

OneClickSSL™

Parallels Plesk Panel Plug-in
(Remote Administration Agent)



TABLE OF CONTENTS

Introduction.....	3
Vouchers.....	3
Before you begin	4
OneClickSSL™ Requirements.....	4
Installation	4
An overview of the OneClickSSL™ System	6
OneClickSSL™ - Parallels Plesk Panel – Admin Mode	7
OneClickSSL™ - Parallels Plesk Panel – User Mode.....	8
OneClickSSL™ – Certificate installation	10
Troubleshooting.....	11
Being caught for phishing	11
DNS Errors	11
Revocation – Errors when entering serial numbers.....	11
OneClickSSL™ Error messages.....	12
About GlobalSign	16

INTRODUCTION

GlobalSign's OneClickSSL is a fast and efficient SSL Certificate lifecycle delivery mechanism. Using a patented domain ownership verification system, OneClickSSL is able to provide a fully operational SSL Certificate within 30-50 seconds. Traditional processes for SSL security can be tedious. Completing the necessary steps requires knowledge of cryptography and recognition of terminology such as keysize; algorithm, CSR (Certificate Signing Request) and Intermediate Certificate Authorities (aka CA Bundle). It also relies on the ability to receive challenge-response email communications from an SSL vendor and processing the necessary steps to install the SSL Certificate requires patience and technical know-how. With the introduction of OneClickSSL, SSL Certificate provisioning can be fully automated, making server security easily accessible to organizations of all sizes. This process is quick and easy and the automated nature of the installations relieves the woes of spending hours troubleshooting the installation, thereby reducing support costs and increasing profit for all stakeholders in the delivery chain. OneClickSSL is based on multi-factor authentication techniques, hence providing the highest security levels, whilst also enabling administrators to manage the entire SSL lifecycle with practically zero training. The only item necessary to understand is the voucher.

VOUCHERS

Vouchers are redeemed for SSL Certificates. They are available either directly from GlobalSign's website through a GlobalSign Certificate Centre (GCC) Account, or from a GlobalSign Partner who may also be providing hosting services for your website/server. Appropriate links are embedded within the control panel to obtain trial vouchers or full versions. Just click on the 'No Voucher' ICON.



Trial Vouchers

Site Vouchers

Super Vouchers

Monthly Vouchers

- Trial Vouchers are usually free trials and are between 5-90 days.
- Full Site Vouchers are delivered on a per domain basis allowing additional features (Wildcards, SANs, Organizational Information, mixed FQDNs, Unified communications etc.).
- Super Vouchers are 3 months to 3 years and available via reseller partners and will usually be tied in to a hosting program with specific IP address ranges or specific control panels.
- Monthly Vouchers use the RAA (Remote Administration Agent) function integrated into the plug-in to automatically install SSL certificates on to the website every month – i.e. no renewal workload.

BEFORE YOU BEGIN

The OneClickSSL™ plug-in may be installed by following the instructions below. If you have any existing certificates installed then it is recommended to back these up before you begin. All temporary files will be cleaned after the install is completed and an unsuccessful install should return the system back to its original configuration. **Note:** It is recommended that you are familiar with the general set-up of your Parallels Plesk Panel and its configuration options and also the DNS (Domain Name Server) by which the webserver is named.

BEFORE YOU START, please make sure you can answer YES to all these questions:

- Your domain is registered with a Domain Name Registrar and can be located with a simple PING test (or equivalent). In order to install SSL Certificates the domain must be on a single dedicated IP address.
- You have a Voucher from GlobalSign or one of its partners.
- Your Parallels Plesk Panel has the desired domain available to you to control.
- You have Port 443 (or a custom alternative) open on your firewall such that a HTTPS session can be initiated during the install process.

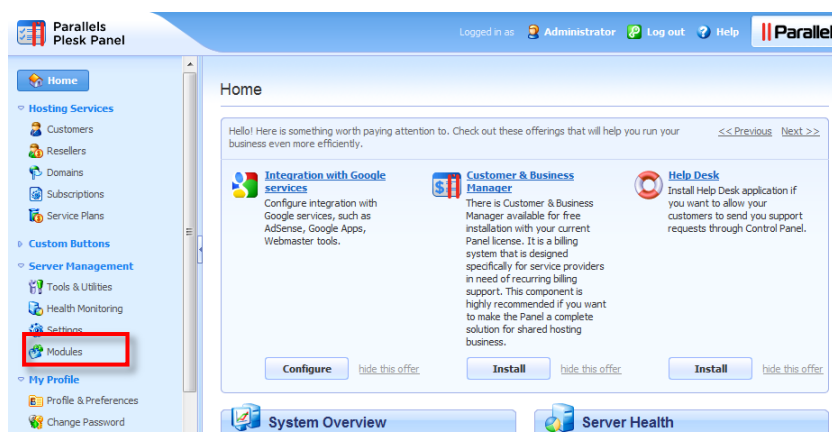
ONECLICKSSL™ REQUIREMENTS

- Parallels Plesk Panel 9.5.2+ or 10.1.0+ install on CentOS or RedHat (All screen shots 10+).
- The latest OneClickSSL rpm installer for Parallels Plesk is available here:-

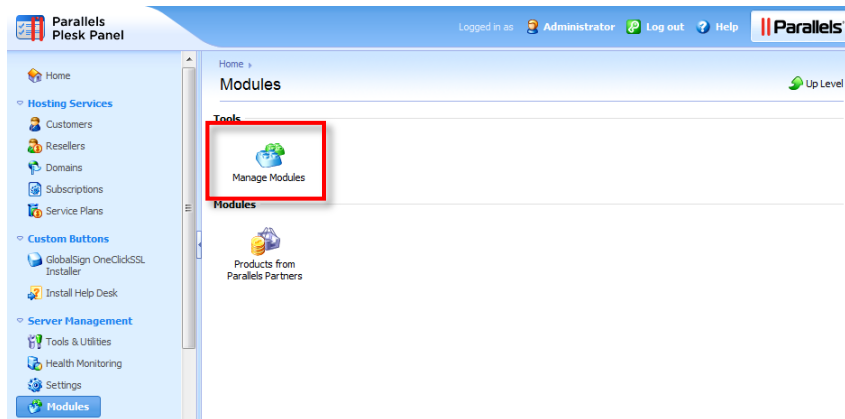
<http://www.globalsign.com/ssl/oneclickssl/parallels/>

INSTALLATION

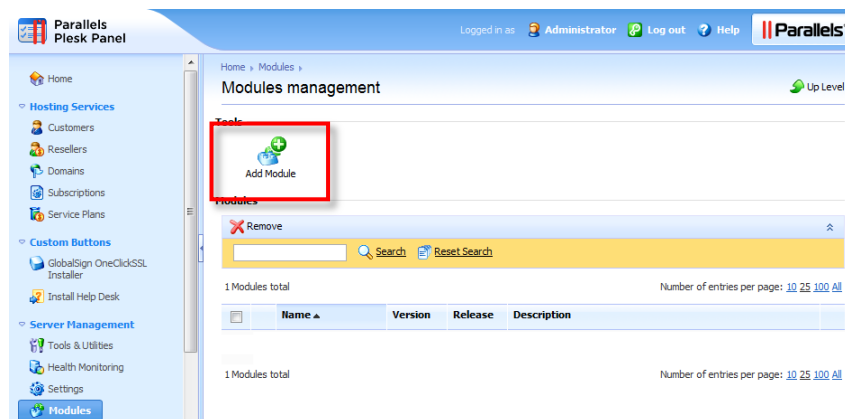
1. Download the latest rpm installer package to the system you use to administer your control panel (We will upload to the web server itself later on).
2. From your Parallels Plesk Panel home page click **Modules** under **System**, on the left hand menu.



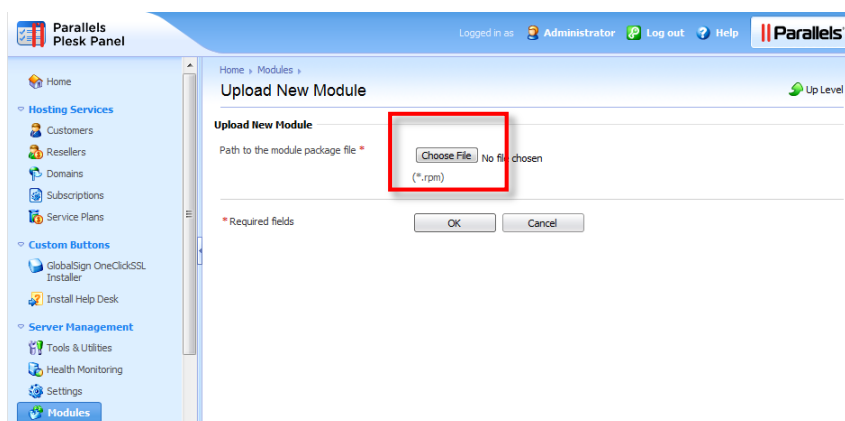
3. Click **Manage Modules**.



4. Click **Add Module**.

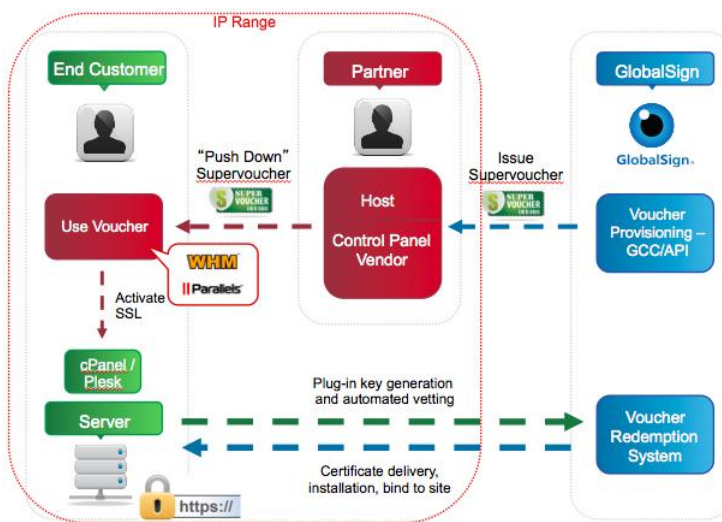
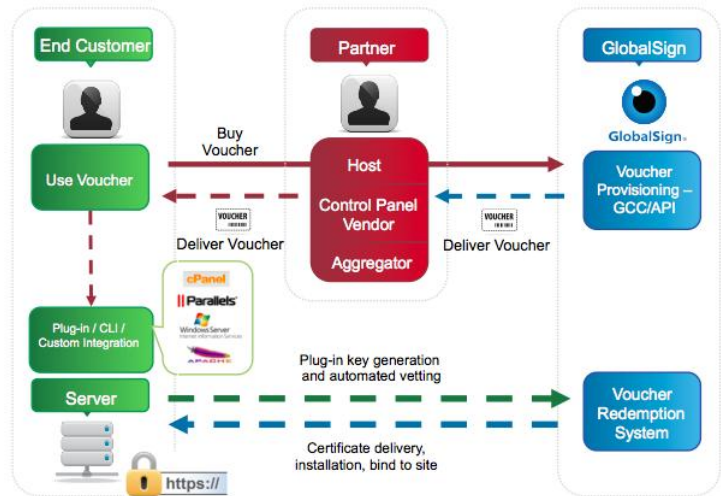


5. Click **Choose File** and specify the directory where your OneClickSSL™ .rpm installer is located and click 'OK'.



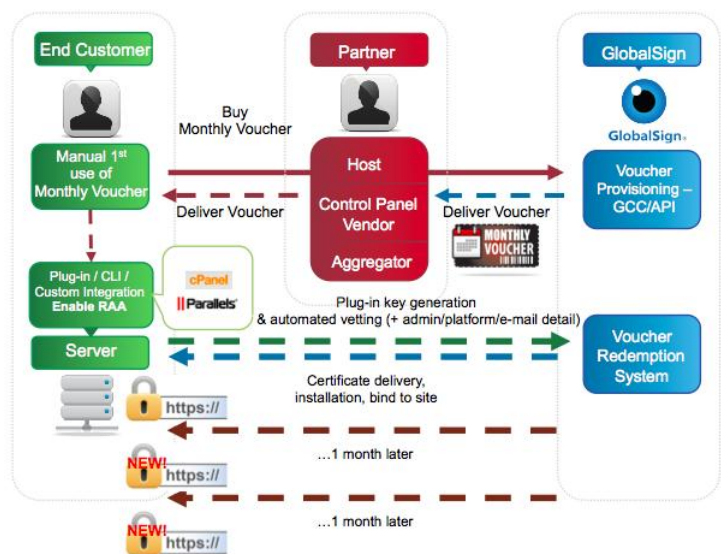
AN OVERVIEW OF THE ONECLICKSSL™ SYSTEM

This section provides a simplistic overview of the architecture and will help resellers, hosting providers and domain owners understand the relationships between the various parties that the plug-in supports. Any of the voucher types can be used by an End Customer/Domain owner to allow an SSL Certificate to be installed. The voucher can be requested via the Partner or directly from GlobalSign. Installation by the end customer initiates the voucher redemption process, effectively exchanging the voucher for an SSL Certificate to provide SSL functionality on the web server. The complete process takes between 30 and 50 seconds.



Hosting providers have the ability to 'push' SSL Certificates onto end customer's domains as a value added service. This is achieved through the WHM administration console, and is primarily design to support 'Super Vouchers'. Super Vouchers have the ability to be constrained by GlobalSign to a specific IP Address, or range of IP Addresses. This protects each of the stakeholders in the process by ensuring that only approved vouchers are used/installed protecting business relationships and allowing hosting providers to 'bundle' SSL Certificates with their hosting package without fear that the Super voucher could be used within a competitor's infrastructure.

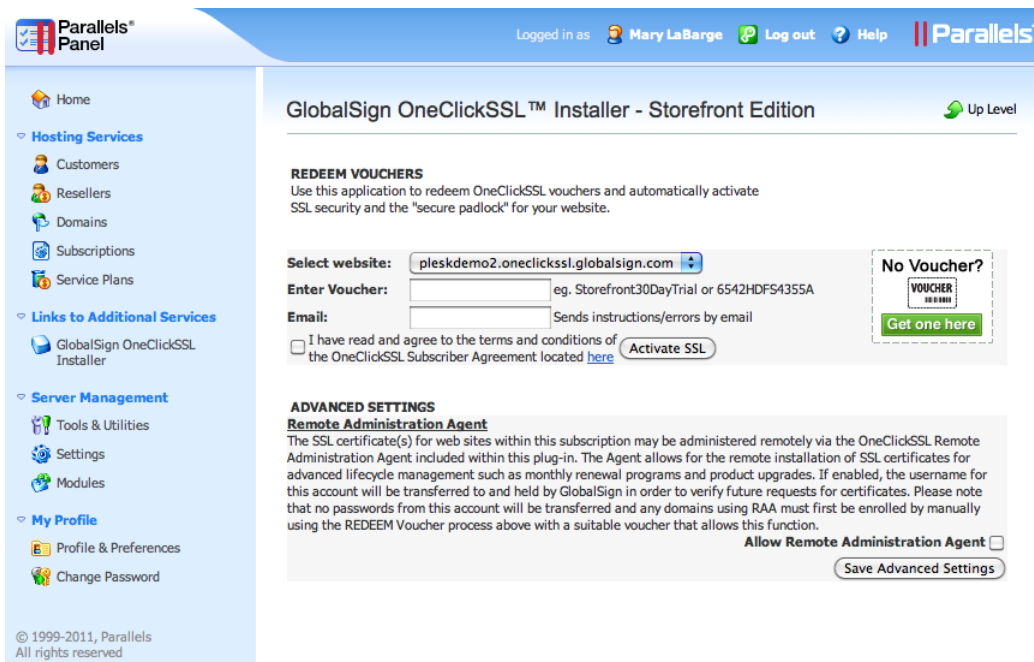
Monthly vouchers install SSL certificates via the RAA (Remote Administration Agent) function built into the end customer's control panel. If RAA is enabled then following a successful bootstrapping installation of an initial certificate, additional short duration certificates may be pushed onto the system by GlobalSign's system at regular intervals. During the install process the username of the Parallels Plesk Panel subscriber is archived by GlobalSign's system to ensure future certificates can be installed. This feature is described in more detail later on in this user guide.



ONECLICKSSL™ - PARALLELS PLESK PANEL – ADMIN MODE

To use the installer in administrator mode, click on the **OneClickSSL Installer**, under **Custom Buttons** on the left hand menu from the Homepage. (Please note that the installer will immediately execute and run when first installed following the previous installation instructions).

Please note that as an administrator, all websites are available to you in the selection box, meaning as an administrator you can ‘push’ a certificate down to users/subscribers who host domains on your system as a service. Please note that GlobalSign offers a www & a non www version of the domain name within the delivered certificate so all domain naming options will work correctly.



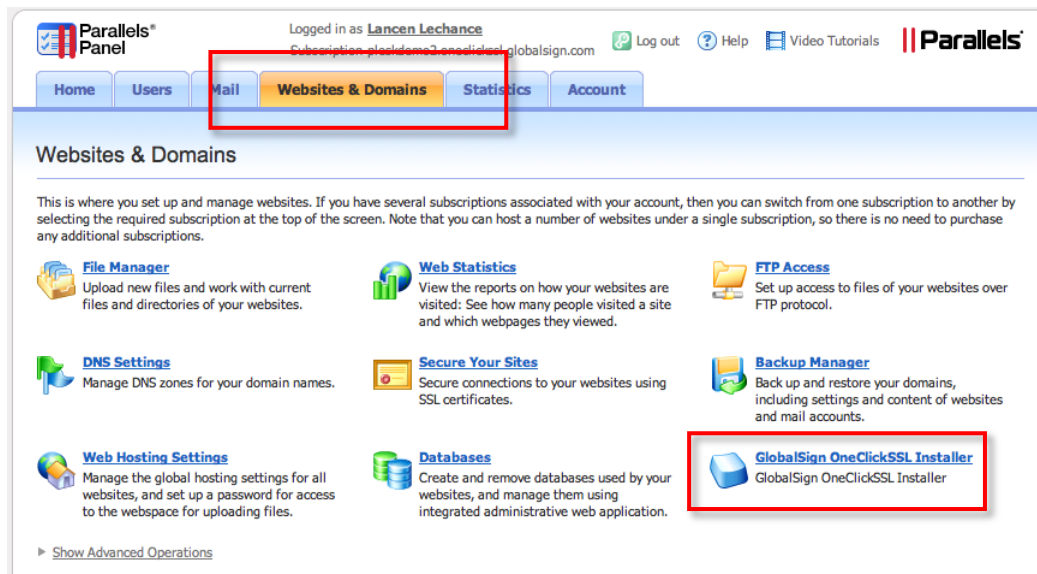
The screenshot shows the Parallels Plesk Panel Admin Mode interface. The top navigation bar includes the Parallels logo, user information (Logged in as Mary LaBarge), and links for Log out and Help. The left sidebar contains a menu with categories: Home, Hosting Services (Customers, Resellers, Domains, Subscriptions, Service Plans), Links to Additional Services (GlobalSign OneClickSSL Installer), Server Management (Tools & Utilities, Settings, Modules), and My Profile (Profile & Preferences, Change Password). The main content area is titled 'GlobalSign OneClickSSL™ Installer - Storefront Edition' and includes an 'Up Level' link. The page is divided into sections: 'REDEEM VOUCHERS' with instructions and an 'Activate SSL' button, a 'No Voucher?' section with a 'Get one here' button, and 'ADVANCED SETTINGS' for the 'Remote Administration Agent' with an 'Allow Remote Administration Agent' checkbox and a 'Save Advanced Settings' button. A copyright notice at the bottom left reads '© 1999-2011, Parallels All rights reserved'.

Note that the ‘Parallels Storefront Edition’ is illustrated above. Reseller URL customization is not included in this version.

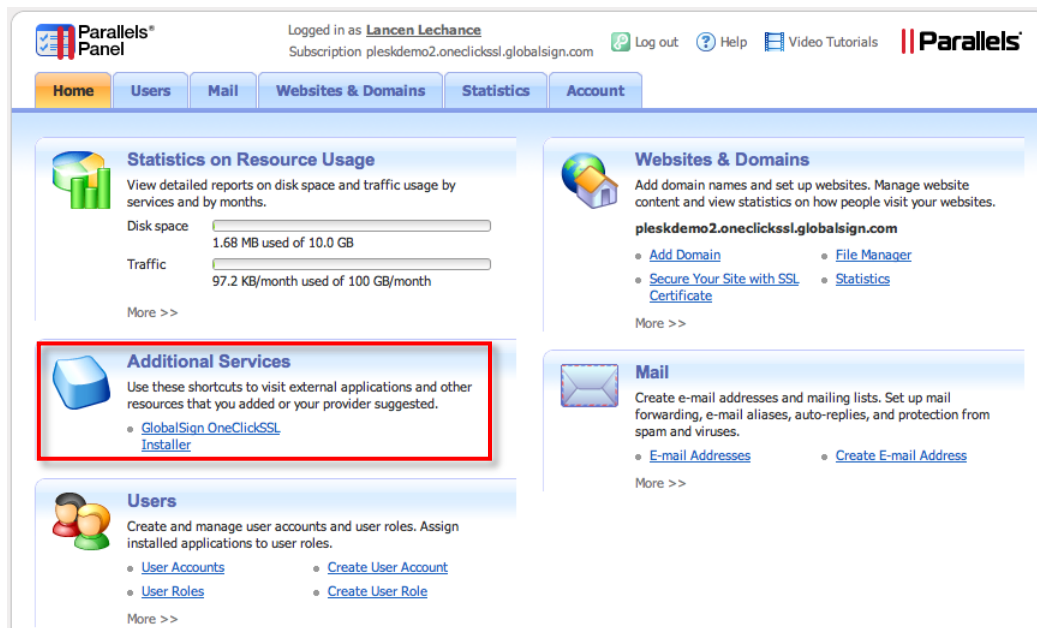
The reseller-landing page URL may be used to customize the action of the ‘No Voucher’ icon for your hosted customers. Traffic can be directed to your site to sell vouchers and services associated with OneClickSSL. Once you have modified the URL you may select ‘Save Changes’ button. As Parallels Plesk Panel offers multiple levels of control, administrators can modify the experience of ‘Resellers’ and likewise ‘Resellers’ can modify the URL for domain owners.

ONECLICKSSL™ - PARALLELS PLESK PANEL – USER MODE

Alternatively, as a subscriber/domain owner, simply choose the **'Websites & Domains'** tab to locate the Installer.

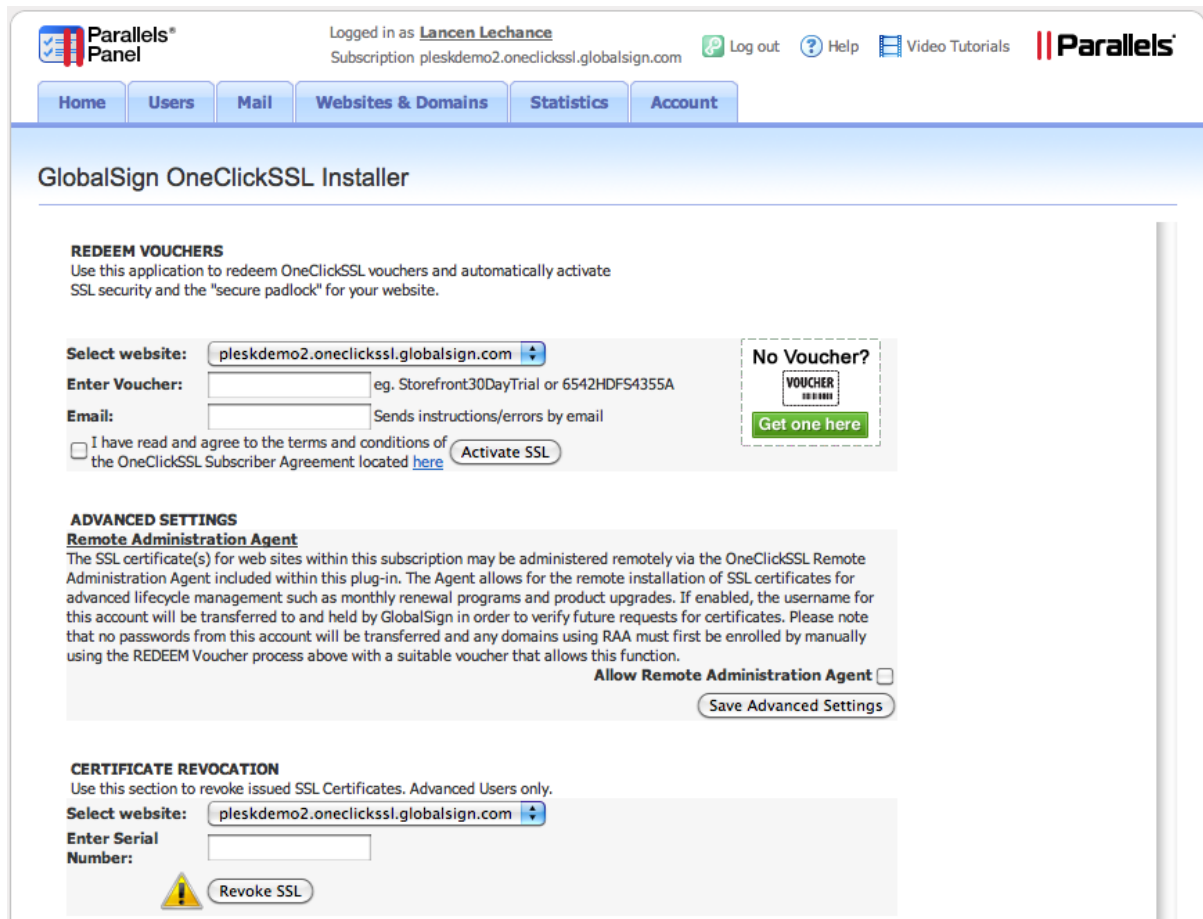


Depending on how you have configured your system, the link may also be available within the **'Additional Services'** menu.



The **'Redeem Vouchers'** menu offers the ability to select the appropriate website to secure, as well as input boxes for the voucher itself and an e-mail address for notification of a successful installation or how to upgrade/renew as appropriate. In the event of an error, details will be sent to this e-mail address to aid debugging activities. There is also a link to purchase vouchers.

An additional feature is available for domain owners: The ability to allow or disallow Remote Administration. This is performed on a per user basis, so if you have multiple websites secured within a single user area then all of them will support RAA if you enable this option. RAA must be enabled if you wish to support automatic renewals, monthly installation of certificates or future lifecycle options from GlobalSign.



The screenshot shows the Parallels Plesk Panel interface. At the top, it indicates the user is logged in as 'Lancen Lechance' with the subscription 'pleskdemo2.oneclickssl.globalsign.com'. Navigation tabs include Home, Users, Mail, Websites & Domains, Statistics, and Account. The main content area is titled 'GlobalSign OneClickSSL Installer' and is divided into three sections:

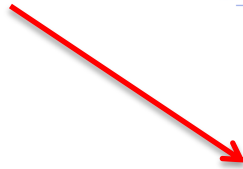
- REDEEM VOUCHERS:** This section allows users to redeem OneClickSSL vouchers. It includes a dropdown menu for 'Select website:' (currently set to 'pleskdemo2.oneclickssl.globalsign.com'), an 'Enter Voucher:' text box, and an 'Email:' text box. A checkbox is present for 'I have read and agree to the terms and conditions of the OneClickSSL Subscriber Agreement located [here](#)'. A 'No Voucher?' box with a 'Get one here' button is also visible. An 'Activate SSL' button is at the bottom of this section.
- ADVANCED SETTINGS:** This section is titled 'Remote Administration Agent'. It contains a paragraph of text explaining the agent's function. At the bottom, there is a checkbox for 'Allow Remote Administration Agent' and a 'Save Advanced Settings' button.
- CERTIFICATE REVOCATION:** This section is for revoking issued SSL certificates. It includes a 'Select website:' dropdown (set to 'pleskdemo2.oneclickssl.globalsign.com') and an 'Enter Serial Number:' text box. A warning icon is shown next to the 'Revoke SSL' button.

Finally, certificate revocation is also possible for domain owners. Please note that revocation is a way to permanently identify an individual certificate on a blacklist as 'bad'. Browsers will use information embedded within certificates to validate that they are still 'good', so please do not revoke a certificate by mistake as it is not possible to reverse this. (A warning will be presented once the Revoke SSL button is pressed). Select the domain for the certificate that you wish to revoke, if you wish to revoke a certificate then you will need to enter its serial number into the box as confirmation of intent.

ONECLICKSSL™ – CERTIFICATE INSTALLATION




Once you click 'Activate SSL' in the redeem vouchers menu, the system will begin to process using web services technology. Each of the significant steps is highlighted with a green check mark as the plug-in runs through the application and installation process.

A successful install.



GlobalSign OneClickSSL Installer

OneClickSSL securesite activation in process...
Do not close or navigate away from this page until completed.

- Sending Voucher and Domain details to GlobalSign OneClickSSL Service... 
- Performing domain verification check and Enrolling for an SSL certificate... 
- Setting up SSL and activating secure web site... 

OneClickSSL secure site setup successful!

[Click to open a test window to check your secure site](#)

GlobalSign OneClickSSL™ Installer

OneClickSSL securesite activation in process...
Do not close or navigate away from this page until completed.

Sending Voucher and Domain details to GlobalSign OneClickSSL Service...

Error Field:

Error Message: The CN has expressions that match our Phishing/Keyword warning list. This order will be delayed until the vetting team can manually review the requested domain. You should receive an e-mail from the system to confirm this issue and another one when it has been cleared. Please have the domain name and Voucher ID available for our support team if you need immediate resolution.
Error Code: -5001



A failure, showing details about why it failed.

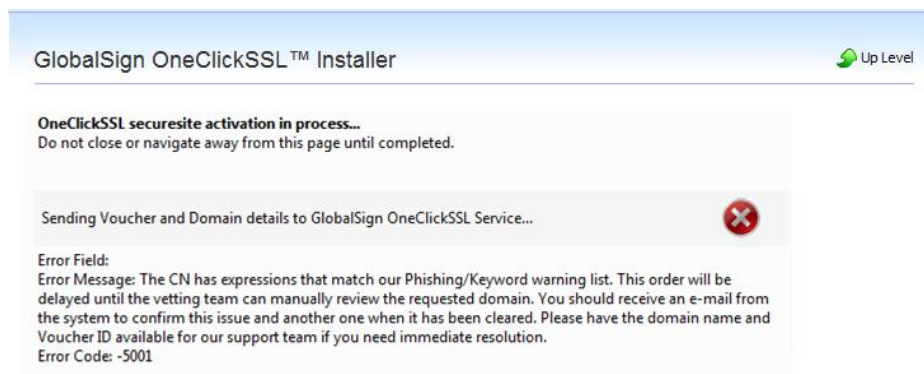


Please see the troubleshooting section within this guide should an error occur.

TROUBLESHOOTING

BEING CAUGHT FOR PHISHING

In some cases where an SSL Certificate is requested for a domain with suspicious keywords, such as 'Bank' or 'Microsoft', the request can be halted for security reasons. This is called being caught for 'Phishing'. The GlobalSign OneClickSSL™ Plugin for Parallels Plesk has a built-in phishing check at the beginning of the voucher verification phase. In the event the domain you have requested a certificate for gets caught for phishing, you will receive an email notifying you and the order will be delayed until the vetting team can manually review the requested domain. If you require immediate resolution please contact the GlobalSign support team with your **Voucher** and domain name.



GlobalSign OneClickSSL™ Installer Up Level

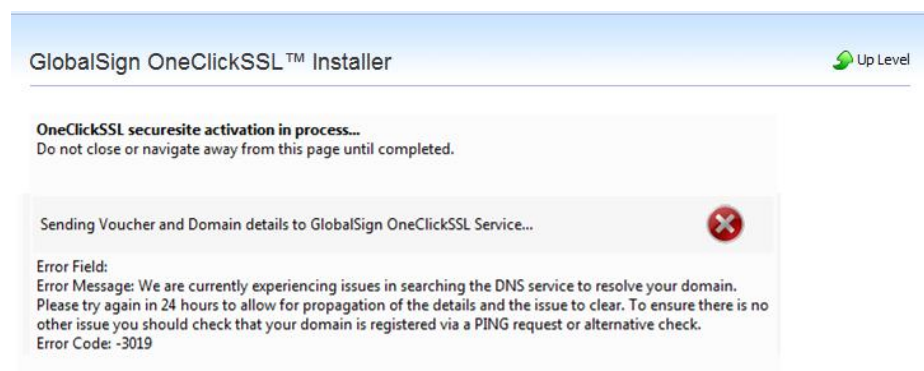
OneClickSSL securesite activation in process...
Do not close or navigate away from this page until completed.

Sending Voucher and Domain details to GlobalSign OneClickSSL Service...

Error Field:
Error Message: The CN has expressions that match our Phishing/Keyword warning list. This order will be delayed until the vetting team can manually review the requested domain. You should receive an e-mail from the system to confirm this issue and another one when it has been cleared. Please have the domain name and Voucher ID available for our support team if you need immediate resolution.
Error Code: -5001

DNS ERRORS

In the event you are presented with a DNS-related error during the OneClickSSL order process, there are several potential issues that need to be addressed. If your domain is a new entry in the DNS system then please allow 24 hours after its creation to propagate and clear. If your domain has existed for more than 24 hours, try a PING request to your domain and check that it resolves.



GlobalSign OneClickSSL™ Installer Up Level

OneClickSSL securesite activation in process...
Do not close or navigate away from this page until completed.

Sending Voucher and Domain details to GlobalSign OneClickSSL Service...

Error Field:
Error Message: We are currently experiencing issues in searching the DNS service to resolve your domain. Please try again in 24 hours to allow for propagation of the details and the issue to clear. To ensure there is no other issue you should check that your domain is registered via a PING request or alternative check.
Error Code: -3019

REVOCACTION – ERRORS WHEN ENTERING SERIAL NUMBERS

cPanel users should note, when attempting to revoke, that great care needs to be taken in selecting the correct serial number of the certificate you wish to revoke and check this against the certificate beforehand. In the event you are presented with an error for a non-existent serial number, double-check the serial number again and ensure the serial number was formatted correctly e.g. **0100011617904c9e** instead of **01 00 01 16 17 90 4c 9e**.

OneClickSSL certificate revocation in process...
 Do not close or navigate away from this page until completed.

Sending Serial Number to GlobalSign CA Service...



Error Field:
 Error Message: The Serial Number you have requested does not exist. Please check the certificate again and ensure the format is correct with no spaces eg. 0100011617904c9e and not 01 00 01 16 17 90 4c 9e
 Error Code: -9007

ONECLICKSSL™ ERROR MESSAGES

ErrorCode	Error Description Returned	Resolution
-101	Invalid parameter entered. Please check the parameters match the API specification.	Please check that you have correctly typed all the parameters. Use debug mode to see if any other information is presented.
-102	Mandatory parameter missing. Please check the parameters match the API specification.	If you have a 'Super Voucher' or a 'Trial Voucher' then an email address is mandatory with the 'voucher option' switch
-103	Parameter length check error. Please check the parameters match the API specification.	Please check that you have correctly typed all the parameters. Use debug mode to see if any other information is presented.
-104	Parameter format check error. Please check the parameters match the API specification.	Please check that you have correctly typed all the parameters. Use debug mode to see if any other information is presented.
-105	Invalid parameter combination. Please check the parameters match the API specification.	Please check that you have correctly typed all the parameters. Use debug mode to see if any other information is presented.
-3008	We have been unable to connect to your web server to validate the presence of the Temporary SSL certificate. Please ensure your firewall settings allow an external https connection to be established on the default port 443 or the custom port you may have selected.	Please ensure that your domain can be queried from the 'public' Internet on the port you have chosen. You may need to check from outside your internal network.
-3012	We have been unable to validate your domain through a Domain Name Search. Please verify that your domain is registered correctly via your Domain Management Registrar.	Please ensure that your domain can be queried from the 'public' Internet on the port you have chosen. You may need to check from outside your internal network.
-3013	Failed to obtain your IP Address via a targeted DNS search. Please verify that your domain is registered correctly via your Domain Management Registrar.	Please ensure that your domain can be queried from the 'public' Internet on the port you have chosen. You may need to check from outside your internal network.
-3019	We have been unable to resolve the IP address of your domain through DNS. Please check your domain is correct and can be seen via a PING request or alternative check. If this is a new domain or subdomain it might be that it has not propagated to the Root DNS server. These checks help to avoid the possibility of DNS Poisoning issues. Please try again later	Please ensure that your domain can be queried from the 'public' Internet on the port you have chosen. You may need to check from outside your internal network.

-5001	The domain has been flagged as either containing a suspicious word or phrase, or it may have triggered a hit on our Phishing database search. It will not be possible to proceed without clearing this issue so please contact your support team directly to resolve the problem. Please have the domain name and Voucher ID available for our support team.	Domain Validated certificates need to be carefully controlled as issuance to a website purporting to be a brand owner when they are not may be cause for concern. If your domain contains keywords or has been identified as a possible 'phishing website' then you will need to contact your support team. An e-mail will be sent to the appropriate contact person who made the request.
-6001	Certificate Signing Request parsing error. Please retry and if the issue persists then contact support with detailed information concerning the issue.	There is a potential issue with CSR generation on your platform. It may not be possible to continue. Please contact your support team to resolve the issue.
-6007	System Error (The Public Key of the certificate has been used previously – Duplicates are not allowed). Please retry and if the issue persists then contact support with detailed information concerning the issue.	It's unlikely, but possible, that your Public Key has been used by another entity. It is recommended to re generate the key again. Please run the process from the beginning which will do this.
-6019	System Error (The Certificate Distinguished Name (DN) exceeds 1024 bytes). Please retry and if the issue persists then contact support with detailed information concerning the issue.	If you have an extremely long domain name you may have exceeded the allowable size of the DN. Please contact GlobalSign directly to talk about alternative options to move forward.
-6029	System Error (The Certificate has already been revoked). Please retry and if the issue persists then contact support with detailed information concerning the issue.	Please check that you have entered the correct S/N as it looks like the certificate has already been revoked. You can obtain the CRL location from the certificate and view the CRL to see if the S/N is included. Please not the format in Windows is in S/N order
-9001	The Voucher you have entered does not exist. Please check and try again.	Please verify that the voucher is correct. It may contain O's (oh's) and 0's (zeros) so please verify these are correct.
-9002	We are unable to verify the presence of the Temporary certificate on your domain. Possible time out issue. Please retry and if the issue happens again contact support.	We can't connect to your domain. We allow 3 minutes to check for the presence of the Temporary certificate. Please check that it is viewable via the public Internet. You can see using the debug option that the certificate has been installed.
-9003	The Domain which you have requested does not match the Common Name (CN) that was specified during the Voucher application process. Please double check and retry.	If you purchased a Voucher then the confirmation e-mail should highlight the domain that was purchased. Please check that you are using the right domain and the right voucher.
-9004	A Public IP Address cannot be used as a Domain Name with this type of SSL Certificate. Please check you have requested the correct certificate type.	You cannot apply for a Public IP address as the primary domain. You need to have an FQDN (Fully Qualified Domain Name) as the principle domain.
-9005	Reissuance using this Voucher is not possible as the underlying certificate has now expired.	Reissuance allows a certificate to be issued again from the same Voucher up to and including the same date of expiry as the original certificate. It seems that the original has expired.

-9007	The Serial Number you have requested does not exist. Please check the certificate again and ensure the format is correct with no spaces e.g. 0100011617904c9e and not 01 00 01 16 17 90 4c 9e	Be sure to type the serial number correctly. Please open the certificate viewer and check the serial number again.
-9008	It is not possible to Revoke this certificate. It may have expired or it may have already been revoked. Please contact GlobalSign directly for confirmation of the certificate status.	You can examine the certificate and locate the CRL location in the Details view. If you download the CRL you can view it on a per S/N basis to see if your S/N is listed (Please allow up to 3 hours before checking as CRLs are renewed every three hours.
-9011	The Voucher used has expired. Please check and try again.	Vouchers have an expiry date. If you receive this message then please contact the supplier of your Voucher and obtain and updated Voucher.
-9012	In order to prevent a race condition for multiple re-issuances, a limit is placed on the number of re-issuances per day. The Daily limit has been exceeded.	Please wait 24 hours before trying to use this Voucher again.
-9016	The domain name within the CSR is different from the Common name (CN) associated with the Voucher. Please verify the domain names are consistent and try again.	Vouchers are sometimes tied directly to a domain. If you believe that the domain you have entered is correct then please contact support. Please note that entering www.domain.com will provide a certificate with www.domain.com & domain.com capabilities, whereas domain.com will only provide domain.com capabilities.
-9018	The Voucher you are using relates to an alternative plug-in family or system type. Please check with the provider of the Voucher.	Vouchers may be tied to a platform such as IIS, cPanel, Plesk, Linux. If you have this error it's possible that the Voucher you are using is for an alternative platform and not IIS. Please contact the provider of your Voucher.
-9019	The Voucher you are using only allows a certificate to be installed within a specific IP address range. The IP address of this domain is not within the allowed range. Please check with the provider of the Voucher.	Vouchers may be tied to a specific IP address range. If you have this error it's possible that the voucher you are using is for an alternative IP Address. Please contact the provider of your Voucher.
-9026	The Voucher you are trying has been cancelled. Please contact support with detailed information concerning the issue.	Please contact the provider of your Voucher.
-9028	The Voucher you are using is for a 'renewal'. Unfortunately the original certificate has either been canceled, revoked or re-issued already, or the expiry date has now passed. Please contact support with detailed information concerning the issue.	Please contact the provider of your Voucher.
-9029	The Voucher you are using is for a "re-issue". Unfortunately the original certificate has either been canceled, revoked or re-issued already, or the expiry date has now passed. Please contact support with detailed information concerning the issue.	Please contact the provider of your Voucher.

-9910	The credit card associated with the account is invalid and it is not possible to complete the order process. Please verify that the credit card is correct and try again.	Please log in to your account and rectify the problem.
-9911	There is insufficient credit in the account to complete the order process. Please verify that the account has sufficient funds and try again.	Please log in to your account and rectify the problem.
-9912	There is an insufficient deposit balance within the account to complete the order process. Please verify that the account has sufficient funds and try again.	Please log in to your account and rectify the problem.
-9935	The Country Code within the certificate is for a country that GlobalSign does not support. Please contact support with detailed information concerning the issue.	Not all countries are supported by GlobalSign. If you receive this message then unfortunately you cannot install a certificate with this method.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As a leader in public trust services, GlobalSign Certificates are trusted by all popular Browsers, Operating Systems, Devices and Applications and include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. It's trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

For more information about the GlobalSign solutions, please contact us:

Singapore

Tel: +65 3158-0346
sales-apac@globalsign.com
www.globalsign.com.sg

Australia

Tel: +61 3-9988-3988
sales-apac@globalsign.com
www.globalsign.com.au

Hong Kong

Tel: +852 5808-1867
sales-apac@globalsign.com
hk.globalsign.com