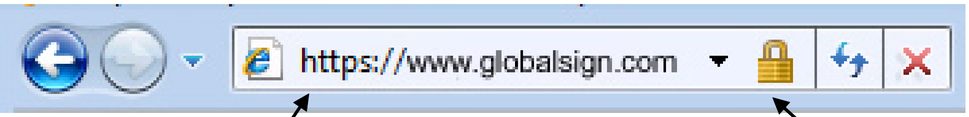
Ordering Guide for Domain SSL

1. Creating a CSR
2. The Ordering Process
3. The Vetting Process
4. Receiving your SSL Certificate
5. Installing your SSL Certificate.

Overview of Domain SSL

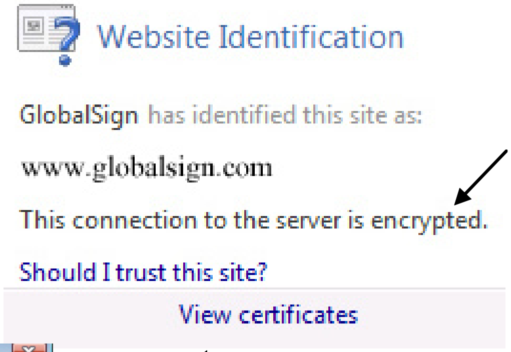
Domain SSL is ideal for businesses who are looking for a highly trusted SSL Certificate with industry standard encryption at low cost and quick issuance. With DomainSSL Certificates you activate the "little yellow padlock" and start securing e-commerce transactions, web account logins, webmail, network traffic, and online services in minutes.

A sample of a webpage with an Domain SSL can be viewed below:



https://www.globalsign.com

The standard HTTP is changed to HTTPS, automatically telling the browser that the connection between the server and browser must be secured using SSL



Website Identification

GlobalSign has identified this site as:

www.globalsign.com

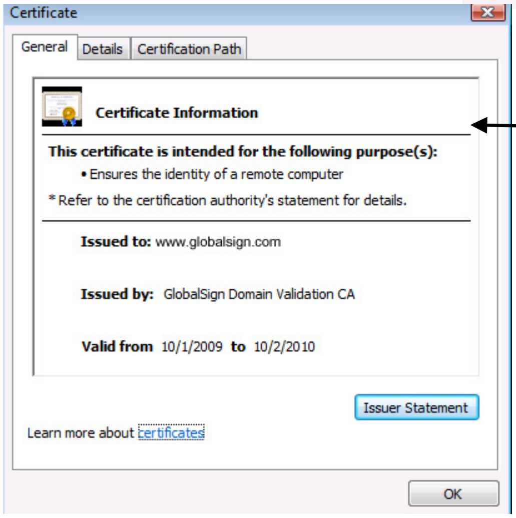
This connection to the server is encrypted.

Should I trust this site?

View certificates

The yellow padlock is activated, showing visitors that the browser connection to the server is now secure.

Furthermore, when visitors click on the padlock you will receive the following window which will confirm the Certificate Authority and that the connection is secure.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.globalsign.com

Issued by: GlobalSign Domain Validation CA

Valid from 10/1/2009 **to** 10/2/2010

Issuer Statement

Learn more about certificates

OK

A Domain SSL Certificate may appear different for each internet browser but a Domain SSL Certificate will show the following information:

- Issued to: (the common name the certificate is issued to)
- Issued By: (Who (what Certificate Authority) issued the certificate)
- Valid From: (the validity peroid of the certificate)

The Ordering Process

Step 1. Creating a CSR

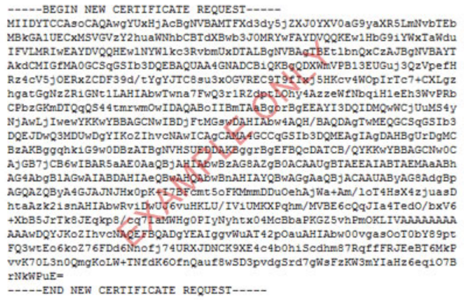
A Certificate Signing Request (usually referred to as a CSR) is a block of encrypted text file generated on a Web Server that the SSL Certificate will be installed on – the server hosting the domain name or hostname contained within the Certificate. The CSR contains information included within the Certificate, typically Organization Name, Common Name (domain name), Locality, and Country.

Auto CSR

With an DomainSSL, you have the option of creating your own CSR or using the free AutoCSR option when ordering and we'll create your SSL Certificate without you. CSR generation remains one of the consistent problem areas faced by customers wishing to secure servers and AutoCSR removes the need for the customer to create the CSR.

Creating your own CSR

Our support website can assist you to create a CSR with detailed instructions depending on what type of webserver you have (Apache, MS Exchange, Oracle, Colbalt, etc). Please locate these instructions at http://www.globalsign.com/support/csrgen.html


EXAMPLE ONLY

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYTCCAsoCAQAwgYUxHjAcBgNVBAMTFXd3dy5jZXJ0YXV0aG9yaXR5LmNvbTEb
MBkGA1UECxMSVGVzY2huaWNhbCBTdXBwb3J0MRYwFAYDVQQKEw1HbG91YWxTaWdu
IFVLMRIwEAYDVQQHEw1NYW1kc3RvbmUxDTALBgNVBAgTBEt1bnQxCzAJBgNVBAYT
AkdCMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXWmVPB13EUGuj3QzVpefH
Rz4cV5jOERxZCDF39d/tYgYJTC8su3xOGVREC9T9fIxj5HKcv4WOpIrTc7+CXLgz
hgatGgNzZRiGNt1LAHIAbwTwna7FwQ3r1RZdptLOhy4AzzeWfNbqiH1eEh3WvPRb
CPbzGKmDTQqQS44tmrwmOwIDAQABoIIBmTAaBgorBgEEAYI3DQIDMQwWCjUuMS4y
NjAwLjIwewYKKwYBBAGCNwIBDjFtMGswDAHIAbw4AQH/BAQDAgTwMEQGCSqGSIb3
DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMC
BzAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYBBAGCNw0C
AjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABTAEMAaABh
AG4AbgB1AGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUAByAG8AdgBp
AGQAZQByA4GJAJNJHx0pK+I7BFcmt5oFKMmmDDuOehAjWa+Am/loT4HsX4zjuasD
htaAzk2isnAHIAbwRviDwUJ6vuHKLU/IViUMKXPqhm/MVBE6cQqJIa4TedO/bxV6
+XbB5JrTk8JEqkp8/cq7IaMWHg0PIyNyhtx04McBbaPKGZ5vhPmOKLIVAAAAAAAA
AAAwDQYJKoZIhvcNAQEFBQADgYEAIggvWuAT42pOauAHIAbw00vgasOoT0bY89pt
FQ3wtEo6koZ76FDd6Nnofj74URXJDNCK9XE4c4b0hiScdhm87RqffFRJEeBT6MkP
vvK70L3n0QmgKoLW+TNfdK6OfnQauf8wSD3pvdgSrd7gWsFzKW3mYIaHz6eqiO7B
rNkWPuE=
-----END NEW CERTIFICATE REQUEST-----
```

Step 2. Placing your order online

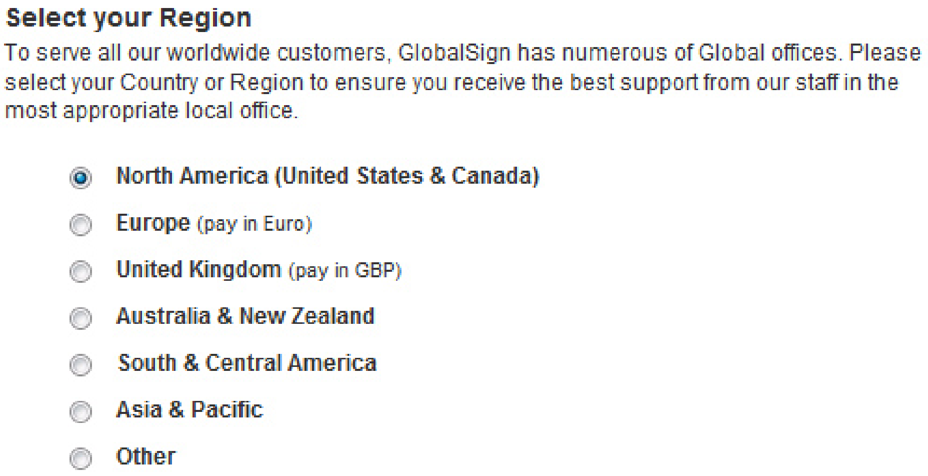
Ordering an Domain SSL Certificate contains multiple steps and various options. This guide will walk you through each option and steps.

Begin the Online Ordering Process

Click the "buy now" link on any DV SSL related page or go to: http://www.globalsign.com/ssl/buy-ssl-certificates/domain-ssl/buy-domain-ssl.html

Select your Region

To ensure you receive the best support from our staff please select the most appropriate office location.



Select your Region

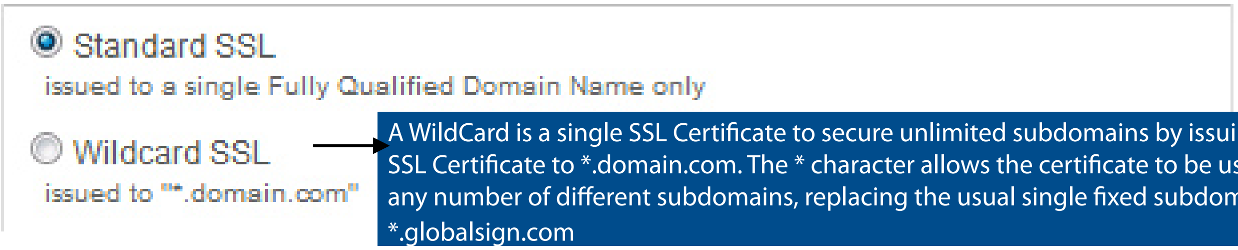
To serve all our worldwide customers, GlobalSign has numerous of Global offices. Please select your Country or Region to ensure you receive the best support from our staff in the most appropriate local office.

- ● North America (United States & Canada)
- ○ Europe (pay in Euro)
- ○ United Kingdom (pay in GBP)
- ○ Australia & New Zealand
- ○ South & Central America
- ○ Asia & Pacific
- ○ Other

Choose your options

Domain SSL Certificates allow you the option of a standard SSL or a WildCard SSL Certificate. Please see the below for further deails about your SSL options.

Option # 1- Choose your Certificate Type



● Standard SSL
issued to a single Fully Qualified Domain Name only

○ Wildcard SSL
issued to "*.domain.com"

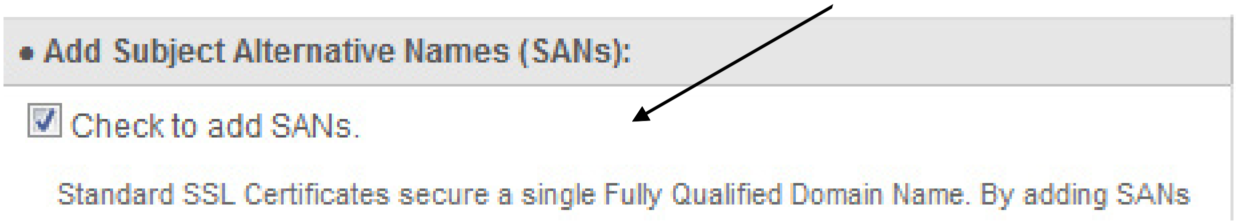
A WildCard is a single SSL Certificate to secure unlimited subdomains by issuing a SSL Certificate to *.domain.com. The * character allows the certificate to be used on any number of different subdomains, replacing the usual single fixed subdomain. *.globalsign.com

Option # 2- Adding Subject Alternative Names (SANs)

Adding the SANs option to your certificate allows you to secure up to 40 domain or server names using the same certificate including additional domain names and subdomains.

Additional Subdomains:	$ 99.00
Additional IP Address:	FREE
Additional Local Host:	FREE
Additional Domains:	Not Available for Domain SSL

If you wish to secure additional subdomains please check off the appropriate box to add SANs. You will be able to configure your SANs on the next page.



• Add Subject Alternative Names (SANs):

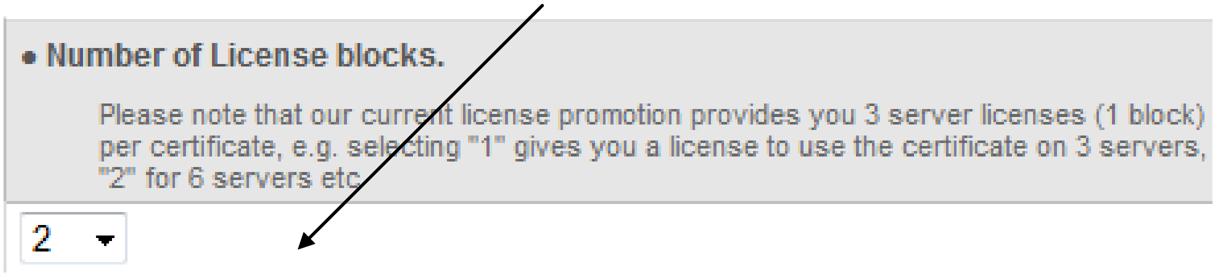
☑ Check to add SANs.

Standard SSL Certificates secure a single Fully Qualified Domain Name. By adding SANs

Option #3- Choosing the number of License Blocks you need.

GlobalSign offers 3 for 1 server licensing program. One "License Block" gives you the ability to secure three servers with one Certificate. Therefore two "License Blocks" will secure six servers, three "License Blocks" will secure nine servers, and so on.

Select how many license blocks you wish to allocate to your SSL Certificate.



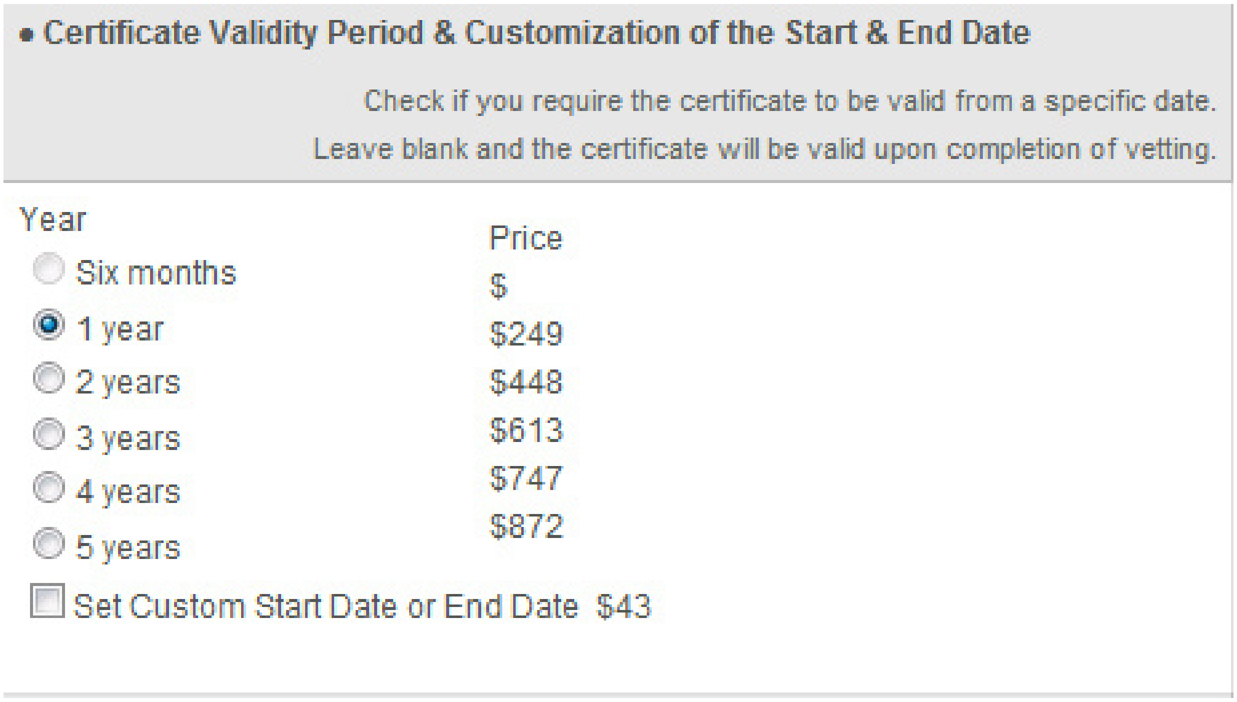
• Number of License blocks.

Please note that our current license promotion provides you 3 server licenses (1 block) per certificate, e.g. selecting "1" gives you a license to use the certificate on 3 servers, "2" for 6 servers etc.

2 ▾

Option #4- Certificate Duration

Choose the validity period of your certificate, up to five years. You also have the ability to customize your start and end dates.



• Certificate Validity Period & Customization of the Start & End Date

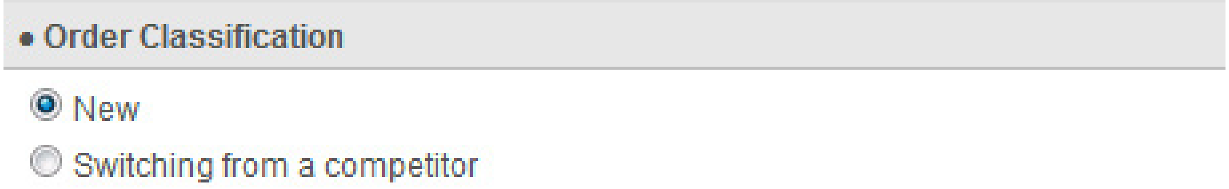
Check if you require the certificate to be valid from a specific date.
Leave blank and the certificate will be valid upon completion of vetting.

Year	Price
○ Six months	$
● 1 year	$249
○ 2 years	$448
○ 3 years	$613
○ 4 years	$747
○ 5 years	$872

□ Set Custom Start Date or End Date $43

Option 5- Choose if you are ordering a new certificate or switching from a competitor

If you are replacing your existing SSL Certificate with a GlobalSign SSL we will give you all the time remaining onto your new certificate plus 30 days added free of charge!



• Order Classification

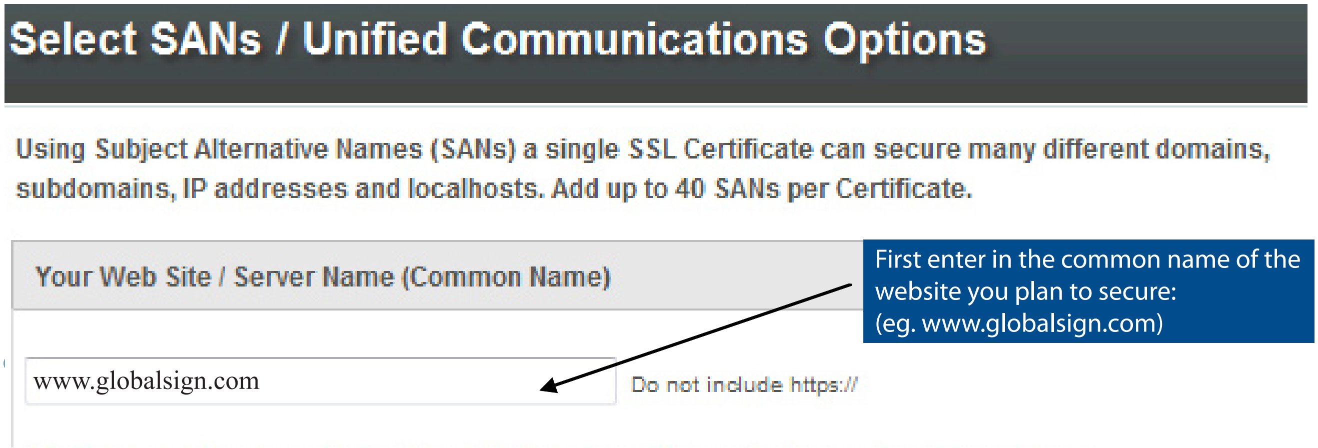
● New
○ Switching from a competitor

Configure your options-If you did not select the SANs option please skip this section and go to pg 6.

The next screen brings you to the option page to configure your SANs/Unified Communications Certificate.

Configure Option #1- Define your SANs

Define your Common Name (domain name, e.g. www.globalsign.com)



Select SANs / Unified Communications Options

Using Subject Alternative Names (SANs) a single SSL Certificate can secure many different domains, subdomains, IP addresses and localhosts. Add up to 40 SANs per Certificate.

Your Web Site / Server Name (Common Name)

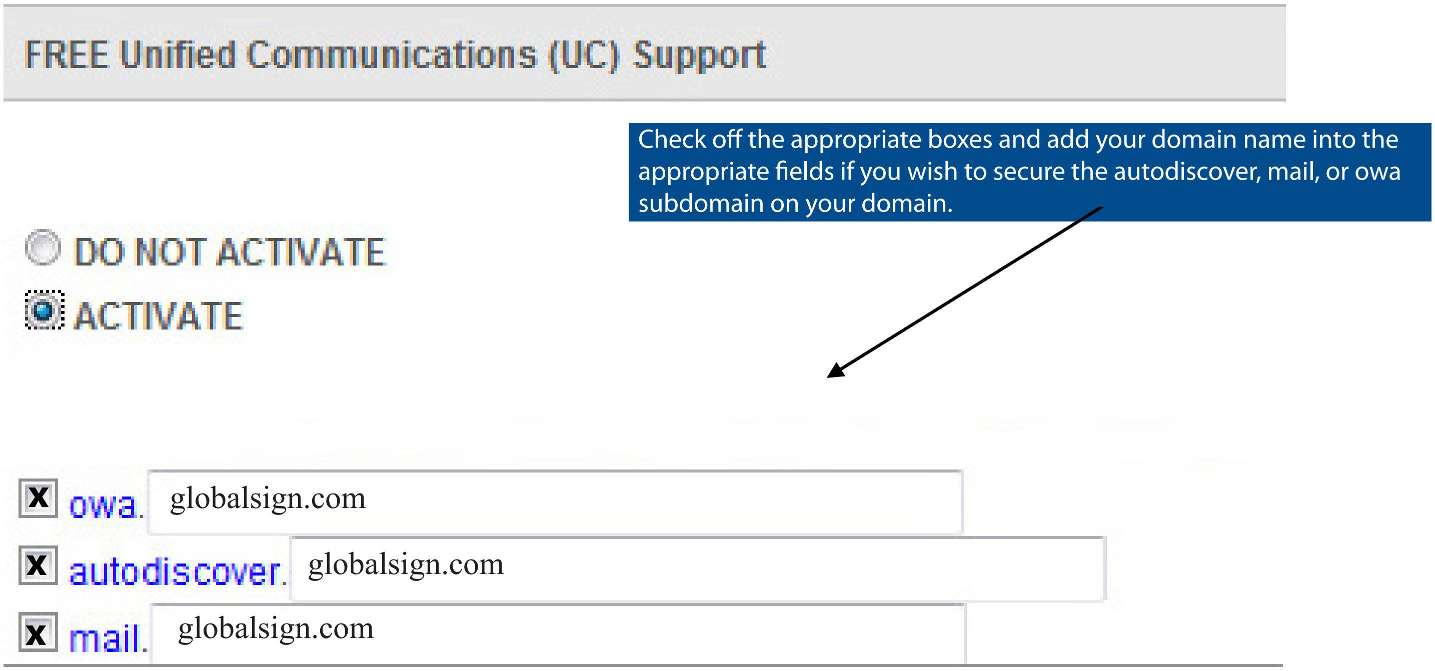
www.globalsign.com

Do not include https://

First enter in the common name of the website you plan to secure: (eg. www.globalsign.com)

Configure Option #2- Activate Unified Communications

Secure the autodiscover, mail, & owa subdomains on your domain for Exchange 2007 Server Office Communications. For the UC implementation, add the required Subdomains in the "additional subdomain" section



FREE Unified Communications (UC) Support

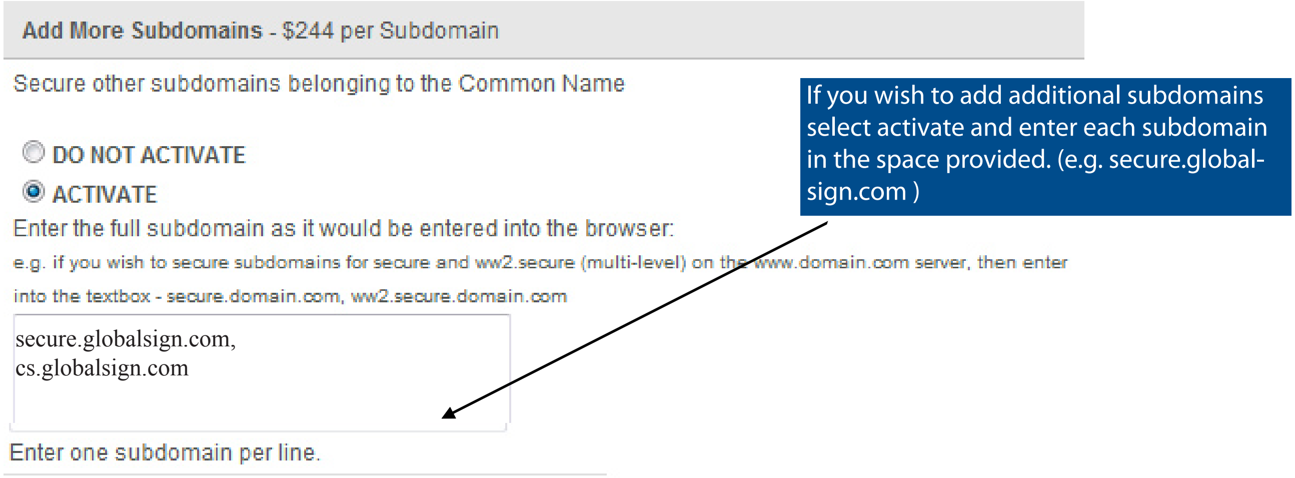
Check off the appropriate boxes and add your domain name into the appropriate fields if you wish to secure the autodiscover, mail, or owa subdomain on your domain.

○ DO NOT ACTIVATE
● ACTIVATE

☒ owa. globalsign.com
☒ autodiscover. globalsign.com
☒ mail. globalsign.com

Configure Option #3- Add additional subdomains

The next step you will have the option to add additional subdomains. Subdomains are commonly used by organizations that wish to assign a unique name to a particular department, function, or service related to the organization. Example: secure.globalsign.com, cs.globalsign.com



Add More Subdomains - $244 per Subdomain

Secure other subdomains belonging to the Common Name

If you wish to add additional subdomains select activate and enter each subdomain in the space provided. (e.g. secure.globalsign.com)

○ DO NOT ACTIVATE
● ACTIVATE

Enter the full subdomain as it would be entered into the browser:

e.g. if you wish to secure subdomains for secure and ww2.secure (multi-level) on the www.domain.com server, then enter into the textbox - secure.domain.com, ww2.secure.domain.com

secure.globalsign.com,
cs.globalsign.com

Enter one subdomain per line.

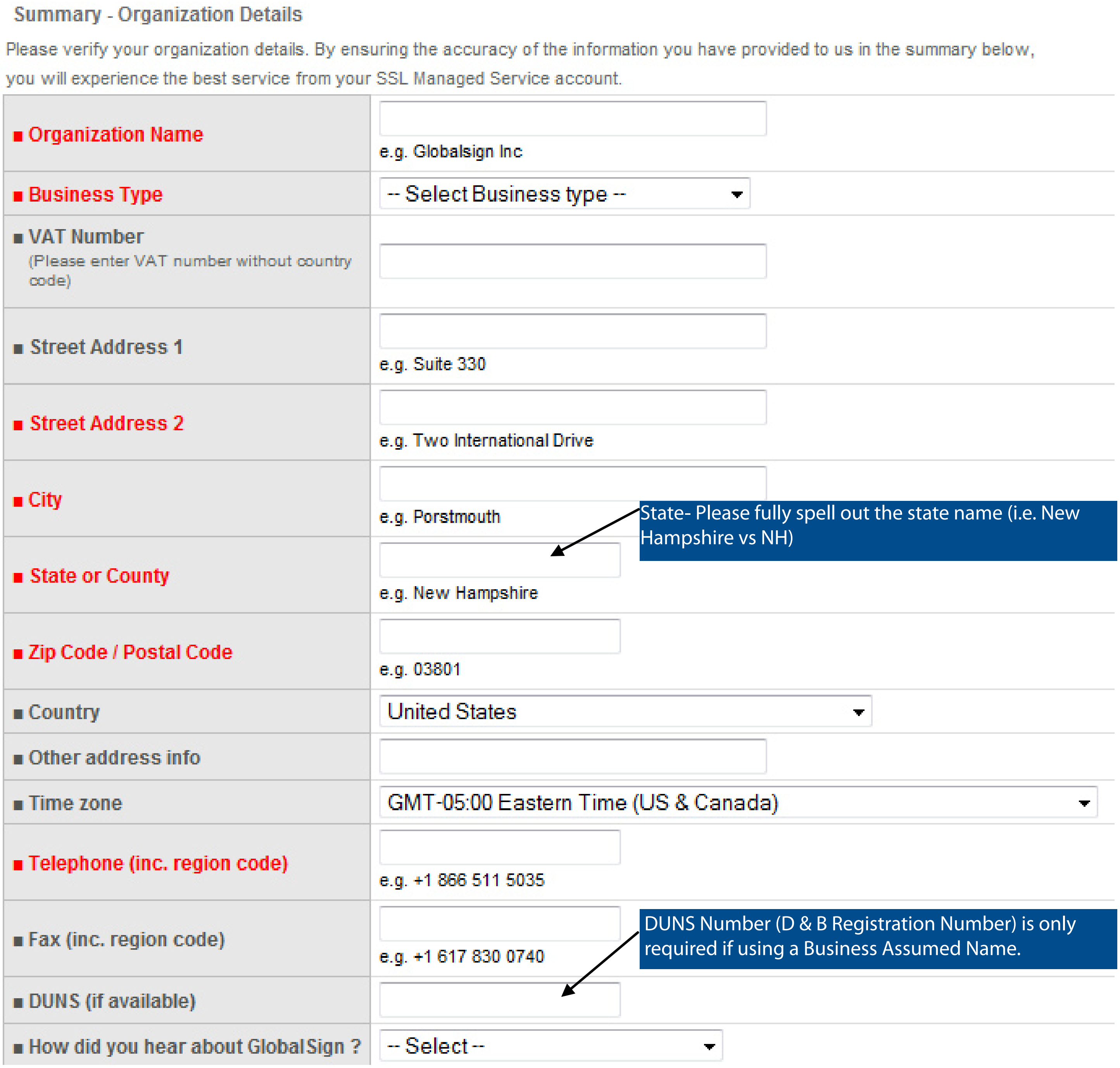
The next page will give you a confirmation page that will summarize the new product details of your Certificate including updated pricing, new subdomains, and new domain names.

Account Setup

Account Setup (Stage 1/3)

Once you have chosen and configured your options, (e.g. SANs) you will need to set up your account. Setting up your account consists of a few steps:

1. **Enter your Organization and Account Administrator details-** Please verify your organization details and provide atleast the minimum required fields.



Summary - Organization Details

Please verify your organization details. By ensuring the accuracy of the information you have provided to us in the summary below, you will experience the best service from your SSL Managed Service account.

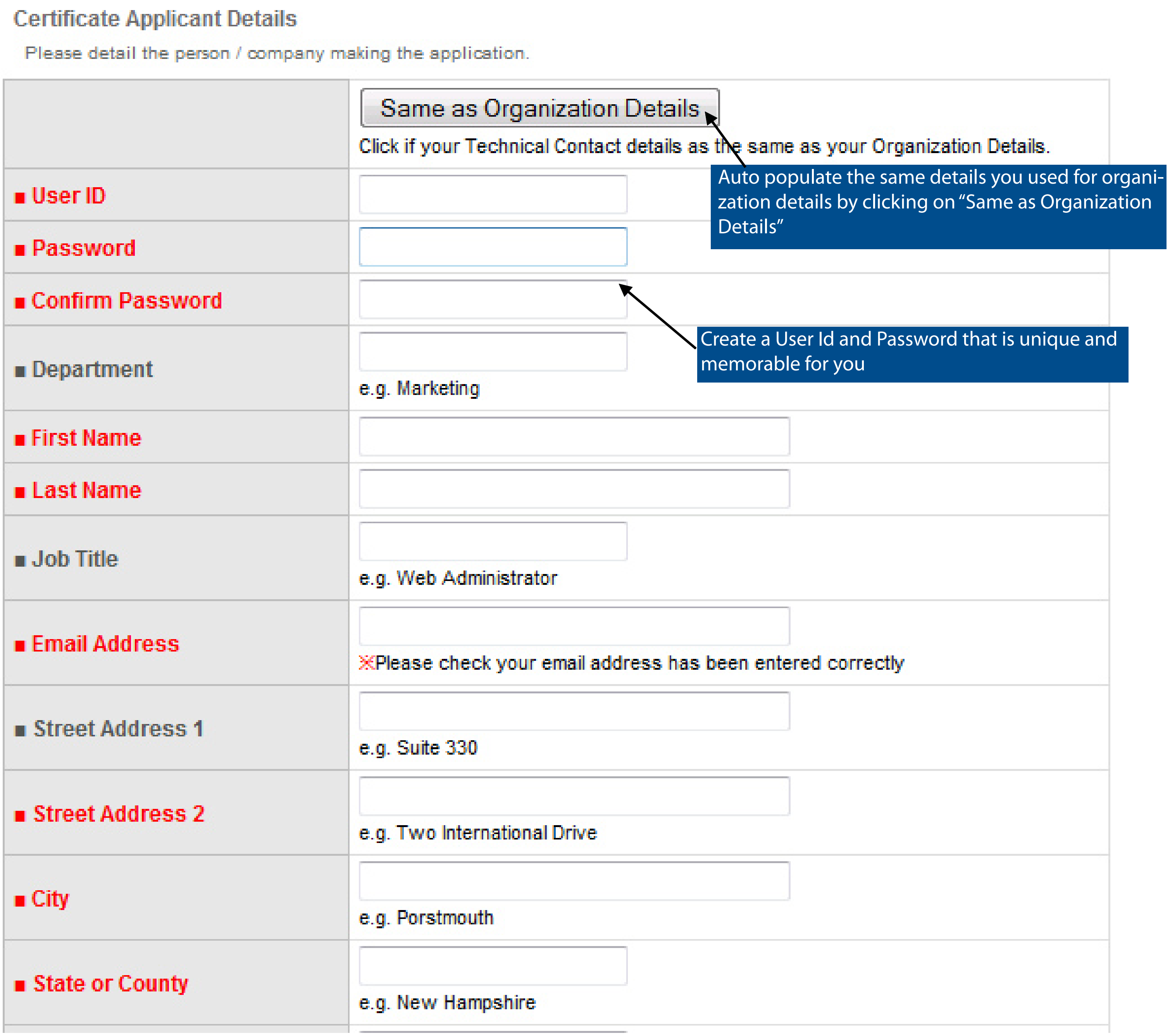
■ Organization Name	e.g. Globalsign Inc
■ Business Type	-- Select Business type -- ▾
■ VAT Number (Please enter VAT number without country code)	
■ Street Address 1	e.g. Suite 330
■ Street Address 2	e.g. Two International Drive
■ City	e.g. Porstmouth
■ State or County	e.g. New Hampshire
■ Zip Code / Postal Code	e.g. 03801
■ Country	United States ▾
■ Other address info	
■ Time zone	GMT-05:00 Eastern Time (US & Canada) ▾
■ Telephone (inc. region code)	e.g. +1 866 511 5035
■ Fax (inc. region code)	e.g. +1 617 830 0740
■ DUNS (if available)	
■ How did you hear about GlobalSign ?	-- Select -- ▾

State- Please fully spell out the state name (i.e. New Hampshire vs NH)

DUNS Number (D & B Registration Number) is only required if using a Business Assumed Name.

Account Setup (Stage 2/3)

2. **Enter the "applicant" details-** (yourself, or whoever is considered to be the applicant). When entering the "applicant" information, organization details can be auto populated from the previous screen.



Certificate Applicant Details

Please detail the person / company making the application.

	Same as Organization Details Click if your Technical Contact details as the same as your Organization Details.
■ User ID	
■ Password	
■ Confirm Password	
■ Department	e.g. Marketing
■ First Name	
■ Last Name	
■ Job Title	e.g. Web Administrator
■ Email Address	※Please check your email address has been entered correctly
■ Street Address 1	e.g. Suite 330
■ Street Address 2	e.g. Two International Drive
■ City	e.g. Porstmouth
■ State or County	e.g. New Hampshire

Auto populate the same details you used for organization details by clicking on "Same as Organization Details"

Create a User Id and Password that is unique and memorable for you

Account Setup (Stage 3/3)

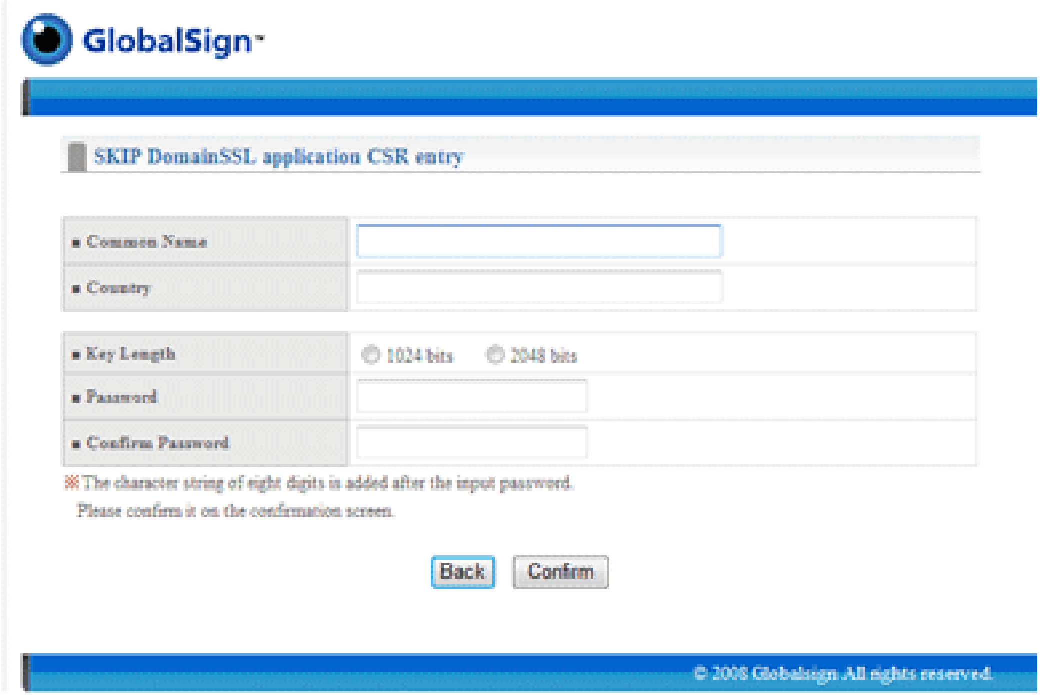
3. **Billing Contact Inforamtion-** Please enter the details of any billing contact or accountant for your organization. If this person is yourself, then simply check the box marked "Check box if same as Application Details" and this will automatically populate the fields you previously entered.

4. **Terms & Conditions-** Next review your account information and the Terms and Conditions,. Upon completion, please select "I agree".

Account Setup (Stage 3/3)

5. **Choose Common Name & Key Length-** Next you will be prompted to enter your "Common Name" (domain name), your country code using two characters (example: US, JP, UK, etc), and a password of at least 8 characters that contains both letters and numbers.

The system will append your chosen password with a randomly generated string to further strength the security of the pfx file.



SKIP DomainSSL application CSR entry

- Common Name
- Country

- Key Length ○ 1024 bits ○ 2048 bits
- Password
- Confirm Password

※The character string of eight digits is added after the input password.
Please confirm it on the confirmation screen.

© 2008 Globalsign All rights reserved.

6. **Choose an email address** to which GlobalSign can send an e-mail challenge. A pre-populated list will appear, please choose an email from the list and click the next button.

7. **Complete Payment Details**. Please complete the payment details for your order and continue. A summary screen detailing your account name and order ID is displayed, please make note of these for future references.

Step 3. The Vetting Process

The ordering process for Domain SSL Certificates is completely automated unless an order is flagged for phishing, in which case GlobalSign will manually clear after additional vetting is completed, if necessary.

Once an order has been placed, our Vetting Department verifies the domain ownership and the domain undergoes phishing checks before being released. If caught for phishing it may be becuase the domain may have a keyword that prompted the system to fault it and a vetting officer will promptly clear the flag, releasing the approval e-mail.

In some circumstances, the order will be flagged for additional vetting (examples: financially related site/ or brand name or trademarked domain names) and a vetting officer will contact the end user for any required supporting documentation. Once the order is placed, an approval e-mail will be sent to the selected e-mail address. Once confirmed the order will issue on its own.

Note: The approval e-mail can be sent to any of the general e-mails listed below or the e-mail address listed on the Whois record. If the e-mail on the Whois record isn't displayed during the application process, we advise the customer to choose a generic e-mail and contact Support to indicate they would like the approval e-mail address to be changed to the one listed on t he Whois record for the domain. A vetting agent would then verify the details and re-send the approval e-mail to the selected Whois address.

admin@domain.com
adminstrator@domain.com
hostmaster@domain.com
root@domain.com
ssladmin@domain.com
sysadmin@domain.com
webmaster@domain.com
postmaster@domain.com

Step 4. Receiving your SSL Certificate

Once the order is placed, an approval e-mail will be sent to the selected e-mail address and the order will be issued on its own. Thereafter you will receive an e-mail from GlobalSign with instructions on how to install your certificate.

You can also login into your GlobalSign Certificate Center (GCC) account and download your SSL Certificate. To login to your GCC Account please visit: http://www.globalsign.com/login/

Step 5. Installing your SSL Certificate

Installing a SSL Certificate will depend on the type of server software you have. Full instructions for all server types can be found at http://www.globalsign.com/support/installcert.php.

Most Commonly Asked Questions- FAQ Section

How many servers can I secure with one SSL Certificate?

To help you meet your budget GlobalSign certificates are provided with 3 for 1 server licenses included in the standard price. This allows you to easily secure your primary server, a secondary or backup server and a load balancer without any further costs. Additional licenses can be purchased in blocks of 3 for the industry's most competitive server licensing rates.

To move your certificate between servers you will need to firstly install the certificate on the same web server that you generated the CSR from and then export the SSL certificate and its private key to a PFX or PKCS12 file, which can then be imported to another web server.

How do I use the WildCard SSL Certificate?

A single Wildcard SSL Certificate can secure multiple Web Sites. Typically a standard secure server SSL Certificate is issued to a single Fully Qualified Domain Name only, which means it can only be used on the exact domain (including sub-domain) to which it has been issued. With the Wildcard SSL option activated you easily get around this restriction by receiving a Wildcard SSL Certificate issued to *.domain.com. The * character replaces a "fixed" sub-domain with a "variable" one.

Can I secure my top level domain with and without the "www." sub-domain?

SSL Certificates are usually issued to a sole Fully Qualified Domain Names (FQDN), so normally customers wanting to secure both https://www.globalsign.com and https://globalsign.com would need two separate SSL Certificates. With GlobalSign SSL Certificates if you purchase an SSL Certificate to secure www.domain.com it will also secure domain.com.

Can I secure my Public IP Address?

Typically a SSL Certificate is issued to a Fully Qualified Domain Name (FQDN) such as www.domain.com. However some organizations need a SSL Certificate issued to an IP address. This option allows you to specify an IP address as the Common Name in your Certificate Signing Request. The issued certificate can then be used to secure connections directly with the IP address, e.g. https://123.456.78.99.

Notes: Only Public IP Addresses may be used. You must be the owner of the IP Address as per records held at RIPE. Make sure you create a CSR with a common name of your IP address, e.g 123.456.78.90.

Can I customize my SSL Certificate start and end dates?

Bring all your SSL Certificates into line and have them co-terminating on the same day. This option allows you to set a Start Date and an End Date within the validity period of the certificate. For organizations that wish to dictate a time period, e.g. a week, in which all certificate renewals must take place, specifying a End Date will ensure the Administrators commit to this activity. Furthermore, setting a Start Date allows SSL Certificates for future projects to be applied for, paid for and issued now, but will not become valid and usable until the chosen Start Date has been reached.

Does GlobalSign provide test server certificates?

Yes, please see http://www.globalsign.com/free-ssl-certificate/free-ssl.html for free 45 day Trial SSL Certificates.

Would a user need his own Personal Certificate to access information securely on a webserver?

The user doesn't necessarily need his own personal certificate to have access to a secure server. However, the secure server can be configured to explicitly ask for the user to select and present a personal certificate (eg. a PersonalSign certificate) before entering a certain page. This is an extra feature of Secure Socket Layer (SSL) v3. In this way, the SSL server also has an idea of who is accessing the site, and can decide whether or not to let that person access certain information.

How do I (as user) verify I have accessed a trusted secure server?

If you access a server secured with a GlobalSign SSL Certificate, you will see a padlock at the bottom of your browser. If you click on it, you will see the details of the server's SSL Certificate.

How can I have 128 bits encryption key length for SSL when using Windows 2000 with IIS 5.0?

Upgrade to Strong Encryption Pack for Windows 2000, here is the URL for Installing it:
http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp.

Which webservers are compatible with GlobalSign's Secure Server Certificates?

GlobalSign issues Secure Server Certificates for any server compatible with the standard x509 v3 and able to make a request in PKCS#10 format. That includes the majority of all recent servers, in particular:

* Microsoft Internet Information Server (IIS) v3 or higher
* Netscape Enterprise Server v3 or higher
* Netscape Commerce Server v1 or higher
* Netscape FastTrack Server
* Stronghold Server
* Internet Application Server 1.0
* Netscape Iplanet Web Server 4.1

NOTE: For Apache Servers, a patch for SSL is needed (http://www.apache-ssl.org/).

Still can't find the answer to your question or need help?

If have any questions about the ordering process for a Domain SSL Certificate, please visit our support webpage for the most common FAQ. If you can't find the answer you need, please contact our support team:

Create a Support Ticket: http://www.globalsign.com/help/- Submit a support ticket
Online Form: http://www.globalsign.com/leadgen/general.html- Send a message for GlobalSign to contact you
E-mail: support@globalsign.com
Tel: 1-866-503-5375

GlobalSign Inc
Two International Drive Suite 330
Portsmouth, NH 03801
+1- 603-570-7091
http://www.globalsign.com