

GlobalSign SSL Certificate Procedures

Step 1: Open to the following URL in a separate window or tab:

<https://system.globalsign.com/bm/public/certificate/poporder.do?domain=PAR346322zp4aky6h65c306u2nb9>

Step 2: Select Validity Period of Certificate:

Certificate Application

Products

OrganizationSSL

SSL Certificate Type

Single Domain Certificate
Secures a single Fully Qualified Domain Name such as www.globalsign.com or secure.globalsign.com

i For Certificates issued to sites beginning with www (or * for Wildcards) we will add the non-www or non-* version of your domain as a SAN free of charge. Your Certificate will work for www.domain.com and domain.com.

Validity Period

<input checked="" type="radio"/>	1 year
<input type="radio"/>	2 year
<input type="radio"/>	3 year
<input type="radio"/>	4 year
<input type="radio"/>	5 year

i Multi-year offers significant per annum savings. Multi-year also means less frequent renewals.

Select number of years you want the certificate to be valid for.

Cost is \$75 per year per domain name.

←

Are you renewing this Certificate ?

No Yes

i If you are renewing within the renewal period (90 days to expiration) we place the remaining time on your current Certificate on your replacement GlobalSign Certificate. You may also add 30 more bonus days free of charge.

This document covers only NEW certificate requests that do not require SANs.

Step 3: Select SANS Option and Insert the CSR:

Add specific Subject Alternative Names (SANs)

Add additional "names" to be secured by this Certificate - sub domains, additional Fully Qualified Domain Names, public or private IP addresses and localhost names.

No Yes

i When a browser comes across a Certificate with SANs, it knows that the Certificate can be used to secure not just the primary domain to which it's been issued, but also whatever it finds in the SANs section. By adding SANs your Certificate can secure other server "names" such as other domain names, subdomains, IP addresses and internal server names.

Enter Certificate Signing Request(CSR)

After creating your server's Certificate Signing Request (CSR) as created in [Generate a CSR](#) support files, paste the CSR in the form below. Make sure that it contains the complete header and footer "BEGIN" and "END" lines as shown in the example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYTCAsCAQAwgYUxHjAcBgNVBAMTFXd3dy5jZXJ0YXV0aG9yaXR5LmNvbTEb
MBkGA1UECmMSVGZyY2huaWNhbCBTdXBw3JOMRYwFAYDVQQKEw1HbG91YXV0aW50
IFVLMRiEAYDVQQHEw1NYW1kc3RvbmUxDTALBgNVBAgTEclbnQxZzA5BjgNVBAYT
AkdCMIGIMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBgQDXXWmVFB13EUGuj3QzVperH
Rz4cV5jOERxZCDF39d/tYgYJTC8su3xOGVREC9T9tWj5HKcv4WOpIrTc7+CXLgz
hgatGgNzZR1GNt1LAHIAbwTwna7FwQ3r1RZdptD0Hy4AzzeWfNbnq1H1eEh3WvFRb
CFbzGKMDIQQS44tmrwmOWIDAQABoIIBmIAA8BgrBqEEAYI3DQIDMqWcJUmMS4y
NjAwLjIwewYKwYBBAGCNwIBDjFtMGswDAHIAbw4AQH/BAQDAgTWMEQCSqGSIb3
DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMAA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMC
BzAKBggqhkiG9w0DBzATBqNVHSUBDAKBBqgrBqEFBQcDATCB/QYKwYBBAGCNw0C
AjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAGSAZqB0ACAAUgBTAEAAIABTAEMAaABn
AG4AbgBlAGwAIAEDAIAEQBwAHQAABwBnAHIAyQBAAGAAQBJACAAUABYAAGSAdgBp
AGQAZQBjA4GJAJNjHxOpK4I7BFcmt5oFKMmDDuOehAjWa+Am/1oT4Hx4zjuasD
htaAzk21snAHIAbwRv1dWU6vuhKLU/IV1UMKXfQhm/MVBE6cQqJia4TedO/bxV6
+XbB5JrTk8JEqkP8/cq7LamWHgOPiYnYhtx04McBbaPKGZ5vhPmOKLIVAAAAAAA
AAAwDQYJKoZIhvcNAQEFBQADgYEAIGgvWuAT42pOauAHIAbw00vgasOoT0bY89pt
FQ3wtEo6koZ76FDd6NhoFj74URXJDNCK9XE4c4b0h1Sodhm87RqfFRJEeBt6MkP
vV70L3n0QmgKoLW+TNfdK6OfnQauf8wSD3pvdgSrd7gWsfzKN3mYIaH6eqi07B
rNkWPuE=
-----END NEW CERTIFICATE REQUEST-----
```

Insert the CSR that you generated on your server in this box.

i Your CSR should contain EXACTLY the details that you wish for your Certificate to be issued to. Make sure the Common Name (CN) contains the fully qualified domain name you wish to secure, the Organization is your legally incorporated name including any company title such as Inc, Ltd, NV/SA etc and that your Country, State (County or Province) and Locality (City or Town) match the details for your registered company office. Providing incorrect information will cause delays in the processing of your order.

SANs are Subject Alternate Names and it is unlikely that you need them. For more info on SANs:

<http://www.globalsign.com/resources/datasheet-unified-communications-ssl.pdf>

If you need assistance with creating a CSR then visit here:

<http://www.globalsign.com/support/ssl.php>

Step 4: Fill in necessary information to finish processing your request:

Contact Information

The Point of Contact will receive the issued Certificate and Renewal Notices when the Certificate approaches expiration. This person will also be our point of contact for vetting and technical issues regarding the application.

* Required field

First Name:	*	<input type="text"/>
Last Name:	*	<input type="text"/>
Telephone:	*	<input type="text"/>
Email Address:	*	<input type="text"/>
Server IP Address	*	<input type="text"/>
Server FQDN	*	<input type="text"/>
Server Operating System	*	<input type="text"/>
Cost Center - Full FOAPAL	*	<input type="text"/>

***** STOP *****

Please Read the Notes below BEFORE Continuing!

Comments

If you have additional comments appropriate to this order please state in the box below:

- **Email Address ** All renewal notices will be sent to the email address entered here ****

It is **STRONGLY** suggested that a **GROUP** email address be used because renewal notices will be sent here and sometimes individuals are no longer in the same group at renewal time.

- **Cost Center – Full FOAPAL** - needs to be the full FOAPAL of the department requesting the certificate.

Your request will be REJECTED if the full FOAPAL is not included!

Step 5: Intermediate Certificate

After installing your certificate be sure you have the latest Intermediate Certificate installed too.

<http://www.globalsign.com/support/index.php> (see Intermediate Certs Section)