points from this menu item to the 'Certificates' section of the main interface. The 'Certificates' section displays a table with the following data:

Server Name	Detected Certificate	Validity	From	To	Subject	View	Actions	Apply
199.66.206.224	www.instantssl.com	●	06/12/2015	06/12/2017	CN=www.instantssl.com,OU=COMODO EV SGC SSL,OU=COMODO EV SSL,D=Comodo CA Ltd,STREET=3rd Floor, STREET=26 Office Village, STREET=Exchange Quay, Trafford Road,L=Salford,ST=Greater Manchester,2.5.4.17=#13064d3520334551,C=GB,2	🔍		

At the bottom of the table, it says 'Showing 1 to 1 of 1 entries'. There are also buttons for 'Export CSV' and 'Bookmark Certificate(s)'.

- 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.

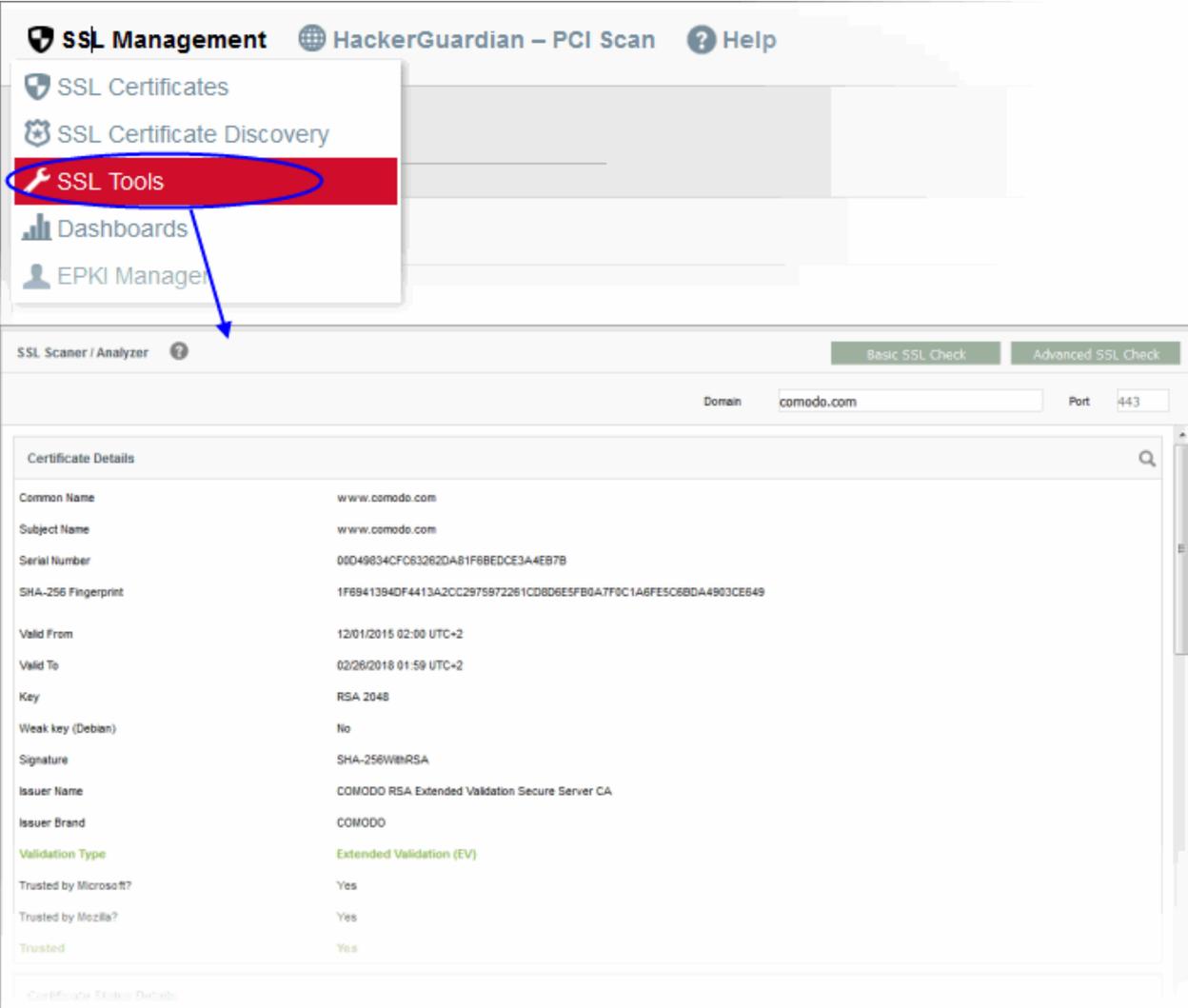
9. SSL Tools

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 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.



The screenshot shows the 'SSL Management' menu with 'SSL Tools' highlighted. Below it, the 'SSL Scanner / Analyzer' tool is displayed. The domain is set to 'comodo.com' and the port is '443'. The 'Certificate Details' section shows the following information:

Certificate Details	
Common Name	www.comodo.com
Subject Name	www.comodo.com
Serial Number	00D49834CFC83262DA81F6BEDCE3A4E87B
SHA-256 Fingerprint	1F6941394DF4413A2CC2975972261CD8D6E5FB0A7F0C1A8F5C68DA4903CE649
Valid From	12/01/2015 02:00 UTC+2
Valid To	02/28/2018 01:59 UTC+2
Key	RSA 2048
Weak key (Debian)	No
Signature	SHA-256WIRSA
Issuer Name	COMODO RSA Extended Validation Secure Server CA
Issuer Brand	COMODO
Validation Type	Extended Validation (EV)
Trusted by Microsoft?	Yes
Trusted by Mozilla?	Yes
Trusted	Yes

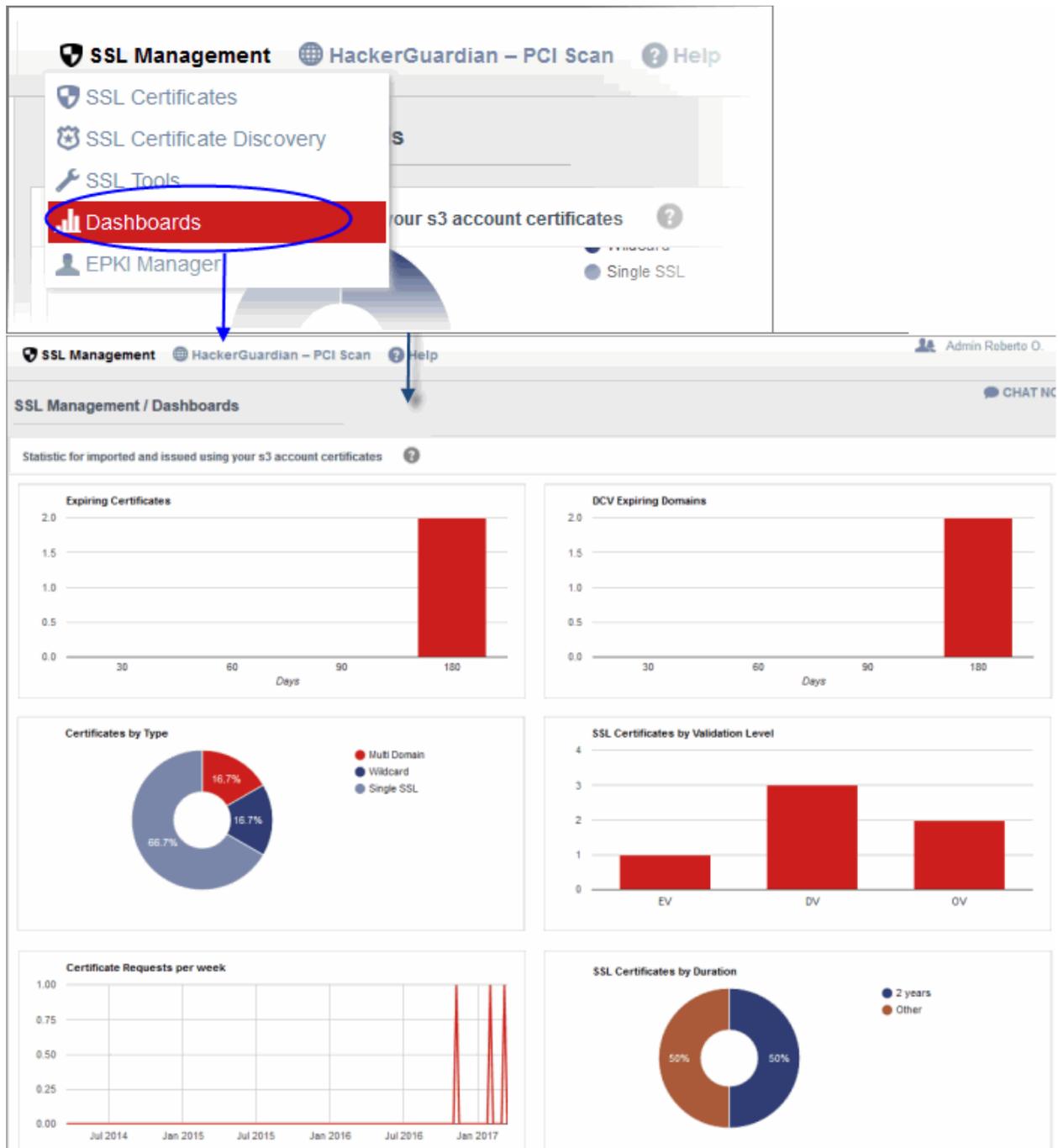
- 'Basic SSL Check' provides basic certificate information and is useful for quickly identifying the validity, type and issuer of the certificate.
- 'Advanced SSL Check' shows the basic information plus details about web-server configuration, including any protocol problems and whether the web server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

10. S³ Dashboards

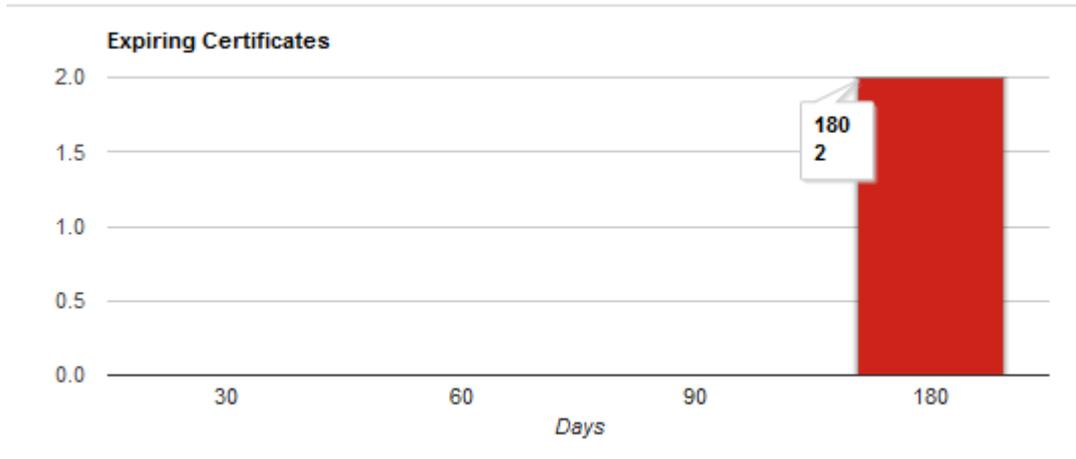
The dashboard is an informative heads-up-display which shows an overview of your Comodo certificate orders and certificates imported from your network.

- 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.

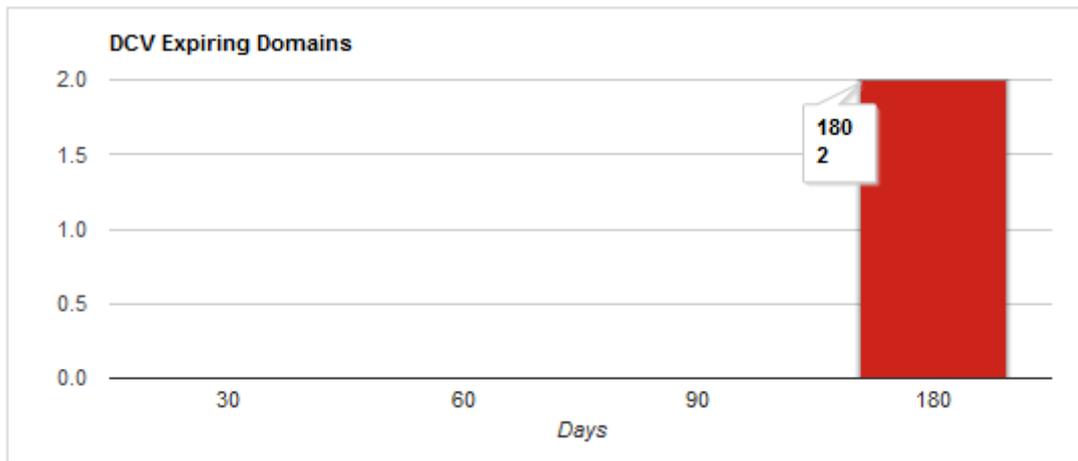


- **Expiring Certificates** – Comodo, self-signed and 'Other Trusted' certificates expiring within 180 days



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.

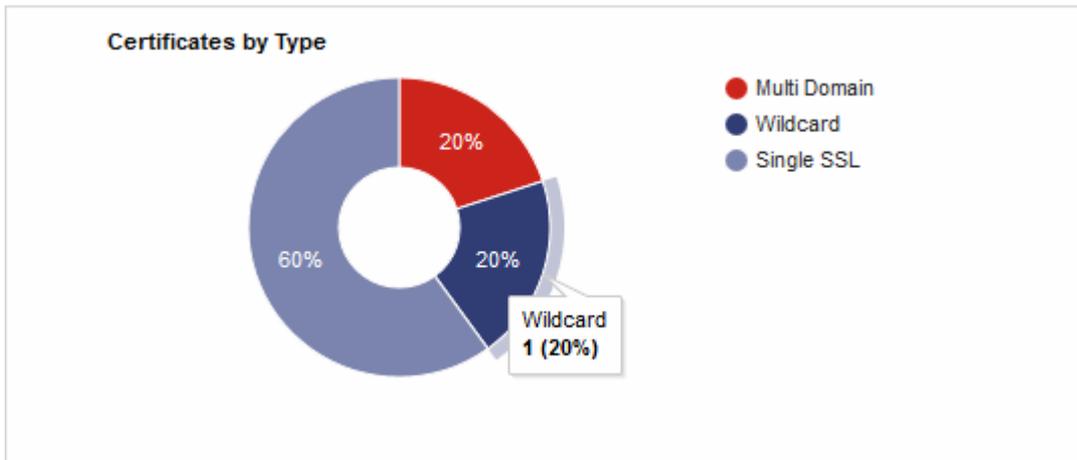
- **DCV Expiring Domains** – Domains for which Domain Control Validation will expire within 180 days



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.

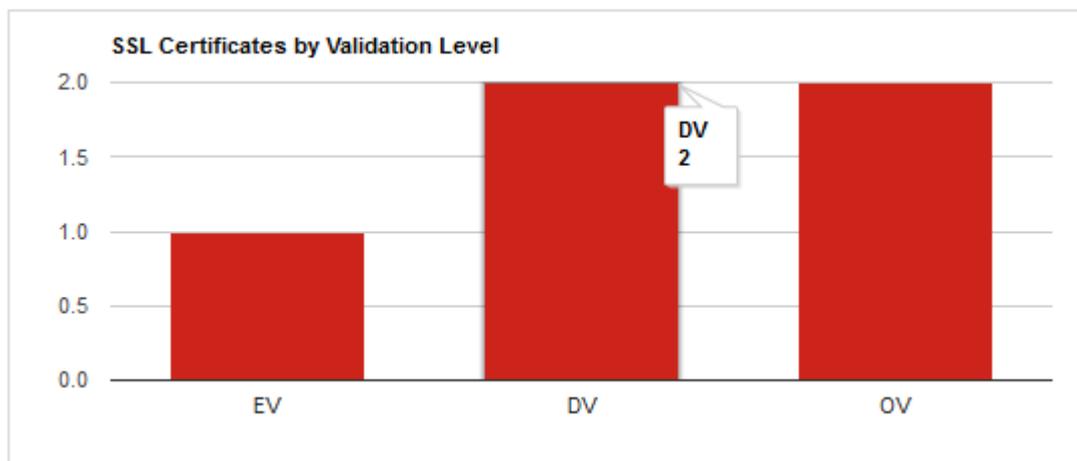
Placing the mouse cursor over a legend or bar displays a tool-tip showing the number of domains within that time-frame.

- **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.

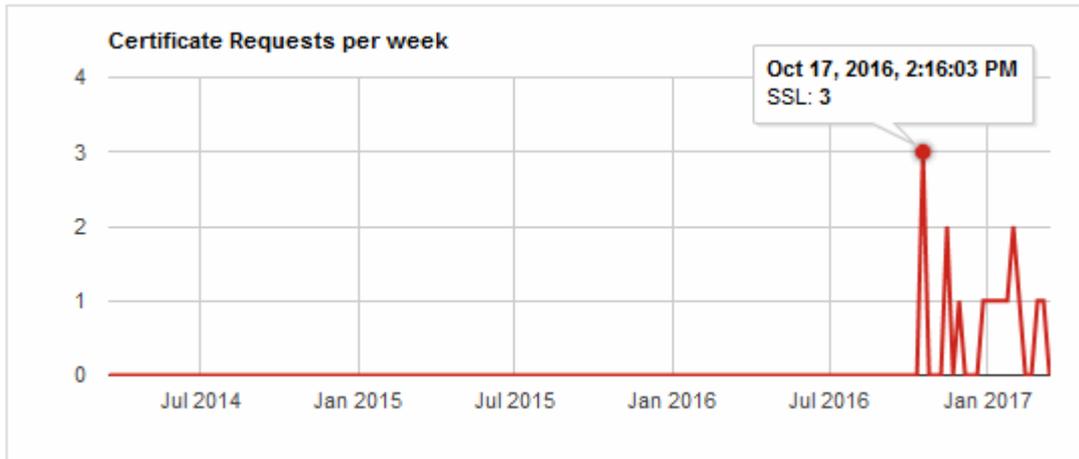
- **SSL Certificates by Validation Level – EV, DV, OV**



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.

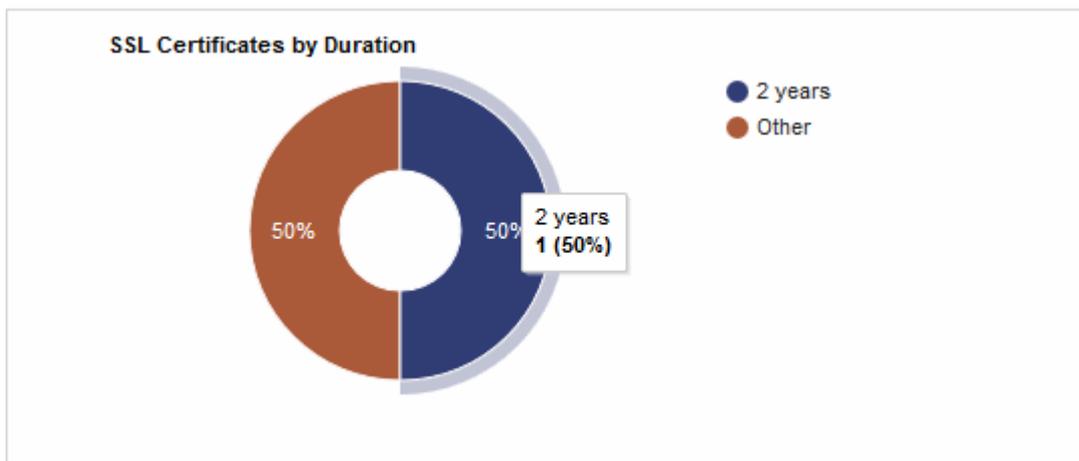
Hovering your mouse cursor over a bar displays the exact number of certificates in that category.

- **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 S³ 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 S³ using their existing username, password and one of their order numbers.
- All purchases made in S³ 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 S³. All user permissions will also apply in S³.

To deposit additional funds

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

The screenshot shows the 'EPKI Manager' interface. At the top, there is a navigation bar with 'SSL Management', 'HackerGuardian - PCI Scan', and 'Help'. A dropdown menu is open under 'SSL Management', with 'EPKI Manager' highlighted in red. Below this, the 'EPKI Manager' page is shown, featuring an 'Add Funds' button circled in blue. The page displays account details such as 'Able to Replenish Balance: Yes', 'Able to Create Order: Yes', 'SSL View Permitted: Yes', and 'Account Balance: \$8,109.40'. A table titled 'EPKI Price List' is also visible, showing various certificate products and their prices.

Product Name	Buy Price	Single Domains	Additional Price	Additional Domains	Wildcard Price	Wildcard Domains
1 Year	\$189.95					
2 Years	\$337.90					
3 Years	\$455.85					
Multi-Domain SSL Certificate						
1 Year	\$110.00	Up to 3	\$95.00	Up to 2005	\$105.00	Up to 100
2 Years	\$202.40	Up to 3	\$174.80	Up to 100	\$205.00	Up to 100
3 Years	\$270.60	Up to 3	\$233.70	Up to 100	\$305.00	Up to 100
COMODO EV SSL Certificate						
1 Year	\$280.00					
2 Years	\$449.00					
COMODO EV SGC SSL Certificate						
1 Year	\$599.00					
2 Years	\$948.00					
Free SSL Certificate						
0 Year	\$0.00					
EssentialSSL Wildcard Certificate						
1 Year	\$449.95					
2 Years	\$795.90					
3 Years	\$1,079.85					
OptimumSSL Trial Certificate						
0 Year	\$0.00					
Unified Communications Certificate						
1 Year	\$95.00	Up to 3	\$35.00	Up to 2005	\$105.00	Up to 100
2 Years	\$175.00	Up to 3	\$45.00	Up to 100	\$205.00	Up to 100
3 Years	\$235.00	Up to 3	\$60.00	Up to 100	\$305.00	Up to 100
COMODO EV Multi-Domain SSL Certificate						

OR

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

The screenshot shows the 'COMODO Server Security Server' dashboard. On the left sidebar, the 'Account Balance' section is highlighted with a red box, displaying a balance of \$8,109.40 and an 'ADD FUNDS' button. The main content area is titled 'SSL Management / SSL Certificates' and features an 'Orders' table with the following data:

Order#	Product
1701287	Topup Funds
1701286	COMODO SSL Wildcard Certificate
1701285	PositiveSSL Certificate

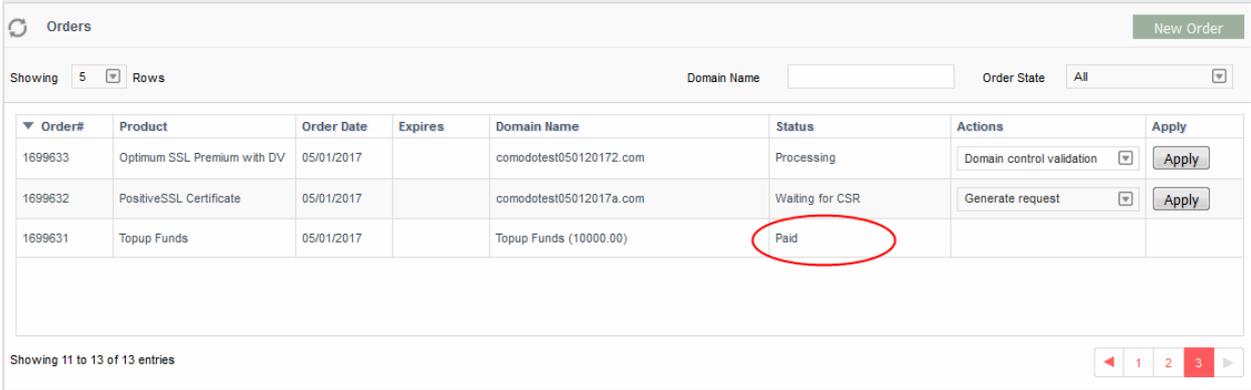
- Type the amount you wish to add in the 'Refill Account Balance' dialog then click 'OK':

The first screenshot shows the 'Refill Account Balance' dialog with an empty 'Amount' input field and 'USD' as the currency. The second screenshot shows the same dialog after a transaction of 1000 USD is completed. A green information icon and message state: 'New order # 1701875 was created. Please go to the order page to complete payment.' A 'Close' button is visible at the bottom right.

- 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:

1701875	Topup Funds	05/10/2017	Topup Funds (1000.00)	Awaiting payment	Complete payment	Apply
---------	-------------	------------	-----------------------	------------------	------------------	-------

- 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':

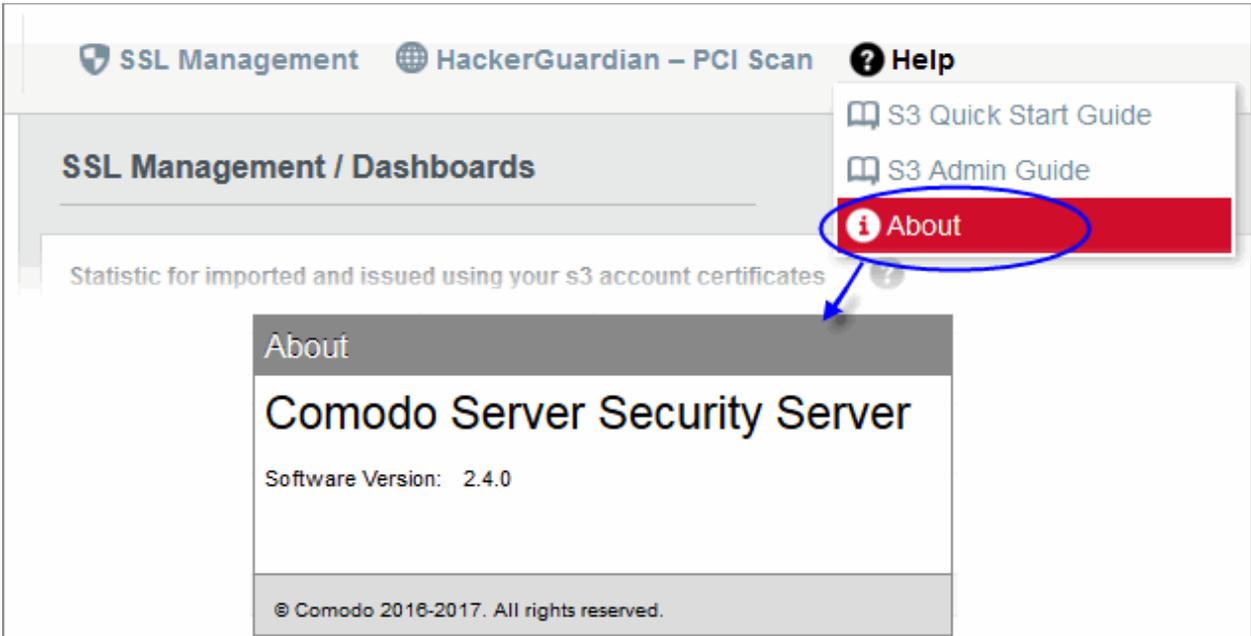


Order#	Product	Order Date	Expires	Domain Name	Status	Actions	Apply
1699633	Optimum SSL Premium with DV	05/01/2017		comodotest050120172.com	Processing	Domain control validation	Apply
1699632	PositiveSSL Certificate	05/01/2017		comodotest05012017a.com	Waiting for CSR	Generate request	Apply
1699631	Topup Funds	05/01/2017		Topup Funds (10000.00)	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



SSL Management HackerGuardian – PCI Scan ? Help

SSL Management / Dashboards

Statistic for imported and issued using your s3 account certificates

About

Comodo Server Security Server

Software Version: 2.4.0

© Comodo 2016-2017. All rights reserved.

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