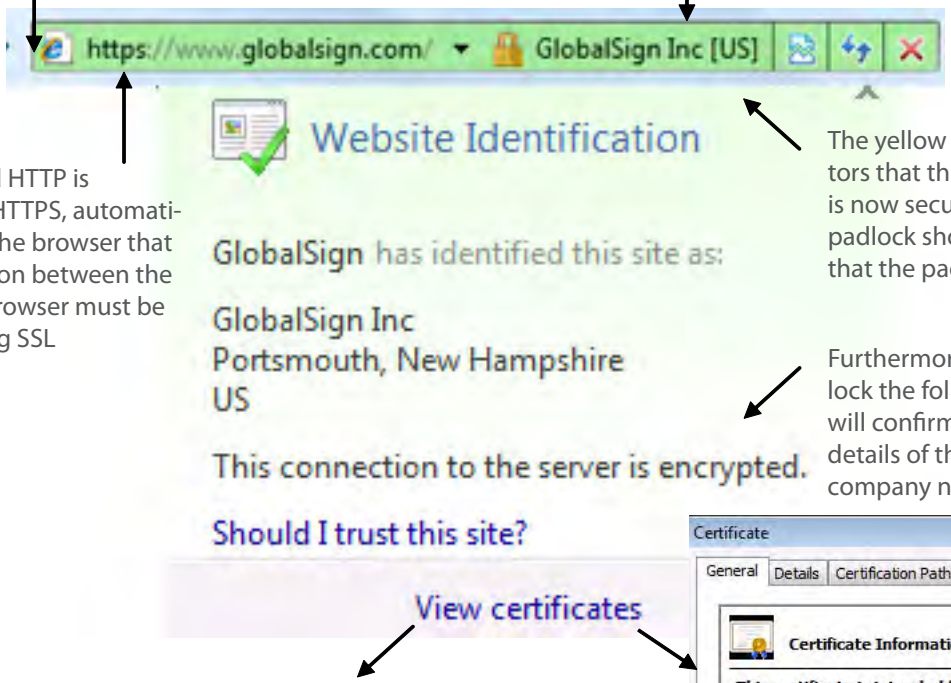
Ordering Guide for Extended Validation SSL

Overview of Extended Validation (EV) SSL

Extended Validation SSL is ideal for businesses who are looking for the highest levels of trust. The Extended Validation SSL has advanced features over other SSL Certificates including turning the address bar green and showing visitors your company name. By turning the address bar green visitors will be able to quickly identify that the website is using an Extended Validation SSL and will provide confidence to the end user.

The address bar turns from white to green, indicating to visitors that the web site is using Extended Validation SSL

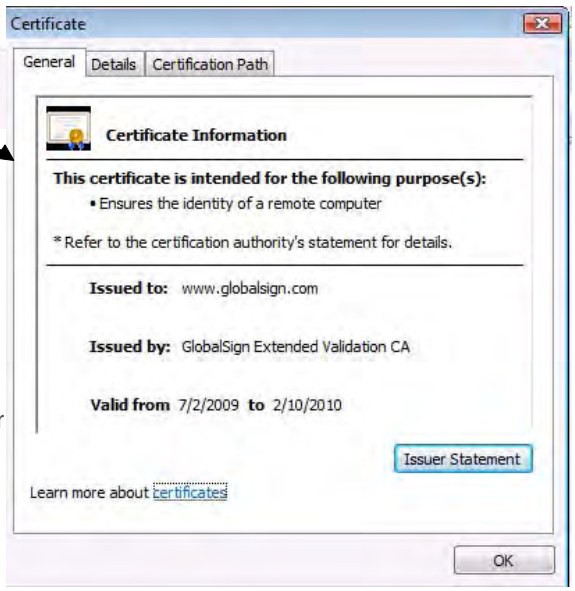
The website owner's legally incorporated company name is displayed prominently on the address bar.



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

The yellow padlock is activated, showing visitors that the browser connection to the server is now secure. If there is no padlock or the padlock shows a broken symbol, this indicates that the page does not use SSL.

Furthermore, when visitors click on the padlock the following window will appear which will confirm the Certificate Authority and the details of the website owner including the company name, city, state, and country code.



Clicking "View Certificates" will display a profile giving further details:

- Issued to: (the common name the certificate is issued to)
- Issued by: (The Certificate Authority who issued the certificate)
-Valid from: (the validity period of the certificate)

These appearance of the profile may appear different for each web browser (Firefox, Internet Explorer, Safari, etc)

Step 1. Vetting Preparation/Extended Validation Guidelines

Extended Validation SSL Certificates have a unique ordering process due to its strictly defined guidelines which have been formed by the CA/Browser form. These guidelines contain specific steps required for the Certificate Authority (Such as GlobalSign) to follow before issuing a certificate. All Certificate Authorities must follow the same guidelines.

As a business entity you will want to make sure you meet the following requirements before applying for an EV SSL:

1. The business entity must be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its Jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency.

2. The business entity must have a verifiable physical existence and business presence

3. At least one principal individual associated with the business entity must be identified and validated

4. The identified principal individual must attest to the representations made in the Subscriber Agreement

5. Where the business entity represents itself under an assumed name, the CA must verify the business entity's use of the assumed name (i.e. American International Group, Inc has a Business Assumed name of AIG). A business assumed named is only required if business is conducted under a different name.

6. The business entity and the identified principal individual associated with the business entity must not be located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction.

7. The business entity and the identified principal individual associated with the business entity must not be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Step 2. CSR Generation

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.

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

Important things to remember when creating the CSR:

1. The Organization Name needs to be the full registered name
2. The Organization Unit is optional
3. City and State fields need to be spelled out
(i.e. New Hampshire not NH)

Step 3. Online Ordering Process

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

Begin the Online Ordering Process

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

Select your Region

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

Choose Options

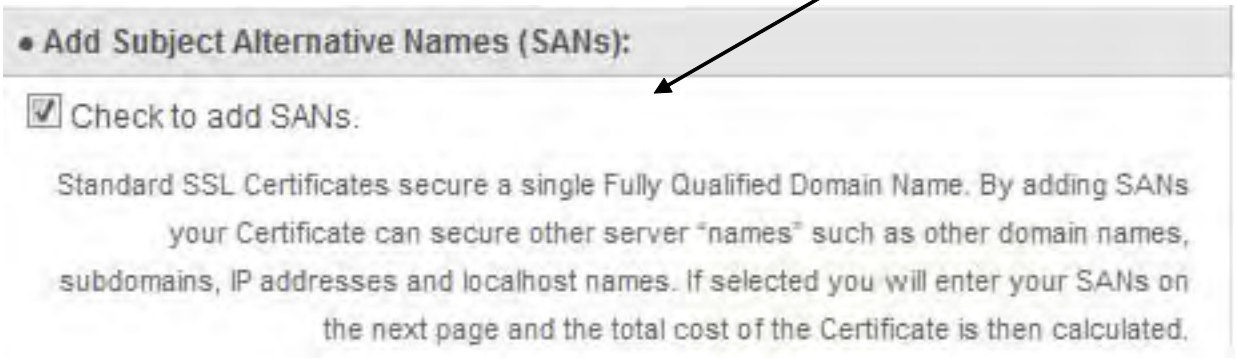
The next screen brings you to the option page for your Certificate, there are various options to choose from to enhance your Certificate.

Option #1-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.

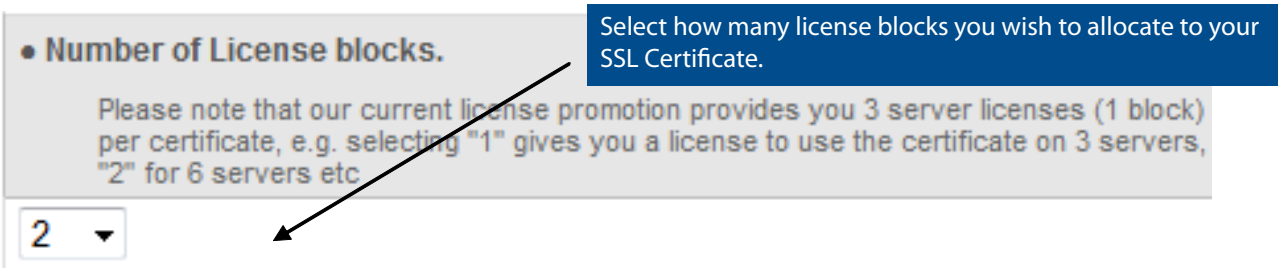
Additional Domain Name: $199 /each
Additional Subdomain Name: $99/each

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



Option #2- 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 3 servers with one Certificate. Therefore 2 "License Blocks" will secure 6 servers, 3 "License Blocks" will secure 9 servers, and so on.



Option #4- Certificate Duration

Next, please choose the validity period of your certificate, 2 year maximum for Extended Validation SSL. You also have the ability to customize your start and end dates.

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!

Configure your options-If you did not select the SANS option please skip this section and go to pg 7.

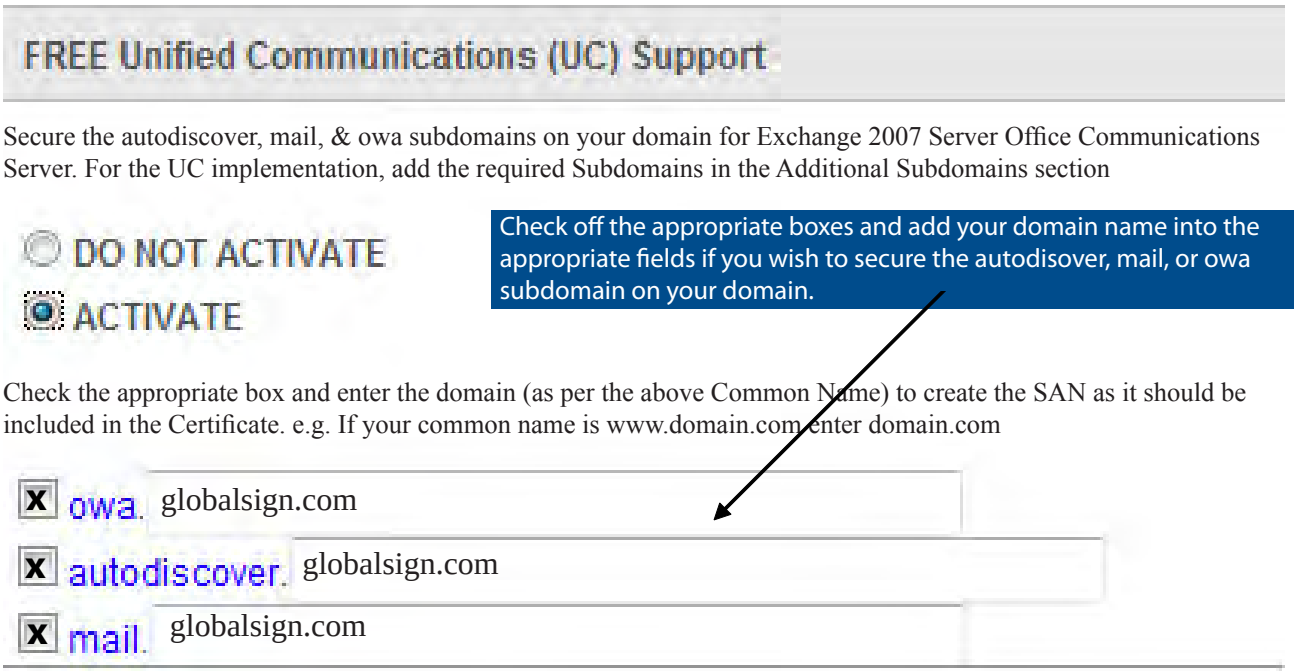
The next screen brings you to the option page to configure your SANs/Unified Communications Certificate.

Configure Option #1- Define your SANs

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

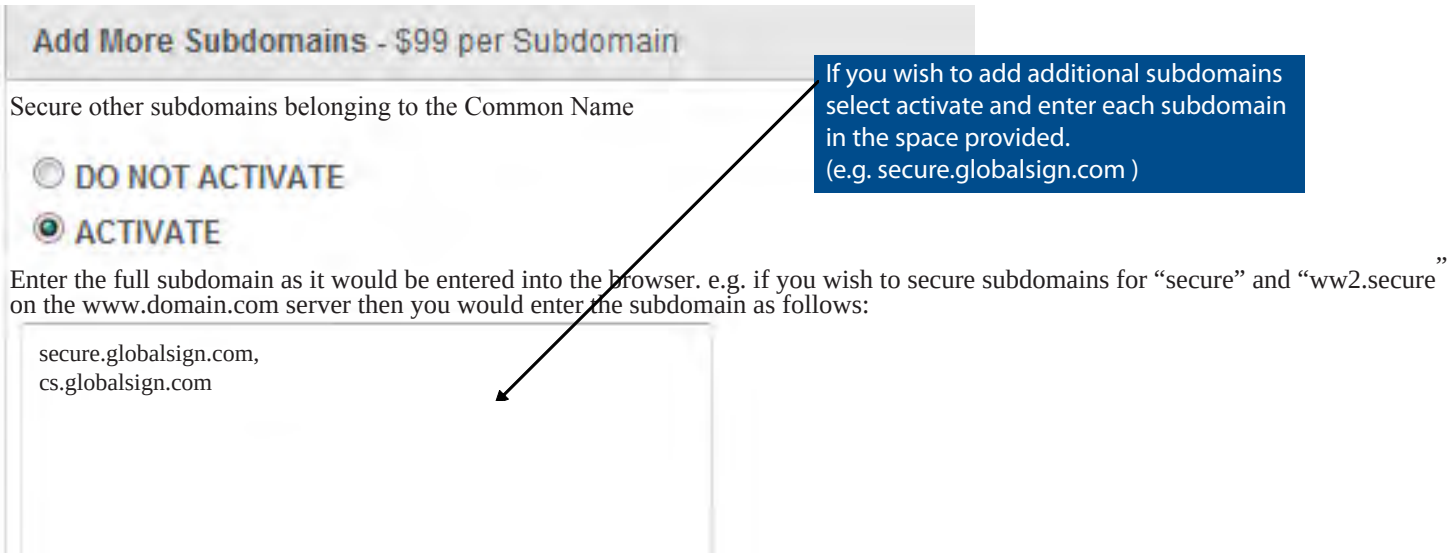
Configure Option #2- Activate UC Support

Next you have the option of adding UC support to secure autodiscover, mail, and owa subdomains.



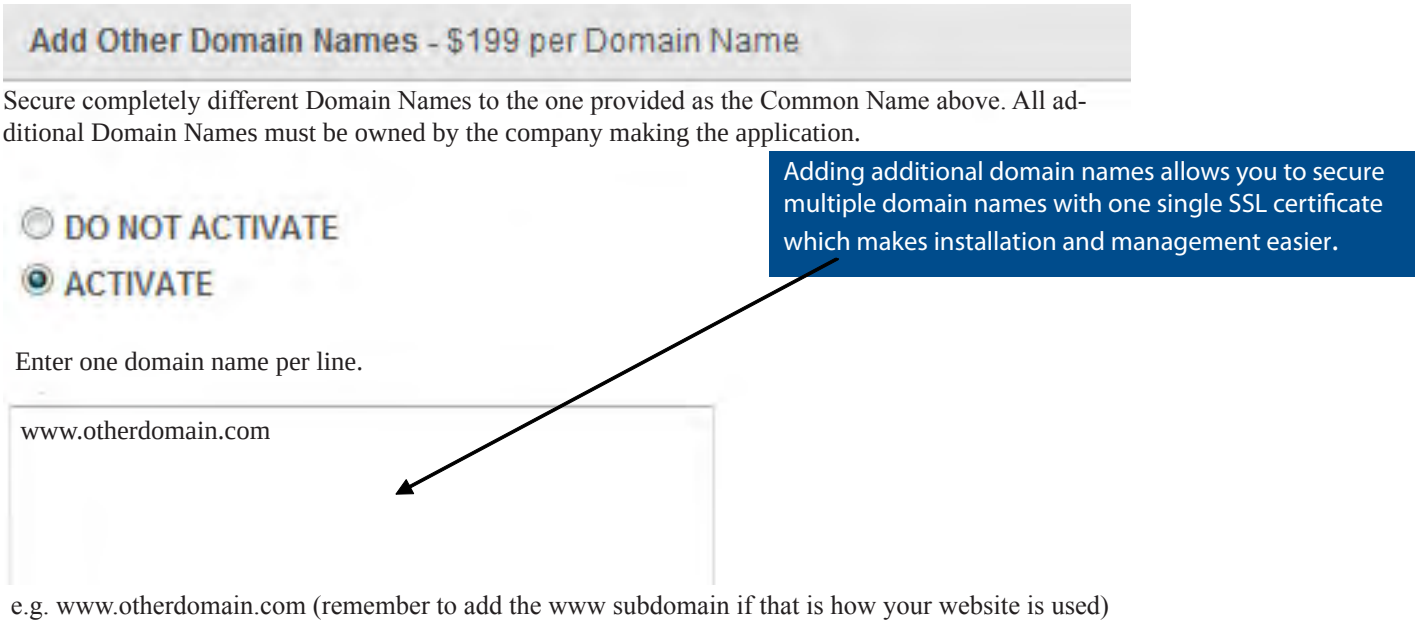
Configure Option #3- Add additional Subdomains

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



Configure Option # 4- Add additional domain names

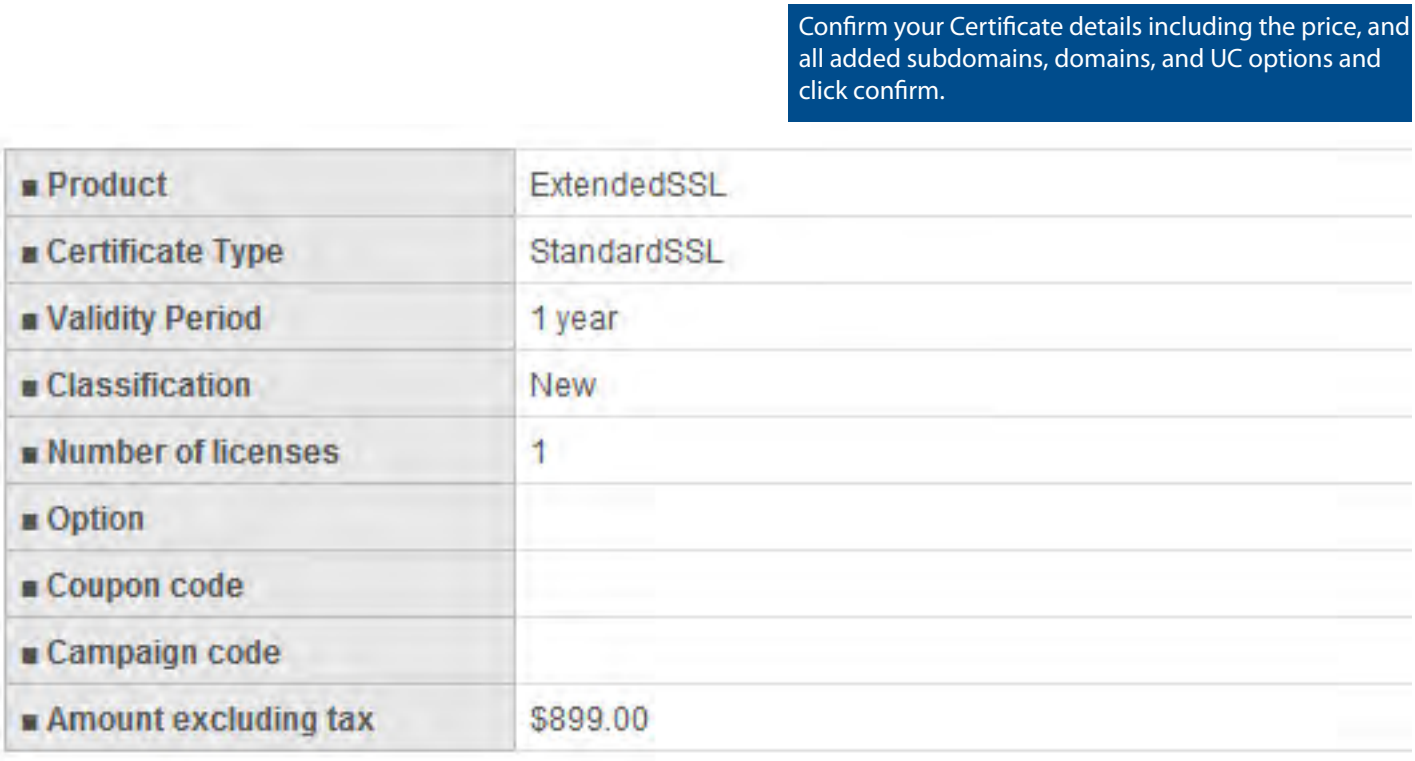
Next you will have the option to secure additional domain names to the common name (globalsign.com).



e.g. www.otherdomain.com (remember to add the www subdomain if that is how your website is used)

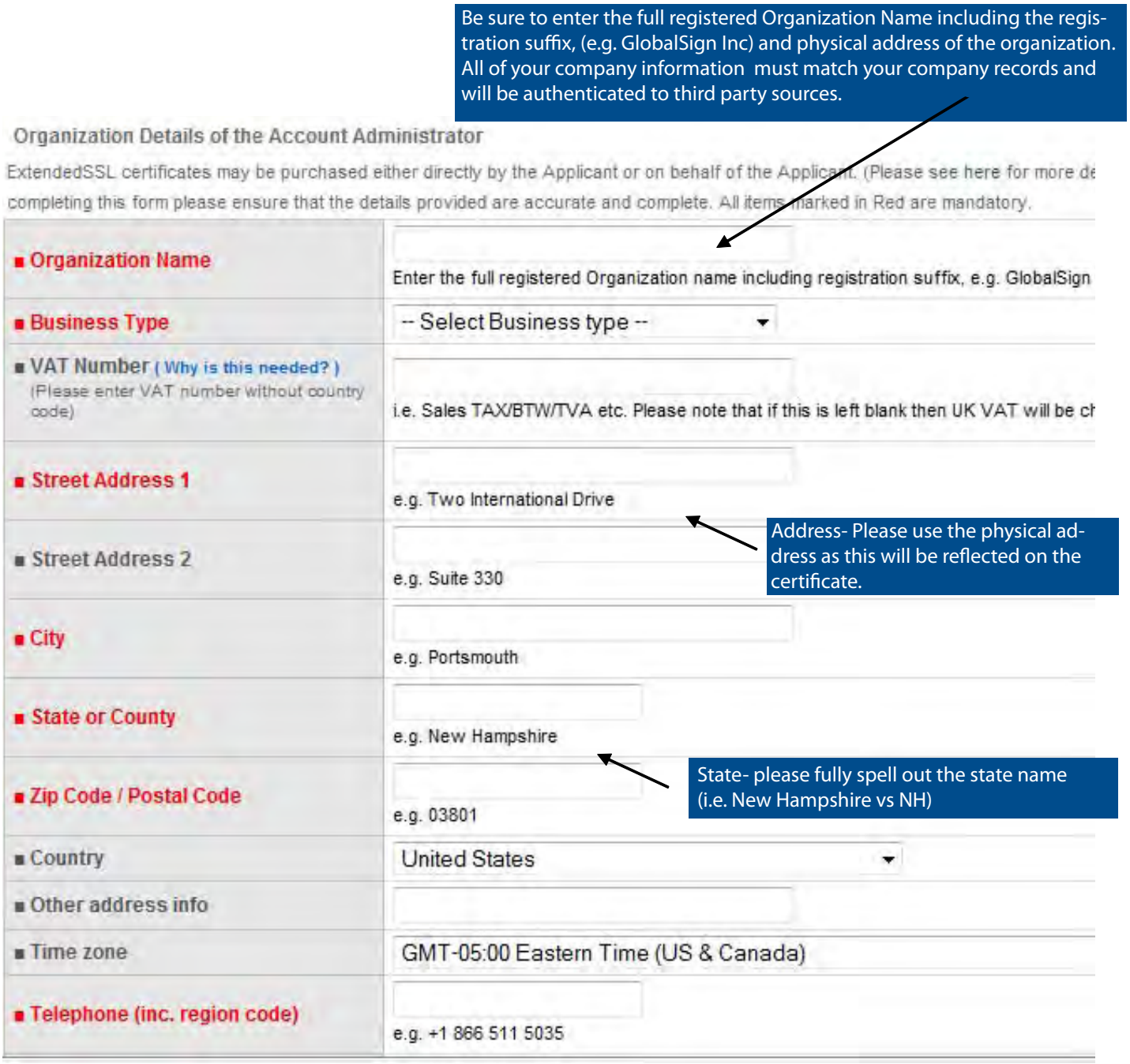
Configure Option # 5- Confirm your options

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

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 entering your Organization and Account Administrator details. **It is very important that you ensure the details are accurate and complete when completing the form.**



Once your order has been submitted, you will be required to sign and fax the order form to (617-830-0779)

A confirmation phone call will be conducted by our Vetting Department to verify your order, employment, and signing capabilities binding the organization to the Subscriber Agreement. After this confirmation the Subscriber Agreement will be emailed to you to sign and fax back to GlobalSign.

Step 4. The Vetting Process

Once your order has been submitted it will be sent to GlobalSign's Vetting department where a Vetting Officer will validate your order and your company information. This process can take up to 3-5 days on average.

The vetting process will confirm your company is a legal entity by conducting a complete organization vetting to meet the CA/B Forum Guidelines . The Extended Validation vetting process establishes the legitimacy of an organization within a specific jurdisdication of incorporation.

The vetting process is completed through third party resources, if any information can not be confirmed by our vetting department a vetting officer will request additional validating information. Our vetting department will use third party resources to check the following information:

1. Verify the legal, physical, and operational existence of your entity

GlobalSign will need to confirm that your company has a legal, physical, and operational existence that matches the records on the SSL Certificate.

2. Verify that your entity matches official records

GlobalSign will need to confirm that your company is a legally formed organization.

3. Verify that your entity has exclusive rights to use the domain name specified for the SSL Certificate.

GlobalSign will check the rights of the domain name you are attempting to secure by verifying that your company owns the domain name. This process is completed by verifying your whois record and confirming it contains your legal company name and current address.

4. Verify that your entity has authorized the ordering and issuance of the SSL Certificate.

GlobalSign will confirm the authorization of ordering an EV SSL Certificate by placing a phone call into your organization to receive approval that this order is authorized.

Step 5- Receiving and Installing your SSL Certificate

Once your order has been approved through our vetting department you will receive an email confirmation with instructions on how to retrieve and install your SSL 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/

Once the Certificate has been issued it needs to be installed on the server. Instructions for installing a SSL Certificate will depend on the type of server software you are using. Full instructions for all servers are available at http://www.globalsign.com/support/installcert.php

Most Commonly Asked Questions-FAQ Section

Why should I buy a GlobalSign Extended Validation SSL certificate?

Due to the CAB Forum guidelines that are designed to ensure the GlobalSign vetting process of the Extended Validation SSL applicant is of the highest level, the Extended Validation SSL gives the end user peace of mind and the knowledge that the web site they are visiting is who it claims to be. Therefore the owner of the web site has the opportunity to increase revenues through online sales and the end user has a more relaxed online experience.

Does the GlobalSign Extended Validation SSL certificate show the green address bar?

The GlobalSign Extended Validation SSL certificate will turn the browser address bar green in all browsers that support the Extended Validation SSL Certificates:- Internet Explorer 7+, Firefox 3+ and Opera 8+, Chrome and Safari.

Does the Extended Validation SSL certificate use a different Intermediate certificate?

The GlobalSign Intermediate Certificate uses it's own intermediate certificate called the Extended Validation SSL Validation CA and a Cross certificate, which can be found at http://www.globalsign.com/support/intermediate/extendedssl_intermediate.php

Can I get free Reissues of my Extended Validation SSL certificate?

If your SSL certificate cannot be installed and was issued under 7 days ago we will issue you a new certificate at no extra cost but you must begin the certificate request from the beginning because the CAB Forum guidelines state that we must vet each certificate request, even if the request is a reissue of a previously issued certificate.

Can I use a 1024 bit Public key inside my CSR?

No, you should use a more secure key size of 2048 bit. Please note we cannot accept a key size of 512 or 1024 bits.

Can I use AutoCSR with Extended Validation SSL?

Extended Validation SSL certificates do not support AutoCSR, your CSR must be generated on the web server you intend to install the certificate on.

Do Extended Validation SSL certificates support the Wildcard option?

Extended Validation SSL certificates do not support Wildcard certificates, but Extended Validation SSL Certificates support Subject Alternative Names (SANs), which support extra fully-qualified domain names and sub-domain names.

What period of time can I request an Extended Validation SSL certificate for?

Extended Validation SSL certificates can be issued for either 1 year or 2 years, with a 2 year certificate being not only better value for money, but also omitting the need to request a new certificate when you renew in a years time.

How do I move my certificate between servers?

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 first 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.

FAQ Section-continued..

Can I use the Wildcard option with Extended Validation SSL?
The Wildcard option is not available with the Extended Validation SSL certificate.

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. GlobalSign issue professional level SSL Certificate that automatically secure both www.domain.com and just domain.com in a single SSL Certificate without any additional charges, IP address purchase or server configuration.

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 ad dress 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 the user need the GlobalSign's server root certificate to access information securely on secure server?
If users don't have the GlobalSign root certificate installed and they go to a server secured through a GlobalSign SSL Certificate, the browser will ask them if they will trust certificates issued by GlobalSign. If they answer yes, the GlobalSign root certificates will be installed automatically. If they answer no, they can still choose to accept the secure session they are about to start but the next time they will receive the exact same question from their browser.

Would the 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.

Which fields are allowed in a request for a SSL server certificate?
common name = mandatory
country name = mandatory
organization = mandatory
organizational unit name = optional
state or province name = optional
locality name = optional
email address = optional (cannot be used with windows iis)

FAQ Section-continued..

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+
* Netscape Commerce Server v1 or higher
* Stronghold Server
* Netscape Iplanet Web Server 4.1
*Netscape Enterprise Server v3 +
* Netscape FastTrack Server
* Internet Application Server 1.0

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

Why does my 512-bit private key not work??

The private key sizes for Extended Validation SSL must be at least 2048 bits, for compatibility with certain web browsers. A keysize of 2048 bits is recommended because the larger key size makes the certificate more secure.

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

If have any questions about the ordering process for an Extended Validation 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
Email: support@globalsign.com
Tel: 1-866-503-5375