

2QH & OLFN66 / OE

Microsoft IIS (6.0, 7.0 & 7.5) SSL Installer
(V2 GUI and CLI)





TABLE OF CONTENTS

- Introduction..... 3
- Vouchers..... 3
- Before you begin 4
- 2 Q H & O L F N 6 6 / Œ 5 H.T.X.L.U.H.P.H.Q.W.V..... 4
- Operation In Administrator Mode (CLI / GUI) 4
- An overview of the OneClickSSL System ±CLI Mode..... 5
 - Revocation 7
 - SSLPort ±Using a port other than the default port of 443..... 7
 - VoucherOption ±typically your e-mail address 7
 - Language options ±Customize error messages & feedback..... 7
 - Network Address Translation ±NATIPAddress 8
 - Siteid ±When IIS does not use Binding 8
- An overview of the OneClickSSL System ±GUI Mode..... 10
 - The GUI Installer - An overview 10
 - The GUI Installer ±Advanced Mode 11
 - Revocation 11
 - SSLPort ±Using a port other than the default port of 443..... 12
 - E-mail address..... 12
 - Language options ±Customize error messages & feedback..... 12
 - Network Address Translation ±NATIPAddress 12
 - Siteid ±When IIS does not use Binding 12
 - A Successful installation 13
 - An UnSuccessful installation 13
- Troubleshooting..... 14
 - Are you sure you are in administrator mode? 14
 - Being caught for phishing 14
 - DNS Errors..... 14
 - Revocation ±Errors when entering serial numbers..... 14
 - 2 Q H & O L F N 6 6 / Œ (U U.R.U...P.H.V.V.D.J.H.V..... 14
- Appendix A 18
- About GlobalSign 20



INTRODUCTION

GlobalSign 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 key size, 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 or from a GlobalSign Partner who may also be providing hosting services for your website/server. Appropriate links are embedded within the GUI version of the tool, which allow you to obtain trial vouchers or full versions. Just click on the



Trial Vouchers

Site Vouchers

Super 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 (Organizational Information, Wildcards, SANs, 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.



BEFORE YOU BEGIN

The OneClickSSL executable (oneclickssl.exe) is delivered as a signed, virus scanned command line tool for Microsoft Server 2003/2008/2008-R2 and Microsoft Windows 7. As configuration changes will need to be made to IIS during the installation, it requires Administrator privileges on the Operating System. These can be given through the use of an Administrator Command Prompt in order to execute and run the tool. All temporary files will be cleaned after the install is completed and an unsuccessful installation of an SSL Certificate should return the system back to its original configuration, however, if you have any existing certificates installed then it is recommended to back these up before you begin. Appendix A offers tips on how to do this.

Note: It is recommended that you are familiar with the general set-up of your IIS server and any DNS (Domain Name Server) to which the IIS web server is connected. The troubleshooting section at the rear of this guide offers some solutions for solving common configuration problems.

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.
- You have IIS bindings set to bind the website to the appropriate IP address of the server.
- You have Port 443 (or a custom alternative) open on your firewall such that a HTTPS session can be initiated during the install process.

2.1 (& / , & . 6 6 /) REQUIREMENTS

- IIS version 6+, 7+ or 7.5+.
- The OneClickSSL.exe GUI/CLI is available here <http://www.globalsign.com/ssl/oneclickssl/iis/>

OPERATION IN ADMINISTRATOR MODE (CLI / GUI)

When you have logged in to your webserver, either use the start menu to run the command prompt for CLI (Command Line Interface) mode or the OneClickSSL.exe itself for GUI (Graphical User Interface) mode. **In both cases right click to allow either to run in Administrator mode.**



DomainName is the domain you wish to secure. (Please note that www prefixed domains will automatically have a **www** and **non-www** version added to the Subject Alternative Name field of the issued certificate.)

[IPAddress] The external IP address of your web server. The web server's IP address must be resolvable through public DNS for the certificate validation to be completed. This is optional. If you do not know the IP address the plug-in will attempt to determine this through a DNS check.

```
C:\>oneclickssl DV78CLSWMRF3UDE1 oneclickssldemo.co.uk 80.46.115.103
```

Using the CLI tool without the optional IPAddress:

```
C:\>oneclickssl DV78CLSWMRF3UDE1 oneclickssldemo.co.uk
```

Getting additional help from the command line tool. Please use the **-?** or **-help** switch as per the example below:

```
C:\>oneclickssl -? or C:\>oneclickssl -help
```

```
GlobalSign OneClickSSL(tm) Installer v2.0.0 (c)GMO GlobalSign, 2011
=====
Use this application to redeem OneClickSSL Vouchers and automatically activate
SSL security and the "secure padlock" for your website
```

Usage:

```
OneClickSSL -? | -help
OneClickSSL [options] Voucher DomainName [IPAddress]
```

Activate SSL Example(s):

```
=====
```

```
oneclickssl AD34EF6700G67142 www.mydomain.com
oneclickssl AD34EF6700G67142 www.mydomain.com -natip 192.168.2.1 -debug
oneclickssl NONUNIQUEVOUCHER www.mydomain.com -voucheroption j.doe@mydomain.com
```

Revoke SSL Example(s): (For Advanced Users Only)

```
=====
```

```
oneclickssl -revoke 0100012698b9b97c www.mydomain.com
oneclickssl -debug -revoke 0100012698b9b97c www.mydomain.com -natip 192.168.2.1
```

Options:

```
-revoke
-sslport SSLPort
-voucheroption "Options"
-language LanguageCode
-natip NATIPAddress
-debug
-testurl WebServiceURL
-quiet
```

Description:

```
-? or -help - Display this help
Voucher - This is the GlobalSign OneClickSSL Voucher as
provided by GlobalSign or an associated partner
DomainName - The website address and common name.
IPAddress - The IP address for the IIS SSL website binding.
If omitted, DNS will be used to obtain this.

-revoke - Revoke a certificate based on Serial Number
and domain name
-sslport SSLPort - Optional SSL HTTP port number if not 443
```



<code>-voucheroption "Options"</code>	- Promotional voucher codes used to create trial certificates must be accompanied with a valid email address to allow additional instructions to be provided.
<code>-language LanguageCode</code>	- Specifies the output translation. Can be either en, fr, ja, nl, de, or es
<code>-natip NATIPAddress</code>	- The local IP address for NAT based networks. Only necessary if using a network translated IP
<code>-siteid IISSiteNumber</code>	- The ID number for the website in IIS. Use this if the site can not be automatically identified by the domain name.
<code>-debug</code>	- Verbose output for debugging problems
<code>-testurl WebServiceURL</code>	- Allows the use of alternative web service URL
<code>-quiet</code>	- Suppresses all output

REVOCATION

Revocation is a method whereby the SSL Certificate itself can be blacklisted to protect relying parties. It is usually completed when a private key has been stolen, compromised or deemed too weak to be used and therefore in danger of compromise. Revocation is something that should not be done lightly as revocation increases the size of the Certificate Revocation List (CRL) ±Blacklist, which has a cumulative effect from all SSL Certificate owners thereby slowing down connection speed of relying parties. Revocation is performed by sending the `-revoke` switch with the appropriate s/n of the certificate which requires revocation. Please note that the key material associated with the certificate will be deemed blacklisted by GlobalSign and therefore revocation should be done with caution.

```
C:\>oneclickssl -revoke 0100012698b9b97c oneclickssldemo.co.uk -natip 10.211.55.3
```

SSLPORT ±USING A PORT OTHER THAN THE DEFAULT PORT OF 443

Webservers usually operate on two standard ports. Port 80 for http traffic and Port 443 for https traffic. This is configurable and therefore the `-sslport` switch can be used to install on an alternative port for example 8080 in the example below.

```
C:\>oneclickssl DV78CLSWMRF3UDE1 oneclickssldemo.co.uk -natip 10.211.55.3 -sslport 8080
```

VOUCHEROPTION ±TYPICALLY YOUR E-MAIL ADDRESS

In some cases your hosting provider may issue you with a trial/test code for a short duration certificate or for a special offer. This type of multi-use voucher is not tied to a specific domain and therefore needs a point of contact for any errors in the issuance process and instructions on how to upgrade in the future. The `-voucheroption` switch is used here. Please note that the e-mail address can be any e-mail address and does not have to be associated with the domain to be secured. This is ideal for Gmail/Hotmail users.

```
C:\>oneclickssl SPECIALCODE oneclickssl.globalsign.com -natip 10.211.55.3 -
voucheroption my_email@mydomain.com
```

LANGUAGE OPTIONS ±CUSTOMIZE ERROR MESSAGES & FEEDBACK.

If the default of English is not your native language, you can modify the default language with the `-language` switch as follows.

English	en
French	fr
Spanish	es
Dutch	nl
German	de



Japanese ja

(coming soon)

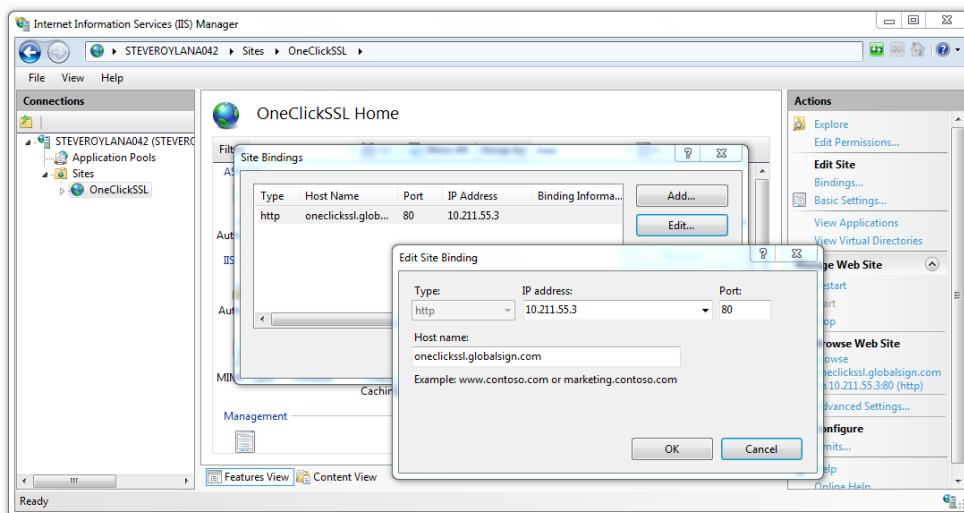
Korean ko
Chinese zh
Swedish se

```
C:\>oneclickssl DV78CLSWMR3UDE1 oneclickssl.globalsign.com -natip 10.211.55.3 -language de
```

NETWORK ADDRESS TRANSLATION \pm NATIPADDRESS

If your webserver is behind a firewall and the firewall uses NAT then you must indicate this to the installer too with the \pm natip switch. Your IIS web server will indicate the setting in the IP address bindings as shown below. In this case oneclickssl.globalsign.com resolves to 80.46.115.103.

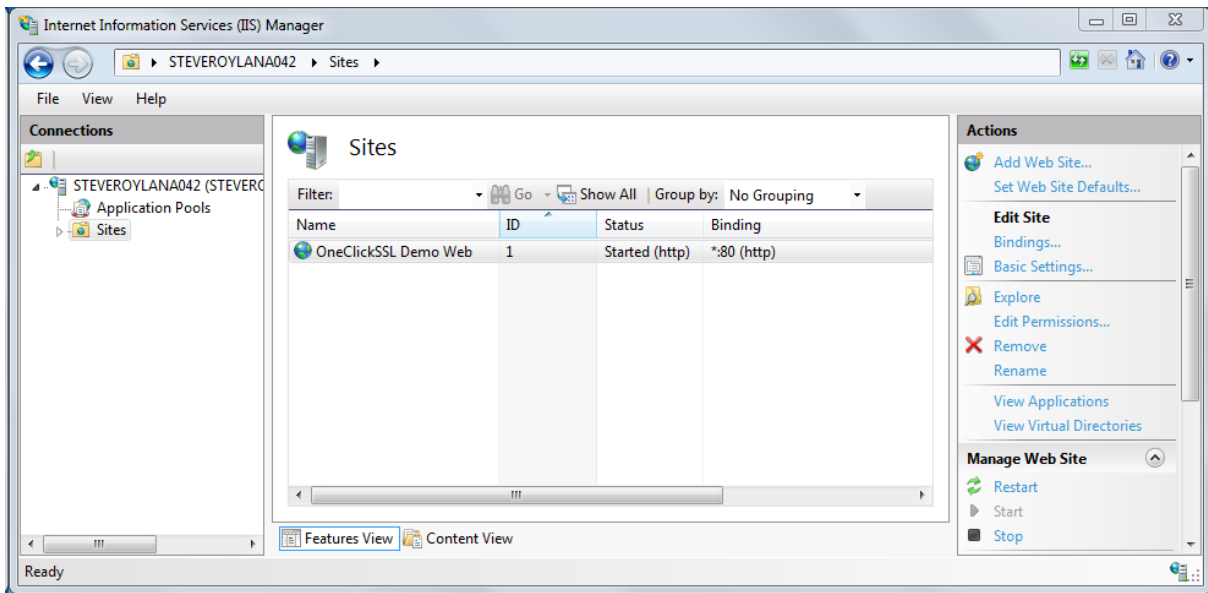
```
C:\>oneclickssl DV78CLSWMR3UDE1 oneclickssldemo.co.uk -natip 10.211.55.3
```



SITEID \pm WHEN IIS DOES NOT USE BINDING

In some cases websites are not bound to a domain name, therefore the site ID is used to identify the correct website to use. Not including the siteID switch would not allow the plug-in to identify the name of the website. (If you would prefer to select the name of the website then please use the GUI mode where this option is available.)

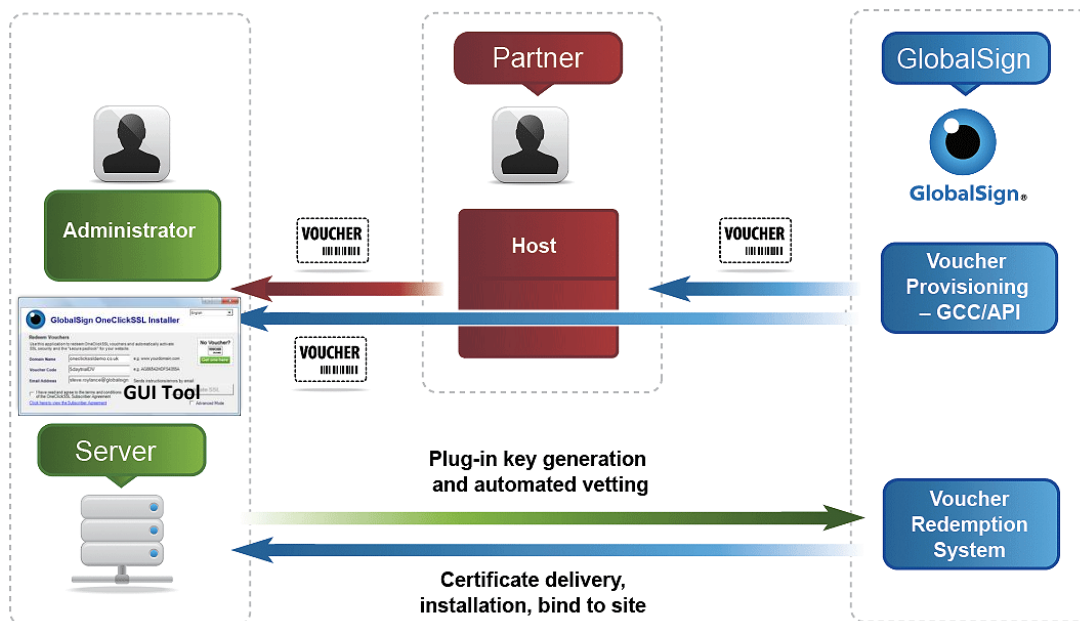
```
C:\>oneclickssl DV78CLSWMR3UDE1 oneclickssldemo.co.uk -natip 10.211.55.3 -siteid 1
```



AN OVERVIEW OF THE ONECLICKSSL SYSTEM ±GUI MODE

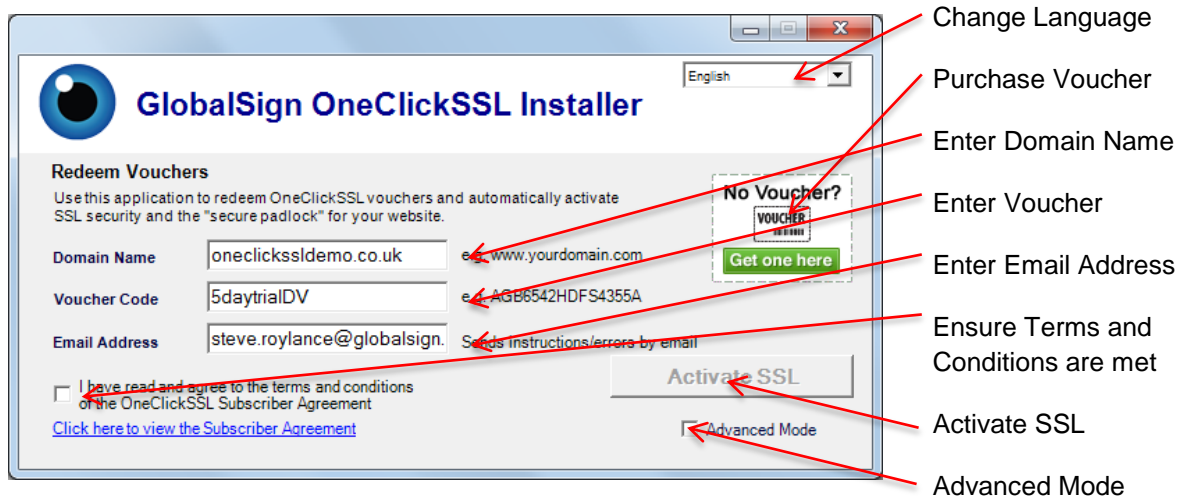
The OneClickSSL Graphical User Interface (GUI) tool offers a high degree of flexibility to administrators in that several switches/options are available to customize the certificate installation process. These include the ability to set up specific ports other than the default port 443 and to allow an SSL Certificate to be installed on a webserver that may have an internal non public IP through Network Address Translation).

/HW 1 V UHYLHZ WKH DUFK EWHFWXUH RI WKH VROXWLRQ



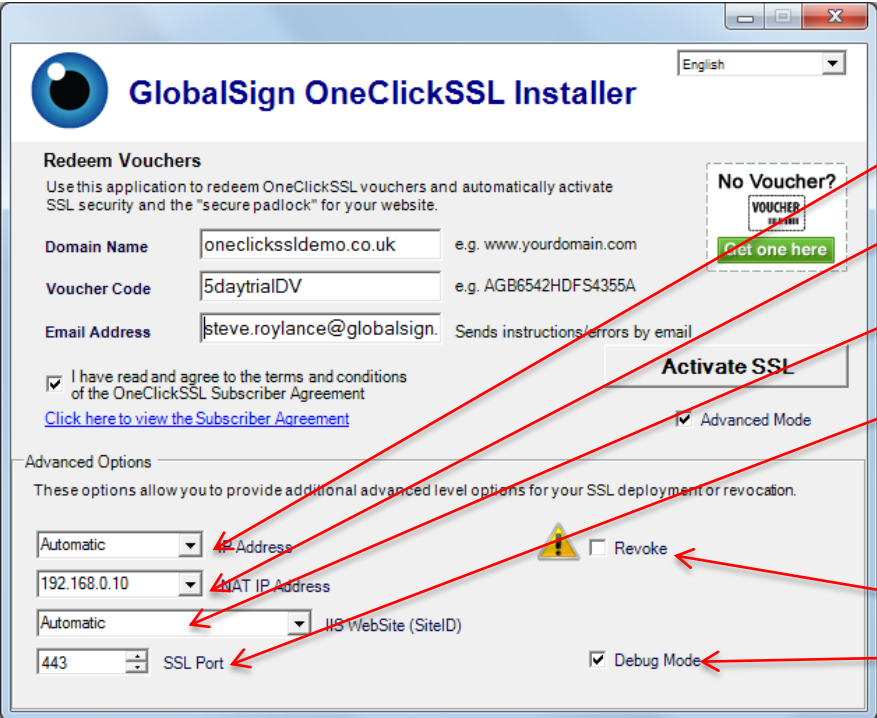
THE GUI INSTALLER - AN OVERVIEW

The basic GUI version of the Installer offers a similar selection of options to the CLI version.



THE GUI INSTALLER ±ADVANCED MODE

The Advanced Menu allows for specific customization options as shown below.



IP Address Selection

NAT IP Address Selection

IIS Web Site Name Selection

SSL Port

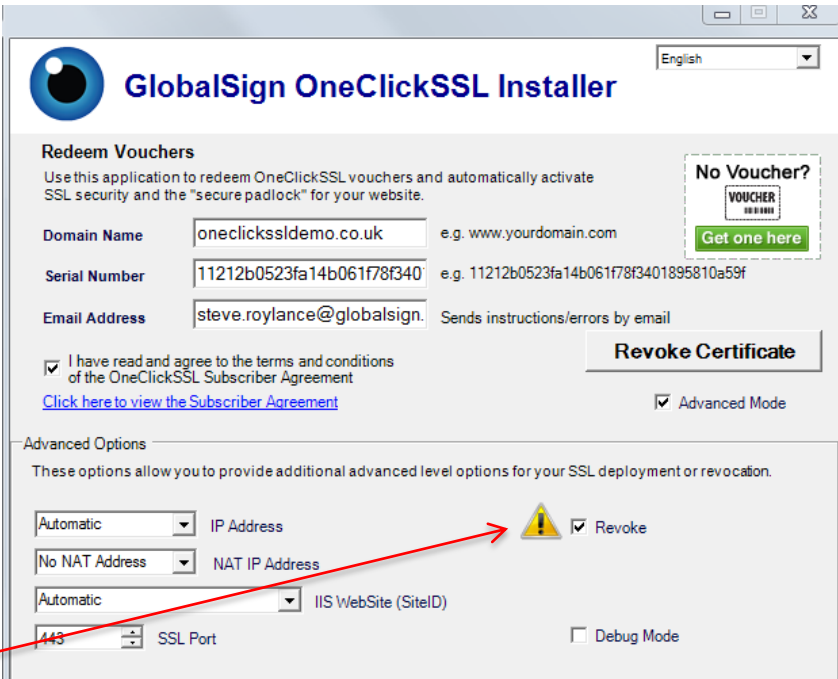
Revoke Mode

Debug Mode

Each of these sections will be covered in more detail in the following sections.

REVOCACTION

Revocation is a method whereby the SSL Certificate itself can be blacklisted to protect relying parties. It is usually completed when a private key has been stolen, compromised or deemed too weak to be used and therefore in danger of compromise. Revocation is something that should not be done lightly as revocation increases the size of the Certificate Revocation List (CRL) ± Blacklist, which has a cumulative effect from all SSL Certificate owners thereby slowing down connection speed of relying parties. Revocation is performed by checking the **Revoke** check box, agreeing to the warning message and entering the serial number of the certificate that requires revocation (*as well as the domain name and e-mail address*). Please note that the key material associated with the certificate will be deemed blacklisted by GlobalSign and therefore revocation should be done with caution.



SSLPORT ±USING A PORT OTHER THAN THE DEFAULT PORT OF 443

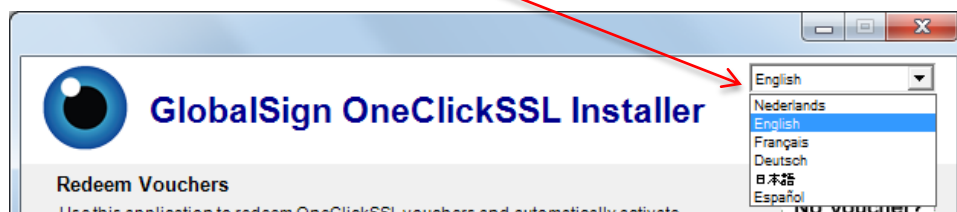
Webservers usually operate on two standard ports. Port 80 for http traffic and Port 443 for https traffic. This is configurable to allow installation on an alternative port for example 8080.

E-MAIL ADDRESS

In some cases your hosting provider may issue you with a trial/test code for a short duration certificate or for a special offer. This type of multi-use voucher is not tied to a specific domain and therefore needs a point of contact for any errors in the issuance process and instructions on how to upgrade in the future. Please note that the e-mail address can be any e-mail address and does not have to be associated with the domain to be secured. This is ideal for Gmail/Hotmail users.

LANGUAGE OPTIONS ±CUSTOMIZE ERROR MESSAGES & FEEDBACK.

If the default of English is not your native language, you can modify the default language with the pull down selection box in the top right hand corner.

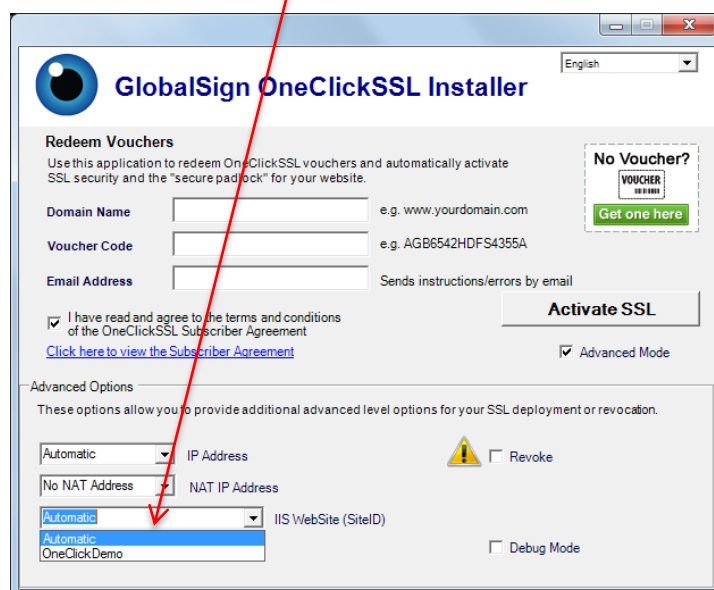


NETWORK ADDRESS TRANSLATION ±NATIPADDRESS

If your webserver is behind a firewall and the firewall uses NAT then you must indicate this to the installer too. Your NATIP options are available from the pull down selection.

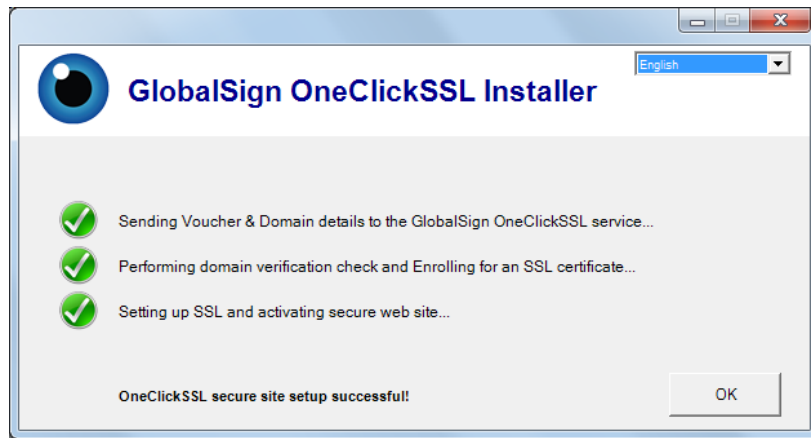
SITEID ±WHEN IIS DOES NOT USE BINDING

In some cases websites are not bound to a domain name, therefore the site ID is used to identify the correct website to use.



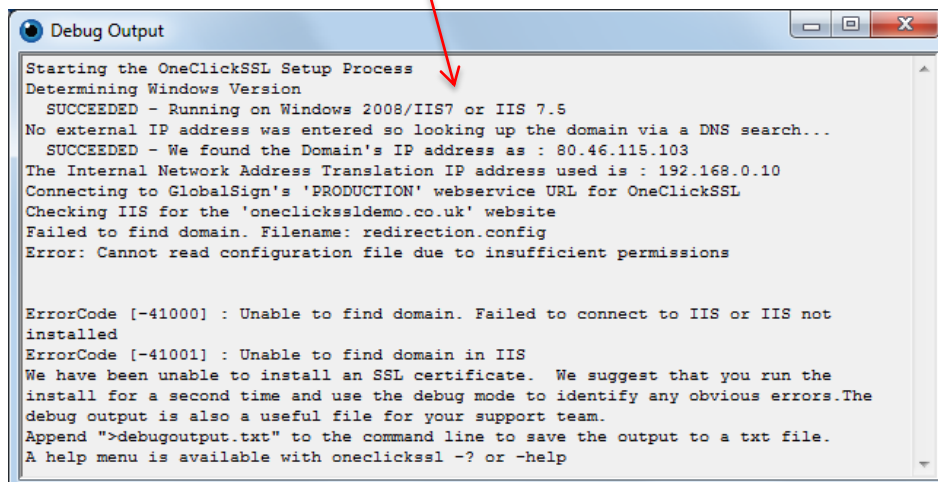
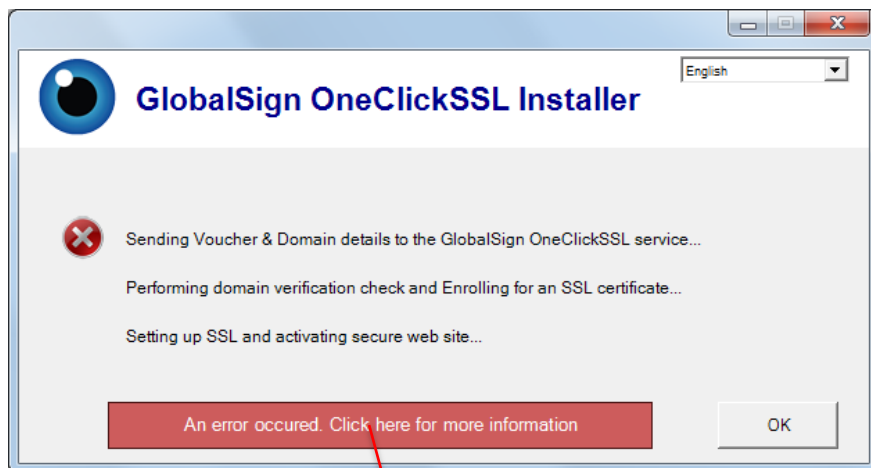
A SUCCESSFUL INSTALLATION

If everything has been configured correctly an SSL Certificate will be available for use by your IIS service within approximately 35-50 seconds. A summary of the process will be given at each major stage.



AN UNSUCCESSFUL INSTALLATION

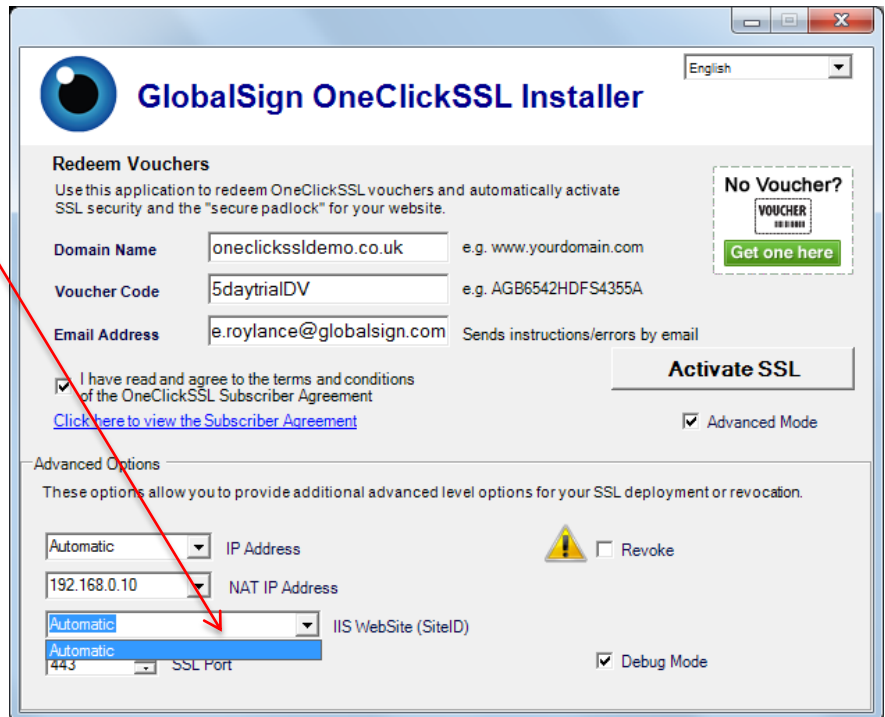
The advanced section offers a specific choice to view the process in debug mode. This provides useful warning messages to help identify problems. Regardless of this the debug Window may be viewed by pressing the Red Button following a failure.



TROUBLESHOOTING

ARE YOU SURE YOU ARE IN ADMINISTRATOR MODE?

One simple way to check if the tool is correctly running in Administrator mode is to see whether IIS offers a selection of websites inside the IIS Website (SiteID) pull down. If only Automatic is listed then either there is a configuration problem with IIS or the GUI is not running in administrator mode.



BEING CAUGHT FOR PHISHING

In some cases where an SSL Certificate is requested for a domain with suspicious keywords, such as %DQRNµ 0LFURVRIW¶ W Kalled for Security Measures DsQTHs called being caught for phishing. The OneClickSSL Installer 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.

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.

REVOCATION ± ERRORS WHEN ENTERING SERIAL NUMBERS

Users should note that when attempting to revoke, great care needs to be taken in selecting the correct serial number of the certificate you wish to revoke. 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**.

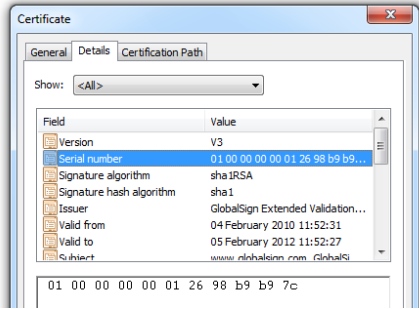
2 1 (& / , & . 6 6 / ERROR MESSAGES

ErrorCode	Error Description Returned	Resolution
-101	Invalid parameter entered. Please check	Please check that you have correctly

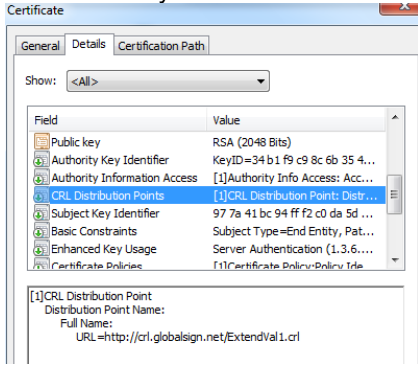
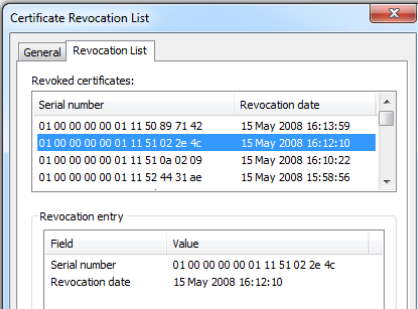


	the parameters match the API specification.	typed all the parameters. Use debug mode to see if any other information is presented.
-102	Mandatory parameter missing. Please check the parameters match the API specification.	, I \ R X K D Y H D μ 6 X S H U 9 R X F K H U ¶ I V o u c K H U ¶ W K H Q D Q H P D L O D G G U I P D Q G D W R U \ Z L W K W K H μ Y R X F K H
-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 webserver 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 T X H U L H G I U R P W K H μ S X E O L F ¶ , Q V 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 T X H U L H G I U R P W K H μ S X E O L F ¶ , Q V 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 T X H U L H G I U R P W K H μ S X E O L F ¶ , Q V 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 T X H U L H G I U R P W K H μ S X E O L F ¶ , Q V 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 S R V V L E O H μ S K L W K H I ¶ Q W I Z H H ¶ \ R X Z L need to contact your support team. An email 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	, W ¶ V X Q O L N H O \ E X W S R V V L E O H V



	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.	Key has been used by another entity. It is recommended to generate the key again. Running the process from the beginning will allow you to 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 note 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. , W P D \ F R Q W D L Q 2 ¶ V R K ¶ V D Q G 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.	: H F D Q ¶ W F R Q Q H F W W R \ R X U G R F 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 email 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. J 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	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



	certificate status.	<p>S/N is listed (Please allow up to 3 hours before checking as CRLs) are renewed every three hours.</p>  
-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 an 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 sometime tied directly to a domain. If you believe that the domain your 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, where as 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 W K L V H U R U H A M P V O U C H E R V L E O H 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 D G G U H V V U D Q J H , I \ R X K D Y H W 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 μ U H Q U Z D O I P. Unfortunately the original certificate has either been canceled,	Please contact the provider of your voucher.



	revoked or re-issued already, or the expiry date has now passed. Please contact support with detailed information concerning the issue.	
-9029	The Voucher you are using is for a 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.	HO\ WKH RULJLQDO 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.

Enhanced option settings ±Suitable for development work or testing environments:

TestURL – Primarily for Developers to test CLI automation hooks.

Use the `testurl` switch to run the CLI tool against a GlobalSign Test API WSDL system ±Developers should contact GlobalSign for specific details.

Quiet – Remove the debug and feedback information.

Use the `quiet` switch to run the CLI tool with no feedback to the console window.

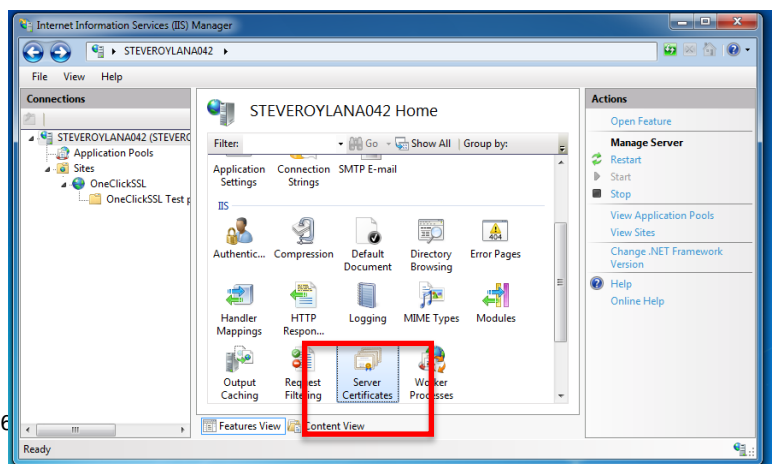
APPENDIX A

1. How to back up your certificates in IIS

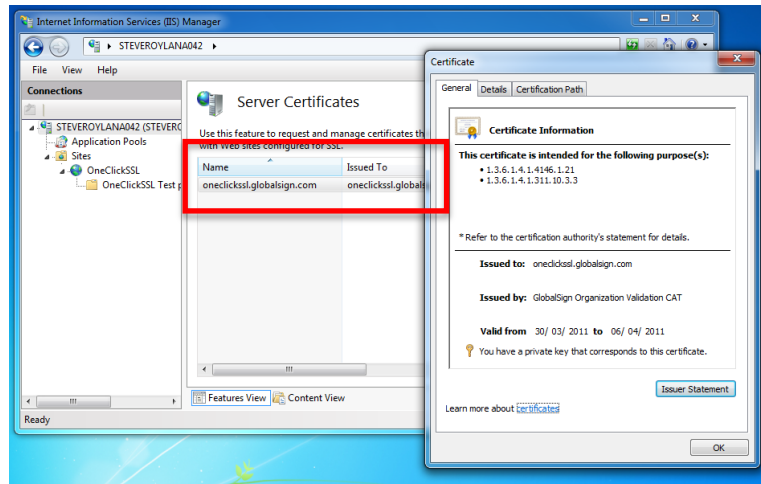
This section offers a quick review of the basic process on the IIS 7 platform ±For specific information on your version of IIS please review your Microsoft Help Guide.

Locate the SSL Digital Certificate Store within IIS.

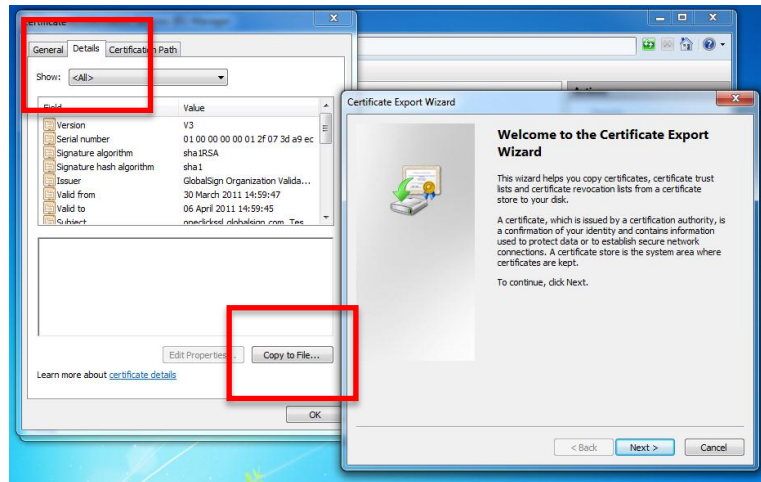
Double click on the existing certificate to open it in the Certificate Viewer within



Windows and check that it is the correct certificate.



& OLFN RQ WKH 3 'HWDLOV' WDE DQG 3 & RS\ WR)LOH' WR H[SRUW \RX
intermediates to a PKCS#12 file. (Saved in windows as a .pfx) ±Please use a STRONG
PASSWORD!





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