

# Ordering Guide for Organization SSL

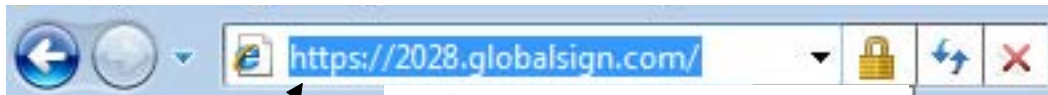
1. Creating CSR
2. The Ordering Process
3. The Vetting Process
4. Installing your SSL Certificate



## Overview of Organization SSL

Organization Validated SSL is ideal for businesses who need identity assurance and higher levels of trust than a domain validated SSL Certificate. Organization SSL Certificates activate the “little yellow padlock” and secure your ecommerce transactions, web account logins, webmail, network traffic, and online services with unsurpassed levels of authentication, integrity, confidentiality, and non-repudation. Organization SSL Certificates are organization vetted—meaning that website visitors see your vetted company details, enhancing the trust they place in your website and providing more confidence to do business with you.

A webpage with a Organization SSL Certificate can be view below:



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



GlobalSign has identified this site as:  
 2028.globalsign.com  
 This connection to the server is encrypted.  
 Should I trust this site?

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.

[View certificates](#)

General		Details	
<b>This certificate has been verified for the following uses:</b>			
SSL Server Certificate			
<b>Issued To</b>			
Common Name (CN)	2028.globalsign.com		
Organization (O)	GlobalSign Ltd		
Organizational Unit (OU)	Technical		
Serial Number	01:00:00:00:00:01:22:7F:24:4D:70		
<b>Issued By</b>			
Common Name (CN)	GlobalSign Organization Validation CA		
Organization (O)	GlobalSign		
Organizational Unit (OU)	Organization Validation CA		
<b>Validity</b>			
Issued On	7/15/2009		
Expires On	7/15/2012		

Depending on the browser an Organization SSL Certificate will display the following information:

- Common Name (CN) of the certificate holder
- Common Name (CN) of the certificate issuer
- Organization Name (ON) of the certificate holder
- Organization name (ON) of the certificate Issuer
- Organization Unit (OU) of the certificate holder
- Organization Unit (OU) of the certificate issuer
- Validity dates of the Certificate
- Serial Number
- SHA1 & MDA fingerprints- (digital fingerprints that corresponds to a specific file)

# The Ordering Process

## Step 1. Creating a CSR

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 Organization SSL, you have the option of creating your own CSR or using the free AutoCSR option when ordering and we'll create your CSR 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>

### 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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYTCAsocCAQAwYUxHjAcBqNVBAMTFXdx3dy5jZXJ0YXV0aG9yaXR5LmVhTEB
MkGA1UECkMSVGVzY2huaNNhbCBTdXBw3J0MRWwFAFDVQKKEw1HbG91YXwTaWdu
IFVIMRlWEAYDVQHEw1NYW1k3RvbmUxDTALBgqNVBAgIBEt1bnQxQzAaBqNVBAIT
AkdCMIGtMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBBQXNmVFB1SEUGuj3QzVpefH
Rz4cV5jOERxZCDF39d/cYqYUTC8eU3KOGVRECF94IwJ5HKov4WOp1rTo7+CXLgz
ngatGgNzZR1GNt1LAHIAbwTwna7FwQ3r1RZdptLQhY4AzzeWfNbnq1H1eEh3WvFRb
CFbzGKmDIqqQ544cmrwmOwIDAQABoIIBmTAABozBgEEAYI3DQIDMqWcJUmMS4y
NjAwLjIwewYKRwYBBAGCNwIBDjFUMG9yOAHIAbw4AQH/BAQDAgTWMEQGC5qS5Ib3
DQEJdWQ3MDUwDgYIKoZIhvcNAwICAQCAAgGCCqGSIb3DQMEAgIAgDAHBgUzDgMC
BzAKBgqghk1G9w0DBzATBqNVHSUBDkKqqrBgEFBQcDATCB/QYKwYBBAGCNwOC
AjGB7jCB6wIBAR5aAE0AaQ8jAHIAbwBzAGSAZgB0ACAAUgBTAEAAIABTAEMAAABn
AG4AbgB1AGwAIABDAAHIAeQ8jAHIAbwBnAHIAIYQ8B0ACAAUgBTACAAUABYAG8AdgBp
AGQAZQByA4GJA0NjHx0pK17BFcmt5oFKMmmDDuOehAjWa+Am/Lot4HsX4zjua5D
htaAzk21snAHIAbwRv1DwUUG6vuHKL0/IV1UMKXFPqhm/MVBE6cQqJia4Ted0/bxV6
+XbB5JrTk8JEqkps/cg71AMNHg0PIYnyhtx04McBbaPKGZ5vhPmOKLIVAAAAA
AAAAAQYJKoZIhvcNAQEFBQADgYEAJggvWuAT42pOauAHIAbw00vgasOoT0bY89pt
FQ3wtEo6ko276FDd6Nhofj74URXJDNCK9XE4c4b0h1Sodhm87RqfFRJEeBT6MkP
vVK70L3n0QmgKoLW+TndK6ofnQauf8wSD3pvdgSrd7qWwFzKW3mYIaHz6eq107B
rNkNpUE=
-----END NEW CERTIFICATE REQUEST-----
```

## Step 2. Placing your order online

Ordering an Organization SSL Certificate contains multiple steps and various options. This guide will go over each option available and the steps so you can be prepared when you are ready to place your order.

### Begin the Online Ordering Process

Click the “buy now” link on any Organization SSL related page or go to: <http://globalsign.com/ssl/buy-ssl-certificates/organization-ssl/buy-organization-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**

## Choose your options

With an Organization SSL there are various options to choose from to enhance your Certificate. Please see the below details of each option available.

### Option # 1- Choose your Certificate Type

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

**Wildcard SSL** → 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

**Public IP address SSL**  
Issued to a publically accessible 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.

### 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 Domains: \$199  
Additional Subdomains: \$99

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.

**• Add Subject Alternative Names (SANs):**

Check to add SANs.

Standard SSL Certificates secure a single Fully Qualified Domain Name. By adding SANs your Certificate can secure other server "names" such as other domain names, subdomains, IP addresses and localhost names. If selected you will enter your SANs on the next page and the total cost of the Certificate is then calculated.

### 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.

**• 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 ▼

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

### 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.

**Select Validity Period** Please select the validity period of the SSL Certificate.  
 Multi-year offers significant per annum savings.

Year	Price
<input type="radio"/> Six months	\$
<input checked="" type="radio"/> 1 year	\$392
<input type="radio"/> 2 years	\$717
<input type="radio"/> 3 years	\$978
<input type="radio"/> 4 years	\$1206
<input type="radio"/> 5 years	\$1411

Set Custom Start & Expiration Date

Check if you require the Certificate to be valid from a certain date or to expire on a certain date. Leave unchecked and the Certificate will become valid upon completion of the

### 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 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)

## 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 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 Server. For the UC implementation, add the required Subdomains in the Additional Subdomains section

**FREE Unified Communications (UC) Support**

DO NOT ACTIVATE  
 **ACTIVATE**

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

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.

## 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

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.

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

Adding additional domain names allows you to secure multiple domain names with one single SSL certificate which makes installation and management easier.

#### Add Other Domain Names - \$199 per Domain Name

Secure completely different Domain Names to the one provided as the Common Name above. All additional Domain Names must be owned by the company making the application.

DO NOT ACTIVATE

ACTIVATE

Enter one domain name per line.

www.otherdomain.com

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

### Configure Option # 5- Add Public IP Addresses

Next you will have the option to secure public IP Addresses (\$490/each) & internal IP addresses (\$0/each)

#### Add Public IP Addresses - \$490 per Public IP Address

Add Public IP Addresses (must be publicly accessible and owned by the applicant organization)  
Available for OrganizationSSL and ExtendedSSL only.

DO NOT ACTIVATE

ACTIVATE

Enter one Public IP Address per line

### Configure Option # 5- Add Public IP Addresses-Continued

Add Internal IP Addresses or Local Hostnames - \$0 per Internal Address

Add Internal Addresses such as [10.10.10.01](#) or [localhost](#).

DO NOT ACTIVATE

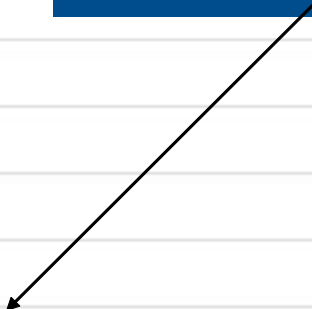
ACTIVATE

### 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.

■ Product	OrganizationSSL
■ Certificate Type	StandardSSL
■ Validity Period	1 year
■ Classification	New
■ Number of licenses	1
■ Option	
■ Coupon code	
■ Campaign code	
■ Amount excluding tax	\$349.00

Confirm your Certificate details including the price, and all added subdomains, domains, and UC options and click confirm.



## 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- It is very important that you ensure the details are accurate and complete when completing the form.

Be sure to enter the full registered Organization Name including the registration suffix, (e.g. GlobalSign Inc) and physical address of the organization. All of your company information must match your company records and will be authenticated to third party sources.

#### Organization Details of the Account Administrator

ExtendedSSL certificates may be purchased either directly by the Applicant or on behalf of the Applicant. (Please see [here](#) for more details. completing this form please ensure that the details provided are accurate and complete. All items marked in Red are mandatory.

<b>■ Organization Name</b>	<input type="text"/>	Enter the full registered Organization name including registration suffix, e.g. GlobalSign Inc
<b>■ Business Type</b>	<input type="text" value="-- Select Business type --"/>	
<b>■ VAT Number ( Why is this needed? )</b> <small>(Please enter VAT number without country code)</small>	<input type="text"/>	i.e. Sales TAX/BTW/TVA etc. Please note that if this is left blank then UK VAT will be charge
<b>■ Street Address 1</b>	<input type="text"/>	e.g. Two International Drive
<b>■ Street Address 2</b>	<input type="text"/>	e.g. Suite 330
<b>■ City</b>	<input type="text"/>	e.g. Portsmouth
<b>■ State or County</b>	<input type="text"/>	e.g. New Hampshire
<b>■ Zip Code / Postal Code</b>	<input type="text"/>	e.g. 03801
<b>■ Country</b>	<input type="text" value="United States"/>	
<b>■ Other address info</b>	<input type="text"/>	
<b>■ Time zone</b>	<input type="text" value="GMT-05:00 Eastern Time (US &amp; Canada)"/>	
<b>■ Telephone (inc. region code)</b>	<input type="text"/>	e.g. +1 866 511 5035
<b>■ Fax (inc. region code)</b>	<input type="text"/>	e.g. +1 617 830 0740
<b>■ DUNS (if available)</b>	<input type="text"/>	DUNS Number (D & B Registration Number) is only required if using a Business Assumed Name.
<b>■ How did you hear about GlobalSign ?</b>	<input type="text" value="-- Select --"/>	

## 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.

	<input type="checkbox"/> <b>Same as Organization Details</b> Click if your Technical Contact details as the same as your Organization Details.	
■ <b>User ID</b>	<input type="text"/>	Auto populate the same details you used for organization details by clicking on “Same as Organization Details”
■ <b>Password</b>	<input type="text"/>	
■ <b>Confirm Password</b>	<input type="text"/>	Create a User Id and Password that is unique and memorable for you
■ <b>Department</b>	<input type="text"/> e.g. Marketing	
■ <b>First Name</b>	<input type="text"/>	
■ <b>Last Name</b>	<input type="text"/>	
■ <b>Job Title</b>	<input type="text"/> e.g. Web Administrator	
■ <b>Email Address</b>	<input type="text"/> ✘Please check your email address has been entered correctly	
■ <b>Street Address 1</b>	<input type="text"/> e.g. Suite 330	
■ <b>Street Address 2</b>	<input type="text"/> e.g. Two International Drive	
■ <b>City</b>	<input type="text"/> e.g. Porstmouth	
■ <b>State or County</b>	<input type="text"/> e.g. New Hampshire	

## Account Setup (Stage 3/3)

3. **Billing Contact Information-** 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-** You will then be prompted to review all of the information you have entered so far and be asked to review the Terms and Conditions, after you have read the Terms and Conditions and click “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 using two characters (example: US, JP, UK, etc), and enter 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.



GlobalSign™

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. Please choose from the pre-populated 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 6: After your order is placed

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

## Step 7: Install your Certificate

Once the Certificate has been issued it needs to be installed on the server. Installing a SSL Certificate will differ for each type of server software. Full instructions for all servers are available at <http://www.globalsign.com/support/installcert.php>

## Step 3. The Vetting Process

Organization Validated SSL Certificates must go through a vetting process to validated the organization requesting the certificate before they can be issued.

### The Vetting Process

The vetting process is conducted by our vetting department by using third party resources to validate your company information and 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 EV Cert.**

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 an EV 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 4. Receiving your SSL Certificate

1. Once your order has been submitted, it will be sent to our vetting department who will validated your order and your company information. (This process on average takes 1-2 days)

2. A confirmation phone call will be conducted by our Vetting Department to verify the order. If we shall need any further information along the way for supporting documentation (such as proof of registration, an address verification letter, or a phone bill, etc.) we will contact you right away. All of the information we obtain is conducted through third party sources unless we can't find it then we will contact you.

## Step 5. Installing your SSL Certificate

Once the Certificate has been issued it needs to be installed on the server. Installing a SSL Certificate will differ for each type of server software. Full instructions for all servers are available at <http://www.globalsign.com/support/installcert.php>

## Most Commonly Asked Questions-FAQ Section

### 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](https://www.domain.com) it will also secure [domain.com](https://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](https://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](https://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.

### Which fields are allowed in a request for SSL server certificate?

Common Name	= mandatory
Country Name	= mandatory
Organization	= mandatory
Organizational Unit Name	= optional
State or Province Name	= optional
Locality Name	= optional
E-mail 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 web servers 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/>).

### 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.

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

If have any questions about the ordering process for an Organization 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](mailto:support@globalsign.com)

**Tel:** 1-866-503-5375