

GlobalSign Enterprise Solutions

Managed SSL Quick Start Guide

Version 5.3



Managing EV, OV and IntranetSSL Certificates Across Your Organization Effectively

TABLE OF CONTENTS

- TABLE OF CONTENTS 2
- 1 INTRODUCTION 5
 - ACCOUNT LOGIN..... 5
 - MANAGED SSL PAGE REFERENCE 5
 - GETTING HELP..... 6
- 2 ORDERING CERTIFICATES 7
 - 1.1 ORDERING CERTIFICATES 7
 - 1.2 SUMMARY OF MSSSL PRODUCTS 7
 - 1.3
 - 2.1.1 EXTENDEDSSL 7
 - 2.1 ORGANIZATIONSSL..... 7
 - 2.1.2 ORGANIZATIONSSL..... 7
 - 2.1.3 INTRANETSSL..... 7
 - 2.1.4 CLOUD SSL..... 7
 - 2.1.5 MSSSL PRODUCT FEATURE COMPARISON..... 8
 - 2.2 ORDERING MSSSL CERTIFICATES 8
 - 2.2.1 ADDING SANS DURING THE ORDERING PROCESS 12
 - 2.3 USING THE PUBLIC ORDERING PAGE..... 13
 - 2.3.1 ACTIVATING THE PUBLIC ORDERING PAGE..... 13
 - 2.3.2 CONFIGURING THE PUBLIC ORDERING PAGE 14
 - 2.4 APPROVING ORDERS 16
- 3 CLIENT CERTIFICATE AUTHENTICATION 17
- 4 MANAGING & REPORTING ON CERTIFICATES AND ORDERS 19
 - 4.1 MANAGING & REPORTING ON CERTIFICATES AND ORDERS 19
 - 4.2 SEARCHING FOR CERTIFICATES..... 19
 - 4.1.1 SEARCH RESULTS..... 20
 - 4.3 SAN REPORTING & SEARCH 21
 - 4.2.1 SUMMARY SAN REPORT 21
 - 4.2.2 SAN SEARCH 23
 - CERTIFICATE ACTIONS 24
 - 4.3.1 REISSUE AN SSL CERTIFICATE 24
 - 4.3.2 RENEW AN SSL CERTIFICATE 24
 - 4.3.3 REVOKE A CERTIFICATE 25
 - 4.3.4 CANCEL A CERTIFICATE 25
 - 4.3.5 CHANGE USER ASSOCIATED WITH CERTIFICATE..... 26

- 4.3.6 ADD/REMOVE SANS 26
- CERTIFICATE DETAILS..... 26
- 4.4.1 ORDER SUMMARY..... 27
- 4.4.2 FULL ORDER DETAILS 27
- 4.4.3 USER & CONTACT DETAILS..... 27
- 4.4.4 GCC EMAIL LOG..... 27
- 4.4.5 GCC AUDIT LOG..... 27
- 5 MANAGE DOMAINS & PROFILES..... 28
- MANAGING PROFILES..... 28
- 5.1.1 EDIT PROFILE..... 29
- 5.1 MANAGING DOMAINS..... 29
- 5.2.1 ADD NEW DOMAIN 29
- 5.2.2 RENEWING DOMAINS 31
- 5.2.3 MANAGE DOMAINS 32
- 5.2.4 SEARCHING FOR DOMAINS..... 35
- 5.2.5 ACTIVATE POP or EDIT POP..... 36
- 5.2.6 EV APPLICATION..... 36
- 5.3 UPGRADE TO EV LEVEL VETTING 36
- 6 ACCOUNT AND FINANCE PAGE 36
- 6.1 LICENSING OPTIONS 37
- 6.1.1 BULK PURCHASE..... 37
- 6.1.2 PAY AS YOU GO 37
- 6.2 6.1.3 CERTIFICATE LICENSING 37
- 6.1.4 SAN LICENSING..... 37
- PAYMENT OPTION –DEPOSITING FUNDS INTO ACCOUNT 38
- 6.3 6.2.1 ADD DEPOSIT..... 38
- 6.4 6.2.2 HOW TO PAY FOR YOUR DEPOSIT..... 38
- 6.5 6.2.3 DEPLETED DEPOSITS 38
- 6.6 VIEW/REQUEST INVOICES 39
- VIEW REQUESTS FOR PAYMENT (RFPs)..... 39
- VIEW STATEMENTS – OUTSTANDING FUNDS 40
- ACCOUNT MANAGEMENT 40
- 6.6.1 AMEND COMPANY DETAILS..... 40

6.6.2	VIEW ALL RECEIVED EMAILS	40
	USER MANAGEMENT	40
6.7.1	USER ROLES	41
6.7.2	MANAGE USERS	41
6.7	TAB MANAGEMENT	42
	6.8.1 SETTING THE DEFAULT TAB.....	42
	6.8.2 HIDING THE SSL TAB.....	43
6.8	USEFUL FUNCTIONS	44
	CSR CHECKER	44
8	GLOBALSIGN CONTACT INFORMATION	44
7.1		

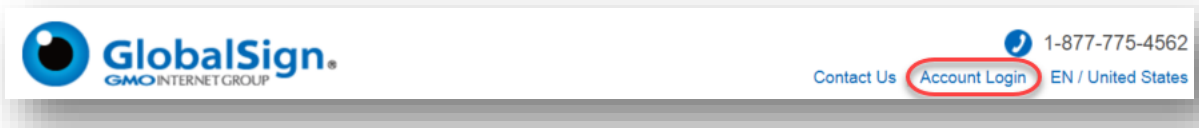
1 INTRODUCTION

The GlobalSign Certificate Center (GCC) is a highly flexible, cloud-based certificate lifecycle management platform. GCC centralizes certificate management for all types of GlobalSign Digital Certificates and allows for multiple users. **Managed SSL (MSSL)** is a solution available within GCC.

ACCOUNT LOGIN

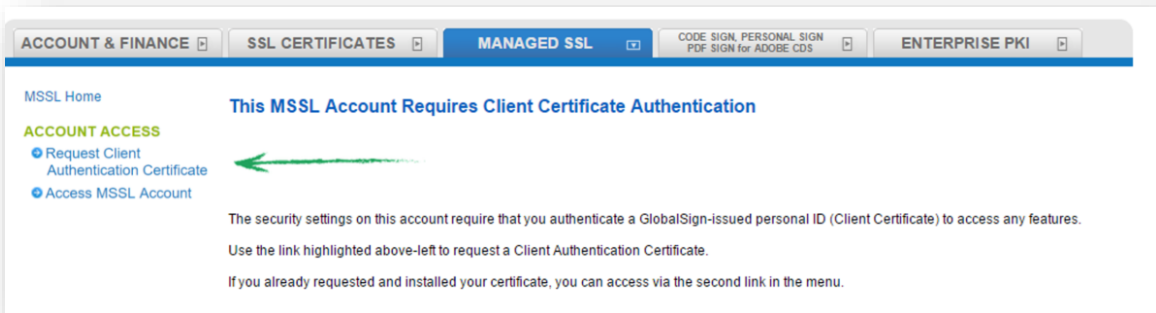
Once your Managed SSL Account has been approved, you can log into the GlobalSign Certificate Center (GCC) straight away to start managing the lifecycle of your SSL Certificates.

1.1 Go to www.globalsign.com and click **Log In** at the top of the screen.



Enter your **User ID** and **Password**. Your **User ID** is the PARXXXX_xxxxx number given to you at the end of the MSSL signup process. You can also find it in your Welcome Email. Your **Password** is the password you entered during the signup process.

If your account is configured for Client Authentication, then you will see a page similar to this when you log in. See **Section 3** for details.



If you forget your password, click **Forgot Your Password? Click here** on the login page to reset it. View this [Support Article for assistance](#) or if necessary contact our Support Team at support.globalsign.com.

1.2 You will only be able to order certificates once the vetting of your organization and domain name(s) has been completed. You can check your vetting status anytime by logging into your account.

MANAGED SSL PAGE REFERENCE

Below is the screenshot of what you will see under the MANAGED SSL Tab in GCC. The numbered indicators correspond to a reference that will help you navigate and use Managed SSL. When ordering SSL Certificates please be sure you are within the **MANAGED SSL** tab.



REFERENCES

1. **Account & Finance Tab** - This will redirect you to the Account & Finance Page where you can manage all of your account information. View Section 5 for more information.
2. **Upcoming Renewals** - View all certificates that are about to expire and are available for renewal (Section 4.3.2).
3. **Expiring Domains** - View all domains that are expiring and are available for renewal (Section 5.2.2).
4. **Pending Approvals** - View orders which are pending for approval (Section 2.4).
5. **Find & Report on Certificates** – Search for SSL Certificate orders placed under your account and manage them (Section 4.1).
6. **Find & Report on Domains** - List of all domains, profiles and their vetting level (Section 5).
7. **View SAN License Usage** – View and report on issued Subject Alternative Names (Section 4.2).
8. **Order Certificate** - Order SSL Certificates through the pre-vetted profiles (Section 2.2).
9. **Add New Domain** – Submit a domain to be associated with a specific profile (Section 5.2.1).
10. **Manage Domains** - Manage the domains associated with a specific profile (Section 5).
11. **Other Actions** – Access other actions including Edit Profile, Edit Public Ordering Page & Upgrade vetting level (Section 6).
12. **CSR Checker** - Redirect to the CSR checker page allowing you to parse and verify your CSR (Section 7.1).

1.3

GETTING HELP

Every GlobalSign Enterprise customer has a dedicated Account Manager who is on hand to help with any product and account related inquiries. Additionally, GlobalSign provides technical support through our Client Service departments around the world. See more information at: <https://support.globalsign.com>.

2 ORDERING CERTIFICATES

SUMMARY OF MSSL PRODUCTS

Depending on your account configuration you will see one or more of these product options:

2.1.1 EXTENDEDSSL

2.1

ExtendedSSL is the product name for GlobalSign's Extended Validation (EV) SSL Certificate offering and is issued in strict adherence to the published CA/B Forum EV SSL guidelines covering certificate profile format, vetting method and workflow. This product is limited to a 2-year validity period option (and up to a maximum of 27 months with added renewal/bonus months). It also does not support wildcard nor IP address options.

2.1.2 ORGANIZATIONSSL

OrganizationSSL is the product name for GlobalSign's Organization Validated (OV) SSL Certificates which contain the company name on the certificate subject DN. When placing an OrganizationSSL order into an MSSL profile the applicant has a number of options available to them:

- **Base Certificate Type:** OrganizationSSL supports Standard, Wildcard and Global IP (Publicly routable IP addresses) as values in the certificate Common Name.
- **SAN Options:** Depending on the options configured for your account, you can order certificates with various SAN types including FQDN, Subdomain, Global IP, Unified Communications and Wildcard.
- **Unified Communications Support:** You may specify the entry of the following host names for no additional fee: www, owa, autodiscover and mail.

2.1.3 INTRANETSSL

IntranetSSL Certificates are issued under a set of Non-Public Roots which are not distributed within the major browser or operating system Root key stores. The use of non-Public roots allows the issuance of certificates which do not need to comply with the industry CA/B Forum or Root store requirements, specifically the ability to issue certificates with internal server names. If you want to use IntranetSSL you will need to distribute the Root(s) to your applications and/or browsers accessing sites secured with IntranetSSL or they will receive untrusted CA warnings.

IntranetSSL supports many of the options in OrganizationSSL plus the use of Internal Server names or reserved IP addresses in the CN or SAN, use of the SHA-1 hashing algorithm, as well as certificate validity periods up to 5 years.

2.1.4 CLOUDSSL

CloudSSL is designed for providers of cloud-based services, such as CDNs, VDNs, eCommerce platforms, website builders, and other XaaS, that need to secure services or communications for many customers. CloudSSL Certificates are issued to the service provider at the Organization Validated (OV) level. Customer domains can then be added as Domain Validated (DV) SANs after domain control is verified.

This set up means providers can secure multiple domains with one certificate, which may reduce the need for additional IP addresses. Using a SAN licensing model, each certificate can accommodate up to 500 SANs. Providers can dynamically add and remove domains via APIs and if a SAN is removed,

the license can be re-used for another domain without incurring any additional costs. Once a domain has been vetted, additional sub-domains can be added without additional domain validation. Support for Wildcards offers further flexibility.

Service providers should speak to an Account Manager about activating CloudSSL within Managed SSL.

2.1.5 MSSL PRODUCT FEATURE COMPARISON

This is a summary of the various ordering features and options per product:

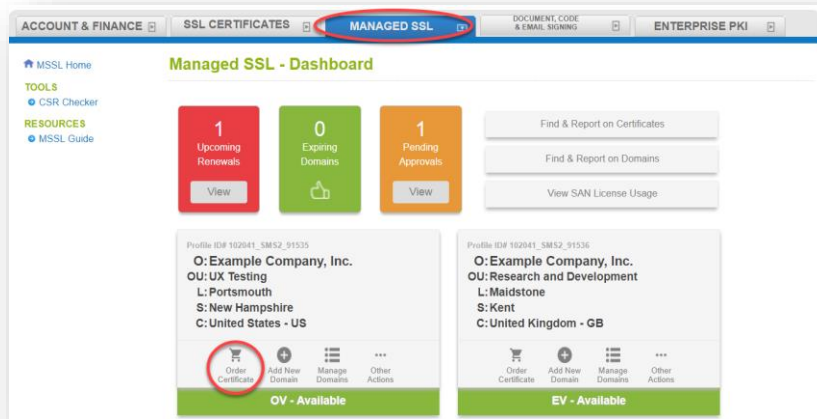
Function	ExtendedSSL	OrganizationSSL	IntranetSSL	CloudSSL
Base Options				
• Wildcard	N	Y	Y	N
• Global IP	N	Y	Y	N
• Private (Internal Server name)	N	N	Y	N
Validity Period in request (years)	Up to 2	Up to 2	Up to 5	Up to 2
Maximum Cert Validity Period	27 months (825 days)	27 months (825 days)	60 months	27 months (825 days)
Type of Order				
• New	Y	Y	Y	Y
• Renewal	Y	Y	Y	Y
• Transfer	Y	Y	N	N
Signing Algorithm (CA Hierarchy)				
• SHA-1	N	N	Y	N
• SHA-256	Y	Y	Y	Y
• ECC P-256	N	N	Y	N
Unified Communications	Y	Y	N	Y
SAN Types				
• FQDN	Y	Y	Y	Y
• Subdomain	Y	Y	Y	Y
• Global IP Address	N	Y	Y	N
• Wildcard	N	Y	Y	Y
• Internal SAN or Reserved IP address	N	N	Y	N
Domain Validity period	13 months	825 days	825 days	365 days
CSR Key Types Supported				
• RSA 2048-4096	Y	Y	Y	Y
• ECC P-256	Y	Y	Y	Y
• ECC P-384	Y	Y	Y	Y
Site Seal	Y	Y	N	N

2.2

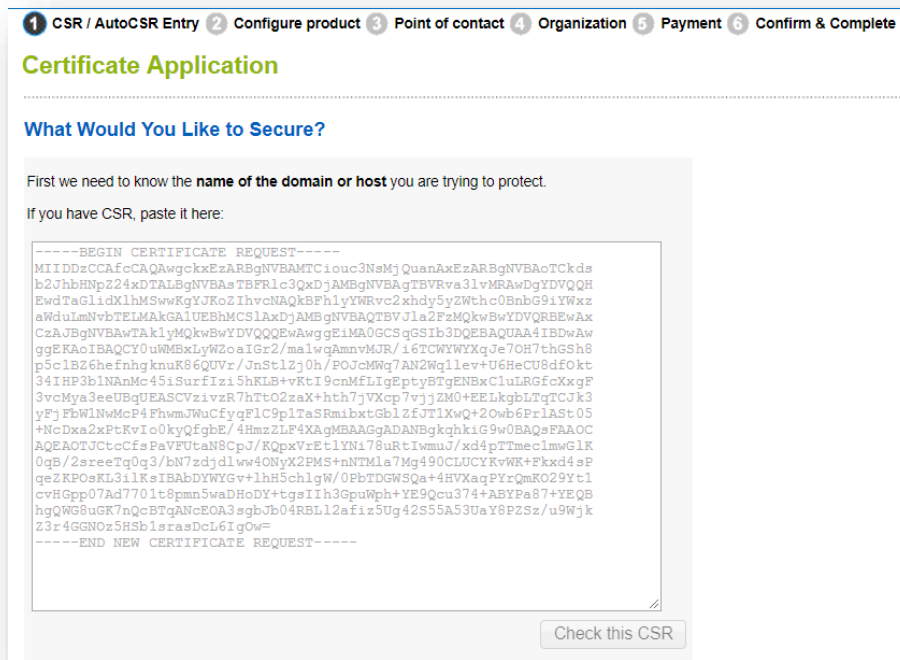
ORDERING MSSL CERTIFICATES

On the **Managed SSL** tab, click the **Order Certificate icon** on the appropriate pre-vetted profile tile.

Note: The domain(s) must be added to the profile and vetting must be completed/ valid, prior to ordering certificates for that domain. See section ADD NEW DOMAIN in this guide for more details.



MSSL Home Screen



Step 1 – CSR Entry Screen

1. You will be prompted to enter a Certificate Signing Request (CSR). For help generating a CSR follow the instructions in this Support article: <https://support.globalsign.com/customer/portal/articles/1229769> . Note: For IntranetSSL, you have the option to enter a common name and use AutoCSR. For IntranetSSL AutoCSR orders, please refer to this [install guide](#).
2. The application workflow will display the product and options available based on that domain's vetting level.

SSL CERTIFICATES | MANAGED SSL | DOCUMENT, CODE & EMAIL SIGNING | ENTERPRISE PKI

1 CSR / AutoCSR Entry 2 **Configure product** 3 Point of contact 4 Organization 5 Payment 6 Confirm & Complete

Certificate Application

Products

OrganizationSSL
 Extended Validation (EV) SSL

Enter Promotional Code

Are you using a Campaign Code or Coupon Code?

No Yes

SSL Certificate Type

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

Wildcard SSL Certificate
 Secures all sub-domains on a single Fully Qualified Domain Name. e.g. the Certificate is issued to *.globalsign.com

Public IP Address SSL Certificate
 Secures a single publicly accessible IP Address such as 210.10.10.01

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.

Step 2 – Configure Product

3. Specify the signing algorithm that will be used to sign the certificate.
4. Specify the point of contact for certificate delivery or vetting issues. Note: You can Auto Fill these fields with the contact information for an existing GCC user. Selecting the **“Is this the Point of Contact for communications”** check box will enable GCC to send email notifications on the email address specified on the **Email Address** field.

Note: If you require **multiple point of contact email addresses** you can enter them as comma separated values in the **Email Address** field. All emails listed will then receive all notifications related to this order, such as order completion, issuance and renewal notifications.

1 CSR / AutoCSR Entry 2 Configure product 3 Point of contact 4 Organization 5 Payment 6 Confirm & Complete

Point of Contact for Certificate Delivery/Vetting Issues

Point of Contact #1

GCC Users: Auto Fill

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: *

Last Name: *

Telephone: *

Email Address: *

Organization Name: If different to above

Department: If different to above

Is this the Point of Contact for communications?: Check the box and to mark this contact as the point of communications for GlobalSign to contact should there be issues with the vetting or renewal of this Certificate.

Back Continue

Step 3 – Specify Point of Contact


- The next steps ask you to confirm your Organization information. This information will be displayed to anyone who clicks on the Site Seal displayed on your website.

1 CSR / AutoCSR Entry 2 Configure product 3 Point of contact 4 Organization 5 Payment 6 Confirm & Complete

Confirm Organization Information

Your Organization Information

You will be able to display the Secure Site Seal on your webpages. When clicked, your visitor will be presented with your company profile. This will give enhanced confidence in your identity. Here is an example of an active Secure Site Seal for the globalsign.com domain.



Organization Name: Example Company, Inc.

Street Address 1:

Street Address 2:

City: Portsmouth

State or County: New Hampshire

Country: United States - US

Other address info:

Business Directory ID / Number:

Back Continue

Step 4 – Confirm Organization & Site Seal Details

6. Select the payment method you wish to use. Not all options may be available based on your account settings:
 - **Credit Card** – Once your certificate has been issued from our system, your card will be charged the full amount.
 - **Payment by Deposit** – Use funds already in your account. If the order is placed by someone without approval privileges your account will be debited upon issuance of the certificate, otherwise your account will be debited immediately.
 - **Payment in Arrears** – This is a post payment option wherein funds will be added to your account after our finance department receives the Purchase Order via email. Availability of this method may vary on your account or region.

7. Finally, review the **Subscriber Agreement**, check the approval box and you will be finished with the application process. Your certificate will now be issued within a few minutes. If the user ordering the certificate **does not** have approval privileges, the order will need to be approved by a user **with** approval privileges before issuance (See Section 2.4).

2.2.1 ADDING SANS DURING THE ORDERING PROCESS

Standard SSL Certificates secure a single Fully Qualified Domain Name (FQDN). By adding SANs, a single certificate can secure multiple server names, such as other domain names, wildcards, subdomains, public IP addresses, internal server names and reserved IP addresses as permitted by the different MSSL products (not all products support all options so only a subset of options will appear depending on the product you are ordering).

To add SANs to a certificate, select the **Add specific Subject Alternative Names (SANs)** option during the second “Configure Product” step of the ordering process. You may add up to 500 SANs per certificate by entering or pasting them, line-separated in the SAN entry window.

Click the **Validate these SANs** button which will validate, categorize and price the SANs accordingly. Follow the remaining ordering steps as listed in the ORDERING MSSL CERTIFICATES section.

Add specific Subject Alternative Names (SANs)

SANs provide the opportunity to protect multiple domains, subdomains, IP addresses or internal server names in the same certificate. [View SAN types available for this order.](#)

No SANs Add SANs

Use the window below to submit line-separated SANs.

store.intranetsitest.com
secure.intranetsitest.com
www2.intranetsitest.com

Summary

Domain Name SANs 3 @ \$0 each

Issued Certificate Will Secure

Common Name GMOCLOUD-PRODUCTION.COM
Domain Name SAN store.intranetsitest.com
Domain Name SAN secure.intranetsitest.com
Domain Name SAN www2.intranetsitest.com

Validate these SANs

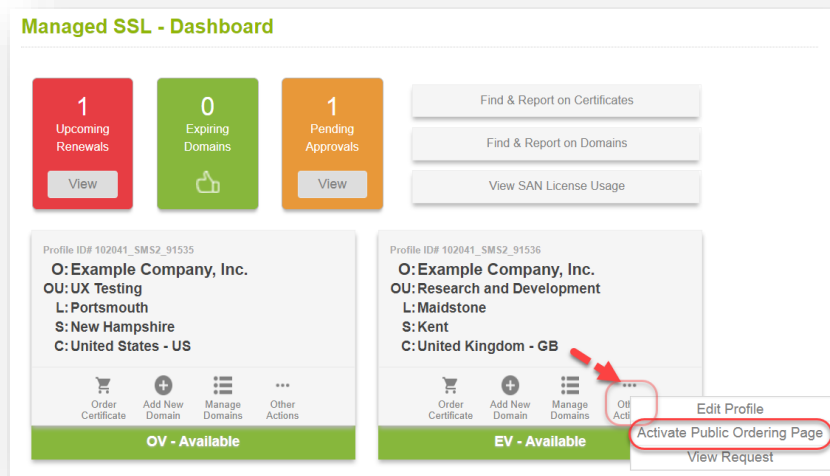
USING THE PUBLIC ORDERING PAGE

SSL Managed Service offers the ability for organizations with distributed offices or departments to centralize the certificate buying process. You can publish a unique application page (Public Ordering Page or POP) so employees or suppliers can apply for a certificate. The URL can be given to applicants or hosted on your intranet. The certificate will not be issued until a User with Approval privileges logs into the account and approves the application – this helps to ensure that organizations issue certificates only to legitimate applicants. For additional security, a pin can be set on the public ordering page.

2.3

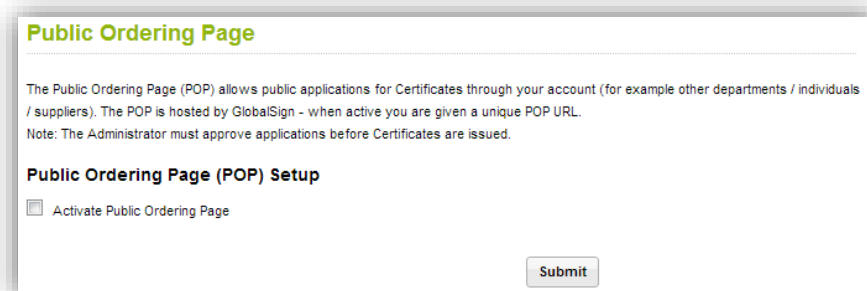
2.3.1 ACTIVATING THE PUBLIC ORDERING PAGE

To activate, edit or deactivate the POP for a pre-vetted profile, go to the MSSL home screen and hover over the **Other Actions** button on the Profile tile. Then click Activate Public Ordering Page (or Edit Public Ordering Page).



Other Actions – Activate Public Ordering Page

When the **Public Ordering Page** screen appears, check the box for **Activate Public Ordering Page** and click **Submit**. To deactivate the POP, uncheck the box and click submit. This will bring up the POP URL, as well as configuration options. See **Configuring the Public Order Page** section below for details.



This page allows you to activate the Public Order Page for a certificate.

2.3.2 CONFIGURING THE PUBLIC ORDERING PAGE

Selecting **Activate POP** for a certificate brings up the POP configuration options.

Within the POP you have the option to upload your corporate logo. Please note the image must be in the format GIF, PNG, or JPG with dimensions no greater than 200x100.

Select the fields you would like to have displayed on the POP by checking the corresponding boxes.

Public Ordering Page

The Public Ordering Page (POP) allows public applications for Certificates through your account (for example other departments / individuals / suppliers). The POP is hosted by GlobalSign - when active you are given a unique POP URL.
Note: The Administrator must approve applications before Certificates are issued.

Public Ordering Page (POP) Setup

Activate Public Ordering Page

Your POP URL:

When the cursor is placed in the textbox, select url.

Upload Logo
Upload your company logo to be displayed on your POP. File format GIF, PNG or JPG with dimensions 200x100 or lower only.
 No file chosen

POP Admin Email Address
This email address will be used as the point of contact for all POP profiles within your account. This account will receive order confirmation, issuance and renewal notifications in tandem with the email address provided by the user who places the order.

POP Configuration Options
Check with items to display on your Public Ordering Page

General Options	Custom Fields
Certificate Types	<input type="checkbox"/> Single Domain Certificate <input type="checkbox"/> Wildcard SSL Certificate <input type="checkbox"/> Public IP Address SSL Certificate <input type="checkbox"/> Subject Alternative (SANs) Options
Validity Period	<input type="checkbox"/> half year <input type="checkbox"/> 1 year <input type="checkbox"/> 2 year <input type="checkbox"/> 3 year <input type="checkbox"/> 4 year <input type="checkbox"/> 5 year
Switching from a Competitor	<input type="checkbox"/> Check box to allow Switching from a Competitor Allows applicant to trade-in competitor's Certificate- trade-ins get further benefits. Leave unchecked to set all applications to New Order only.
Add Authorization Code	<input type="checkbox"/> Add an Authorization Code for access control of Applicants to your POP. Note you must share this Code with applicants via out of bands method. <input type="text"/>
Payment Choices	Payment Method <input checked="" type="radio"/> Use Bulk Deposit <input type="radio"/> Specify When Ordering

POP Configuration Page

- **Certificate Type(s)** – Please note that it is possible to select more than one of these options if you would like to give the recipient flexibility or if you do not know the exact details at the time of configuration.
- **Single Domain Certificate** – is issued to www.example.com (and will contain example.com in the SAN field) and can only be used on that FQDN.

- **Wildcard SSL Certificate** – is issued to *.example.com and can secure all sub-domains of example.com across your entire server farm.
- **Public IP Address SSL Certificate** – is issued to an IP address that is accessible over the internet and will take the form of XXX.XXX.XXX.XX, for example 217.123.236.37.
- **Subject Alternative (SANs) Options** – will allow you to configure any SANs that you require for Unified Communications, specific sub-domains and IP addresses.
- **Validity Period** – Select how long you would like the certificate to be valid for, to the maximum allowed for that particular product (OV = 2 years, EV = 2 years, IntranetSSL = 5 years).
- **Switching from a Competitor** – Choose this option to allow applicants to trade-in a competitor’s certificate. Trade-ins get further benefits, such as deeper discounts, any time remaining on their old certificate transferred to the new certificate and an additional 30 days added to the validity period of the certificate. If you want applicants to only place new orders, leave this option unchecked.
- **Add Authorization Code** – Add an authorization code for access control of applicants to your POP. Note you must share this code with applicants via out of bands method. We do not recommend plain text email for this communication. Digitally signed and encrypted is our recommended method.
- **Payment Choices** – You can choose to have fixed payment method, meaning all costs will be deducted from any bulk balance funds you have in your account, or allow the POP applicant to choose at the point of ordering. The applicant can choose to use existing account funds, pay via purchase order, or use a credit card. You must turn on the option for credit card if you want to make it available to applicants.

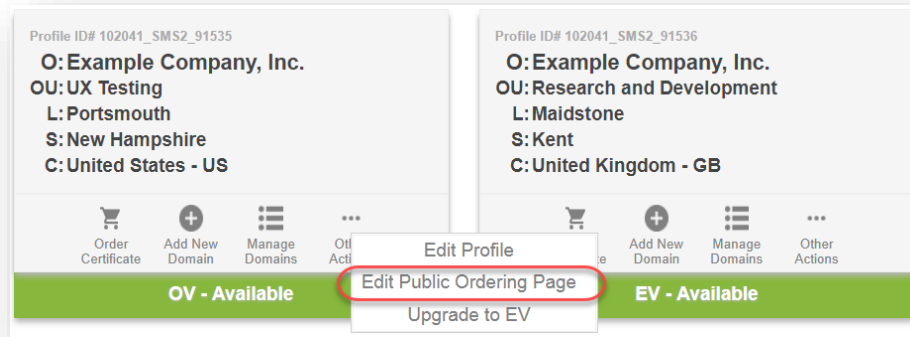
You also have the ability to display custom fields for your environment. Click the **Custom Fields** tab on the **POP Configuration Page** to modify and create fields.

Example custom field entry on the POP Configuration page

For example, if you require an employee number with every request, this can be added as a custom field to your POP. You can make any or all of these fields mandatory. Any custom fields you create will appear under **Contact Information** on the POP itself.

Once you have finished configuring your POP, click **Submit** at the bottom of the screen. You will be asked to review and confirm the configuration. Select **Complete** at the bottom of the page to finalize your POP. You can now pass the URL on to appropriate individuals or host on your intranet.

You can modify the POP at any time by clicking the **Edit POP** icon along the bottom of the certificate profile box.



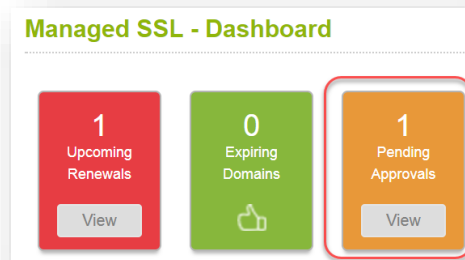
Edit POP Configuration page

APPROVING ORDERS

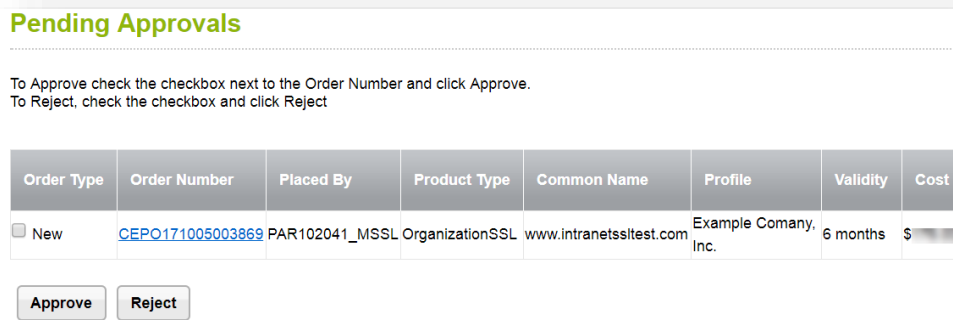
2.4

Applications made by Users **without** approval privileges or applications made using the **Public Ordering Page** must be approved by a User **with** approval privileges. An email confirmation will be sent to applicant informing them that the order needs to be approved by a user with approval privileges. The applicate should inform their designated Administrator regarding the pending order.

Administrators and Users with approval rights can access their lists of pending orders by selecting **View** on the **Pending Approvals** tile on the Managed SSL dashboard or home screen. Each order will have a checkbox next to it. Select the orders you would like to modify and click **Approve** or **Reject**.



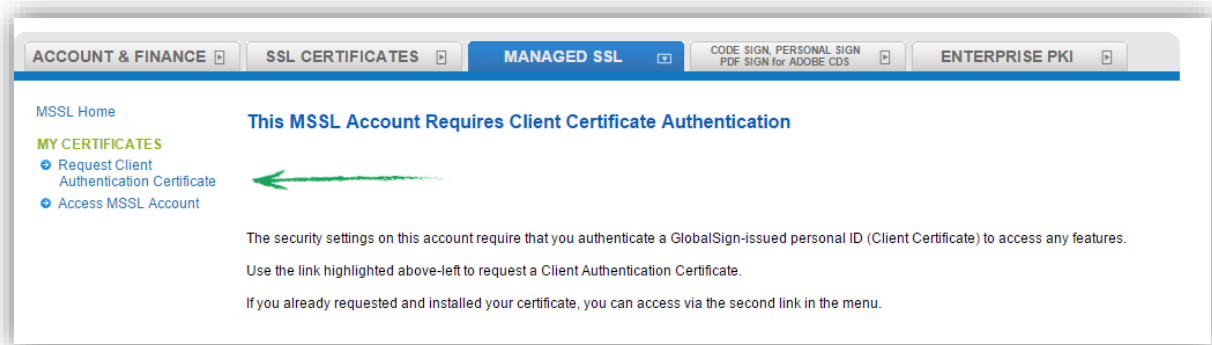
View Pending Approvals – Dashboard Tile



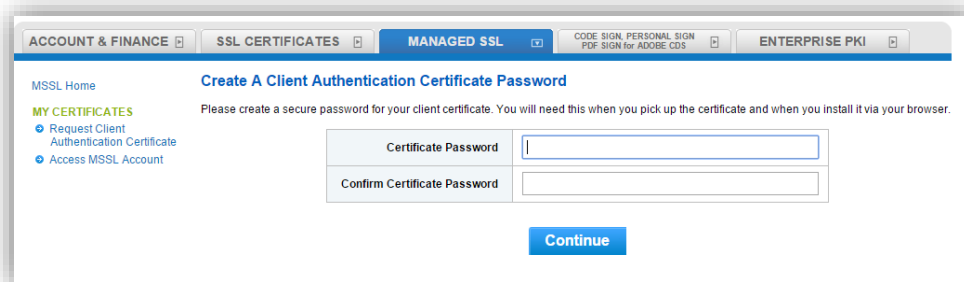
3 CLIENT CERTIFICATE AUTHENTICATION

You have the option to enable Client Certificate Authentication as an additional security feature when accessing your Managed SSL Account. To enable client authentication contact either your Account Manager or GlobalSign Support. Once enabled, you will not have access to the Managed SSL tab until you request and install a Client Certificate as outlined below.

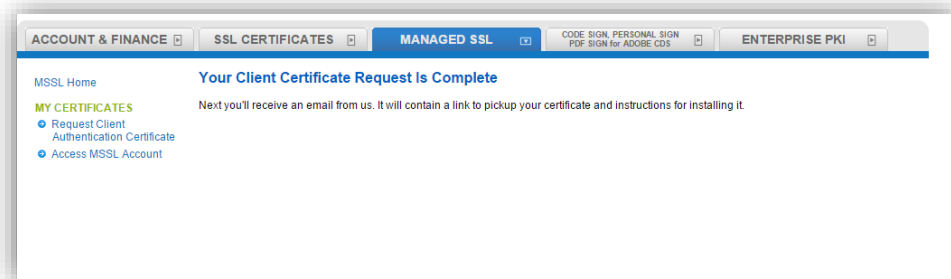
Log into your account and click on the **Managed SSL** tab. Click on the **Client Certificate Authentication** link located on the left side of the page.



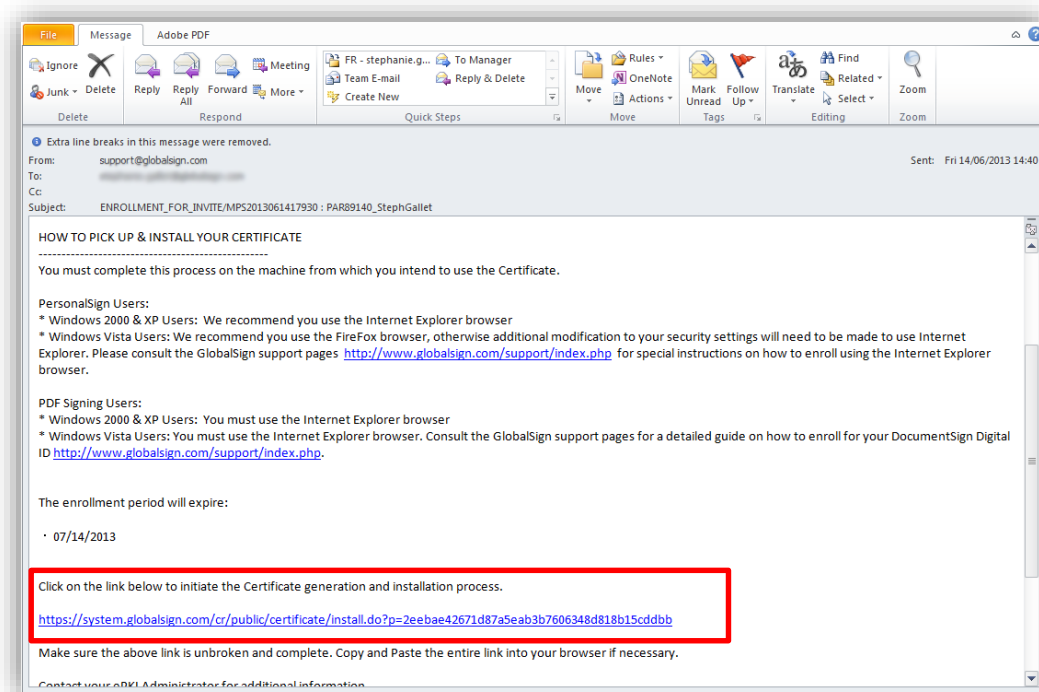
You will be asked to create a secure password. This is a one-time-use temporary pickup password. It will be required to download the Client Authentication Certificate.



Create the pickup password, click continue and you will reach a confirmation page.

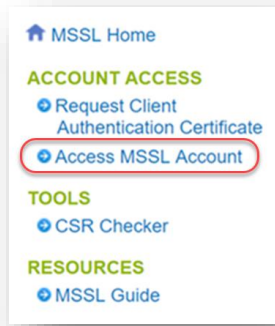


Next you will receive an email with a link for picking up and installing the Client Certificate. Click on the Certificate pick-up link (URL) in the email sent to you in order to start installing your certificate.

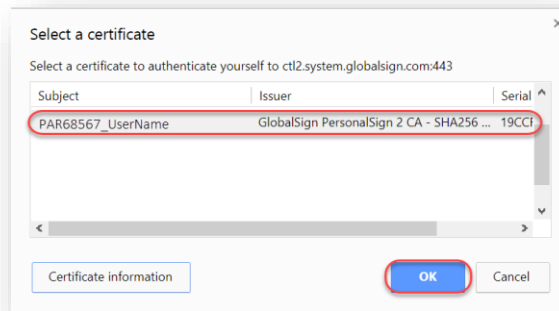


Follow the steps in this [Support Article to download and install your Client Authentication Certificate](#).

At the end of the process, a pop up from the Certificate Import Wizard will confirm that the installation was successful. Then you can then go back to your account, click **Access MSSL Account** on the left hand side.



You will be prompted to select the Client Certificate that you just installed. You can verify the correct certificate as its common name will be your Account User Name.



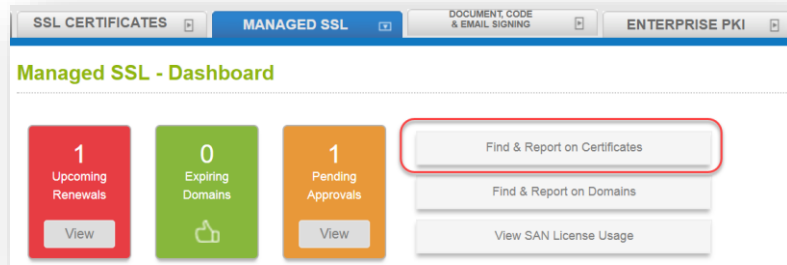
You will then have full access to all of the MSSL portal's functionality.

Note: Client Certificates issued to EPKI administrators for accessing the Enterprise PKI tab can also be used for the MSSL client certificate authentication.

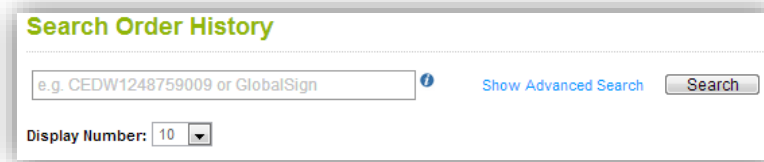
4.1 4 MANAGING & REPORTING ON CERTIFICATES AND ORDERS

SEARCHING FOR CERTIFICATES

From the Managed SSL home screen or dashboard, click on **Find & Report on Certificates**.

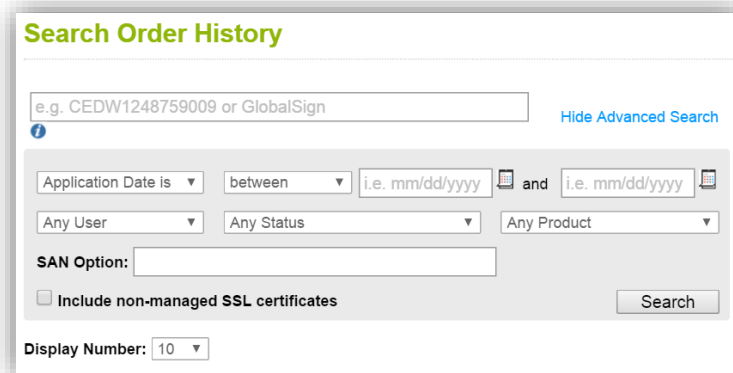


This brings you to the reporting interface to access orders and certificates. Simply click Search will display all certificate orders. The default basic search allows you to search by **order number** or certificate **common name**.



Basic Search – Search by Order Number or Common Name

Click **Show Advanced Search** for additional search criteria, such as application/issue/expiration dates, user, status and product.



Advanced Search Options

The advanced search option labeled: **Include non-managed SSL Certificates** allows you to search for all SSL Certificates including non MSSL Certificate orders associated with your account. For example, this option will allow you to see any order from the *SSL Certificates* tab (Individual Ordering tab).

4.1.1 SEARCH RESULTS

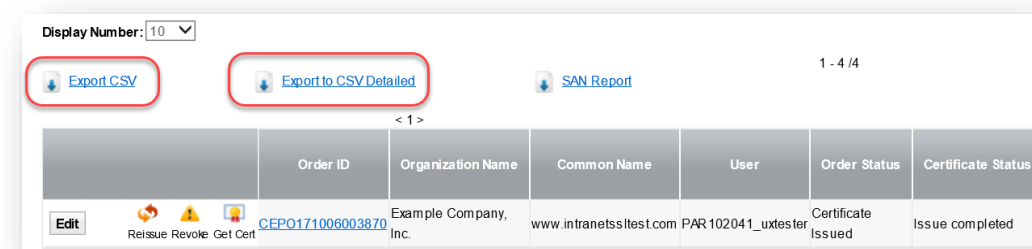
Define the appropriate search criteria and click **Search**. A list of certificates will appear and you will notice **quick action lifecycle management** icons next to each order (e.g. revoke, reissue, Get Cert). If the certificate is within the 90-day renewal window, a renew icon will also appear. See Section 4.3 - **Certificate Actions** below for more information.

Note: Any non-MSSL Certificates in your search results will be highlighted in green.

The following details will be displayed for each order:

- Common Name
- Product Name
- Key Type
- Signature Algorithm
- Order Status
- Certificate Status
- Application Date
- Issue Date
- Expiration Date

All of these details are exportable to a CSV report, either as a summarized list by clicking **Export CSV**, or a complete detailed list by clicking **Export to CSV Detailed**.



The screenshot shows a web interface with a table of certificate orders. At the top, there is a 'Display Number' dropdown set to '10'. Below it are three buttons: 'Export CSV', 'Export to CSV Detailed', and 'SAN Report'. The table has columns for Order ID, Organization Name, Common Name, User, Order Status, and Certificate Status. A single row is visible with the following data: Order ID: CEPO171006003870, Organization Name: Example Company, Inc., Common Name: www.intranetssltest.com, User: PAR102041_ujtester, Order Status: Certificate Issued, Certificate Status: Issue completed. There are also icons for 'Edit', 'Reissue', 'Revoke', and 'Get Cert' next to the Order ID.

Order ID	Organization Name	Common Name	User	Order Status	Certificate Status
CEPO171006003870	Example Company, Inc.	www.intranetssltest.com	PAR102041_ujtester	Certificate Issued	Issue completed

4.2

SAN REPORTING & SEARCH

Use the reporting function within MSSL to manage all issued Subject Alternative Names (SANs).

4.2.1 SUMMARY SAN REPORT

From the Managed SSL home screen click on **View SAN License Usage**. From this report you can view all **active SANs** that are currently in use by certificate type, OV, EV, OV/EV Combined and IntranetSSL. An active SAN is any SAN which is not expired, revoked or cancelled.

SSL CERTIFICATES | MANAGED SSL | DOCUMENT, CODE & EMAIL SIGNING | ENTERPRISE PKI

Managed SSL - Dashboard

1
Upcoming Renewals
[View](#)

0
Expiring Domains
[View](#)

1
Pending Approvals
[View](#)

[Find & Report on Certificates](#)

[Find & Report on Domains](#)

[View SAN License Usage](#)

SAN Report

Counts of unique SANs in **currently active** (not expired, cancelled or revoked) certificates **not covered by your license**.

SAN Type	SANs in Use
OVSSL	3

Display Number:

[Export to CSV Detailed](#)

< 1 >

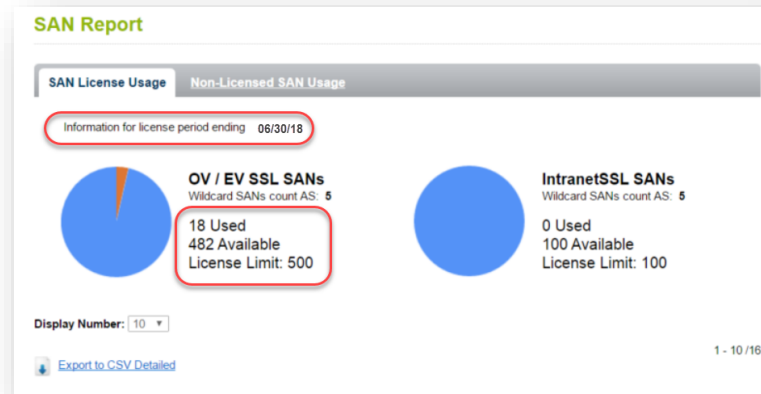
OrderID	Order Status	Product	SAN
CEPO171006003870	Certificate Issued	OrganizationSSL	www.intranetsitest.com
CEPO171006003870	Certificate Issued	OrganizationSSL	secure.intranetsitest.com
CEPO171006003870	Certificate Issued	OrganizationSSL	store.intranetsitest.com
CEPO171005003869	Order awaiting Account Administrator approval	OrganizationSSL	www.intranetsitest.com
CEPO171005003867	Certificate Issued	OrganizationSSL	www.intranetsitest.com

[Export to CSV Detailed](#)

SAN Summary Report

You can also export a report of your active SANs by clicking **Export to CSV Detailed**.

If you have a MSSL SAN License agreement established for your account, **SAN Limits** and the license expiration date will also be displayed in the SAN Summary Report.



SAN Summary Report (Active MSSL SAN License)

4.2.2 SAN SEARCH

To look up a specific SAN and the associated certificate order(s), click on **Find & Report on Certificates** reporting tile on the Managed SSL home screen. Click **Show Advanced Search**. Specify the appropriate SAN in the **SAN Option** field and click **Search**. The search results will display all SANs you have searched for including active, expired, revoked as well as cancelled SANs.

The image shows a 'Search Order History' form. It includes a search input field with a placeholder 'e.g. CEDW1248759009 or GlobalSign' and a 'Hide Advanced Search' link. Below the input field are several filter options: 'Application Date is' with a dropdown, 'between' with a dropdown, and two date input fields with a 'i.e. mm/dd/yyyy' example and a calendar icon; 'Any User' with a dropdown, 'Any Status' with a dropdown, and 'Any Product' with a dropdown. There is a 'SAN Option' field containing 'mail.johnsonstest.com'. A checkbox for 'Include non-managed SSL certificates' is present and unchecked. A 'Search' button is located to the right of the checkbox. At the bottom, there is a 'Display Number' dropdown set to 10.

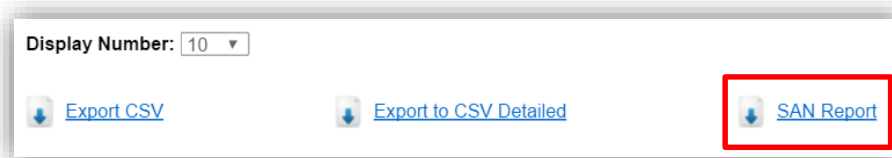
SAN Option Search

Click the **OrderID** link to open the **Certificate Details** and scroll down to the **SANs Option** section to view the SANs associated with the certificate.

SANs Options	
SANs Options	Subject Alternative Name
PV FQDN SAN	mail.johnsonstest.com
PV FQDN SAN	contact.johnsonstest.com

Certificate Detail - SAN Options

You can also export a report of the search results by clicking **SAN Report** which will export a list of the SANs in a CSV format.



Export SAN Results

4.3 CERTIFICATE ACTIONS

4.3.1 REISSUE AN SSL CERTIFICATE

If you need to reissue a certificate in the case of corrupt / broken keys, server reinstall etc., you can do so directly through your account.

1. Click **Find & Report on Certificates** and use the search function to find the certificate you need to reissue.
2. Once the certificate appears in the search results, click the **Reissue** button.



Please note that although you can choose to use a new CSR, the DN information from the profile will be used. The reissued certificate will only be valid for the period remaining on the initial certificate.

4.3.2 RENEW AN SSL CERTIFICATE

You can view a list of expiring certificates (90 days before expiration) by clicking **View** on the **Upcoming Renewals** tile on the Managed SSL home screen. For notification purposes, the tile will dynamically appear **orange** or **red** and display the number of upcoming expiring certificates. Simply click the **Renew** button that appears next to the certificate.



You can also renew certificates using the **Find & Report on Certificates** function.

1. Click **Find & Report on Certificates** and use the search function to find the certificate you need to renew.

2. Once the certificate appears in the search results, click the **Renew** button. Please note: this button will only appear if the certificate is within the renewal range (90 days before expiration).

GlobalSign will send a renewal notice to the contact(s) associated with the order 90 days prior to the expiration of the certificate. See the **User & Contact Details** section below for information on modifying contacts.

If you renew a certificate before it expires, GlobalSign will add any remaining time to the new certificate and optionally add an extra 30 days free of charge.

4.3.3 REVOKE A CERTIFICATE

If your server and / or private keys have been compromised, then you will want to revoke the certificate. Revoking an SSL Certificate will invalidate the certificate. This will add the certificate serial number to the GlobalSign Certificate Revocation List (CRL) and OCSP servers, which are then propagated across the internet. When a web browser encounters a revoked SSL Certificate on a website, it will warn the visitor that the site should not be trusted.

Note: Revoking a certificate is not the same as getting a refund/cancelling an order. The Revoke Certificate option will be available throughout the validity period of the certificate unlike a cancellation request.

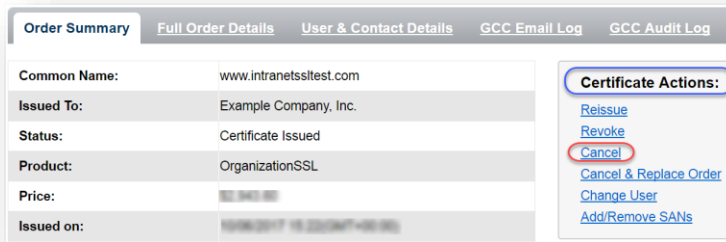
1. To revoke a certificate, **Find & Report on Certificates** and use the search function to find the certificate you need to revoke.
2. Once the certificate appears in the search results, click the **Revoke** button.



4.3.4 CANCEL A CERTIFICATE

This option will be available for 7 days after issuance of the certificate. Choose this to completely cancel your order and have the funds credited to you (via the original payment method).

1. Click **Find & Report on Certificates**; use the search function to find the order that you wish to cancel.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. On the **Order Summary** tab, click **Cancel** under the **Certificate Actions** menu in the right column.



Cancel Certificate Screen

4.3.5 CHANGE USER ASSOCIATED WITH CERTIFICATE

This assignment dictates who will receive notifications associated with the certificate. The person that applied for the certificate is automatically assigned this role, but the user can be changed. This function is especially useful during employee and role transitions within an organization.

1. Click **Find & Report on Certificates**; use the search function to find the certificate to be modified.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. On the **Order Summary** tab, click **Change User** under the **Certificate Actions** menu in the right column.

4.3.6 ADD/REMOVE SANS

This option will enable you to change the Subject Alternative Names (SAN) configuration of your certificate. By adding SANs, a single certificate can secure multiple server names, such as other domain names, wildcards, subdomains, public IP addresses etc. The types of SAN options available are dependent on the certificate type.

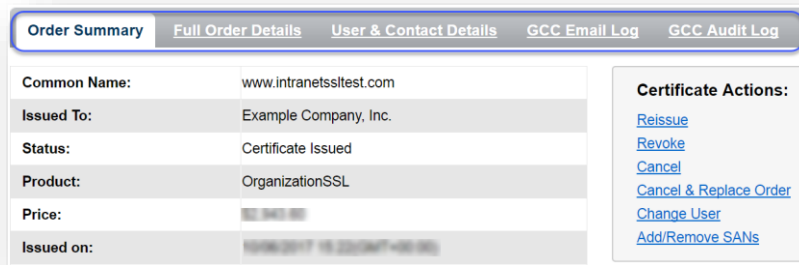
1. Click **Find & Report on Certificates**; use the search function to find the certificate to be modified.
2. Click the **Edit** button next to the appropriate certificate to bring up the **Order Details** screen.
3. On the **Order Summary** tab, click **Add/Remove SANs** under the **Certificate Actions** menu in the right column.

4.4

Follow this Support Article for additional instructions: [How to Add or Remove SANs](#).

CERTIFICATE DETAILS

After performing a search for certificates, you can click **Edit** next to any certificate found in the search results to see details regarding that order.



Complete order details, found under the **Edit** button

4.4.1 ORDER SUMMARY

The **Order Summary** tab displays top level information regarding the order. Details such as product, price, and validity period are shown. You can also find certificate files in various formats here. Important actions relating to the certificate lifecycle can be performed from this screen. For more information on these actions please see **Certificate Actions** above.

4.4.2 FULL ORDER DETAILS

The **Full Order Details** tab provides all information relating to a particular order, such as download status of the .pfx file, the second half of the .pfx password and any SAN options. You can also copy and paste the CSR and issued certificate from this screen, should the need arise.

4.4.3 USER & CONTACT DETAILS

This screen allows you to view and edit the user associated with the order. Please note that any changes made here **will not** be domain-wide and only apply to this particular order. Click **Update** to save any changes.

4.4.4 GCC EMAIL LOG

View all emails that have been sent from the system regarding this order. Typically, you will see **Order Confirmation** and **Order Issuance** (with **Final Action Needed** also listed for EV orders).

4.4.5 GCC AUDIT LOG

View all actions associated with an order, together with date/time stamps of when events occurred. This screen also specified who performed the action, whether it was GlobalSign (SYSTEM) or a user within your account.

Order Details for CEPO1108249494

Order Summary Full Order Details User & Contact Details GCC Email Log **GCC Audit Log**

[Export to CSV](#)

Action details	Action date	Result	User ID
CERT ORDER	08/24/2011 13:00:28(GMT+00:00)	SUCCESS	PAR05988_globalsign
CERT ORDER VALIDATION REQUEST	08/24/2011 13:04:06(GMT+00:00)	SUCCESS	SYSTEM
CERT ISSUED	08/24/2011 13:06:02(GMT+00:00)	SUCCESS	SYSTEM
SEAL_REGISTER	08/24/2011 13:06:02(GMT+00:00)	SUCCESS	SYSTEM
DOWNLOAD_PKCS12	08/30/2011 13:30:10(GMT+00:00)	SUCCESS	PAR05988_globalsign
EDIT_CONTACT	08/30/2011 13:41:05(GMT+00:00)	SUCCESS	PAR05988_globalsign

[Export to CSV](#)

GCC Audit Log – see what happened, when, and by whom

5 MANAGE DOMAINS & PROFILES

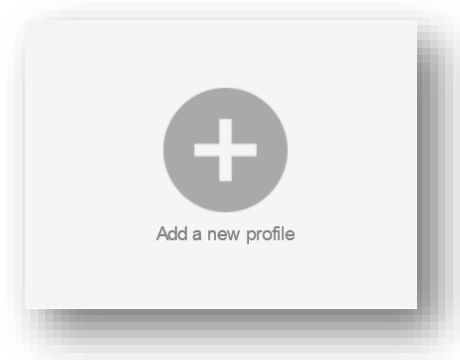
The concept behind Managed SSL is instant issuance and simplified management of certificates for all domains owned by one account. Accounts can consist of one **single organization** or an **umbrella entity** (MSSL Pro), containing multiple companies, branches and departments. These subdivisions are collectively known as **profiles** and contain unique enterprise data and their own set of domains. Each subsidiary can have its own profile Organizational data, related domains and delegated users with specific permissions, while still centralizing management and billing for the parent account.

5.1

MANAGING PROFILES

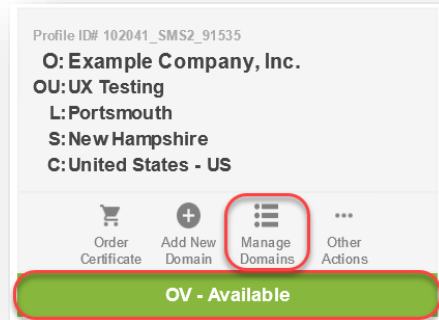
In order to upgrade your MSSL account to Pro, where you can have multiple profiles with separate DN information, please first consult with your Account Manager. Note: **Only** MSSL Pro customers are able to have more than one profile within their account.

After an account has been upgraded to MSSL Pro, the **Add a New Profile** tile will appear on the MSSL Home Screen. Click the **Add** symbol on the Add New Profile tile to set up a new profile.



The Profile status will appear at the bottom of the Profile tile and may have the following status:

- OV – Queued for Vetting
- OV – Available
- EV – Queued for Vetting
- EV – Available



Profile Tile and Manage Domains Icon

5.1.1 EDIT PROFILE

Hover over the **Other Actions** button on the Profile tile and then select **Edit Profile** to amend details contained within your profile.

Note: If your profile is active this action will **suspend** the PROFILE until our Vetting Department have verified the new information and re-activated it. Changes are not retroactive.

5.2 MANAGING DOMAINS

5.2.1 ADD NEW DOMAIN

Once Profile vetting is complete, you need to add and verify Domains to the profile before you can begin issuing certificates. Follow the steps below to add a domain and complete the domain verification steps. Note: Domains must be re-verified or “renewed” after a given time period (varies per product). See the RENEWING DOMAIN section for details.

Click **Add New Domain** to add another domain to a profile.

Note: For **MSSL Pro** Accounts, please ensure that you add the domain to the correct profile.

1. Enter the Domain Name to be associated with the Profile.

Submit a Domain Name

Please enter a top level domain to be associated with the profile below.

O: MSSL Test
OU:
S: Portsmouth
P: New Hampshire
C: UnitedStates

Please **only submit a Top Level Domain** e.g. **domain.com** - no subdomains. You can order certificate with subdomains, like **store.domain.com** once the top level domain has been approved.

Domain name

I intend to order EV certificates for this domain

Continue

Note: If you intend to order **EV SSL** and/or **CloudSSL** for the domain, check the applicable box.

Domain name

I intend to order CloudSSL certificates for this domain

Continue

Adding a New Domain that will be used for **CloudSSL**

Note: CloudSSL must first be enabled in your MSSL Account. Service providers should contact their Account Manager to activate this product.

2. Enter a Point of Contact for the Domain Order.
 3. Select a **Domain Validation Method**. View the following Support Articles for further assistance:
[MSSL Domain Validation Methods](#).
- **Email Approval Method** –
Support Article: [Performing Domain Verification - Approver Email](#)
 - **HTTP Based Verification Method** –
Support Article: [Performing Domain Verification - HTTP Verification Method](#)
 - **DNS Approval Method** –
Support Article: [Performing Domain Verification – DNS TXT Record](#)

Select a Domain Validation Method

Please select from the following methods for **demonstrating domain control**.

Email Verification

We send an email to one of the addresses displayed below and you follow the instructions inside.

WHOIS Email Addresses

i[redacted]m@contactprivacy.com

Constructed Domain Email Addresses

admin@[redacted].com

administrator@[redacted].com

hostmaster@[redacted].com

postmaster@[redacted].com

webmaster@[redacted].com

HTTP Verification

We provide a Domain Verification Code (DVC) and you place that DVC in a text file in a specific location on your website.

Use HTTP verification

DNS Verification

We provide a Domain Verification Code (DVC) and you create a DNS record containing the DVC.

Use DNS verification

Manual Verification Method

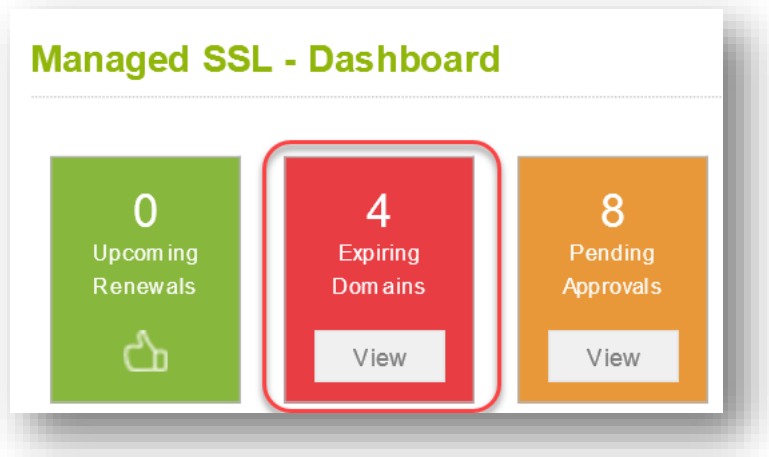
Industry restrictions mean that manual Domain Validation Methods are no longer available. Please select from one of the methods above.

Select a Domain Validation Method Screen

4. **Confirm Details:** Confirm the order information and complete the order.

5.2.2 RENEWING DOMAINS

Domains must be renewed or re-validated prior to expiration or you will not be able to issue, renew or reissue certificates containing those domains. You can view a list of your expiring domain (90 days before expiration) by clicking **View** on the **Expiring Domains** tile on the Managed SSL home screen. For notification purposes, the tile will dynamically appear **orange** or **red** and display the number of upcoming expiring domains. (Note: View the [MSSL Product Feature Comparison chart](#) for more details on Domain validity periods per product type).



Expiring Domains Tile

Click **View** on the Expiring Domains tile and then click the **Renew** button that appears next to the domain. Note: When a Domain expires, it does not affect existing Certificates. However, you will not be able to issue or re-issue a Certificate unless all domains in the Certificate are vetted (not expired). If you have expiring domains that are no longer used, you can delete them and they will be removed from the Expiring Domains tile.

For additional instructions on renewing domains, please refer to this Support Article: [Renewing MSSL Domains](#)

5.2.3 MANAGE DOMAINS

Click the **Manage Domains** icon on the profile tile to delete, set permissions, renew and verify, and view the status of all domains for a profile. A brief description of the domain management options are listed below.

Manage Domains

Profile ID# 102041_SMS2_91535

O: Example Company, Inc.
OU: UX Testing
L: Portsmouth
S: New Hampshire
C: United States - US

OV - Available

Manage the domains associated with this profile.
 You can also [view domain order history](#)

e.g. GlobalSign or www.globalsign.com

Actions				Domain (Domain ID)	Status	Expiration Date (GMT+00:00)	Validation Date (GMT+00:00)
				intranetssltest.com (DSMS22103465557)	Available		
				gmodcloud-production.com (DSMS22103465558)	Available		

1. **Delete:** Click the **Delete** icon to delete a domain that is no longer needed.
2. **Permissions:** Click the **Permissions** icon to bring up a list of all users listed for that domain.

Set User Permissions for [globalsign.com](#)

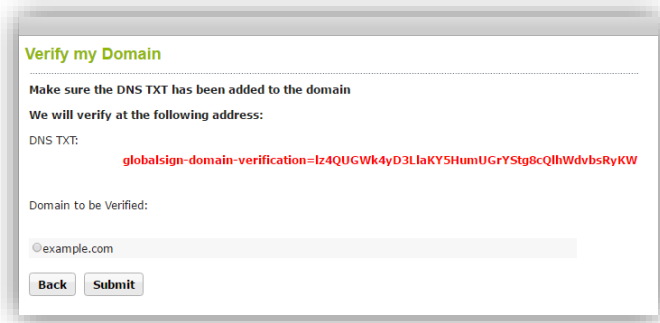
ID	Name	Order Permissions		
		Place Orders	Approve Orders	Revoke Certificates
PAR05988_global99	Test User	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Users available for selected domain

Specify the permissions Staff in Charge users should have by checking the appropriate boxes:

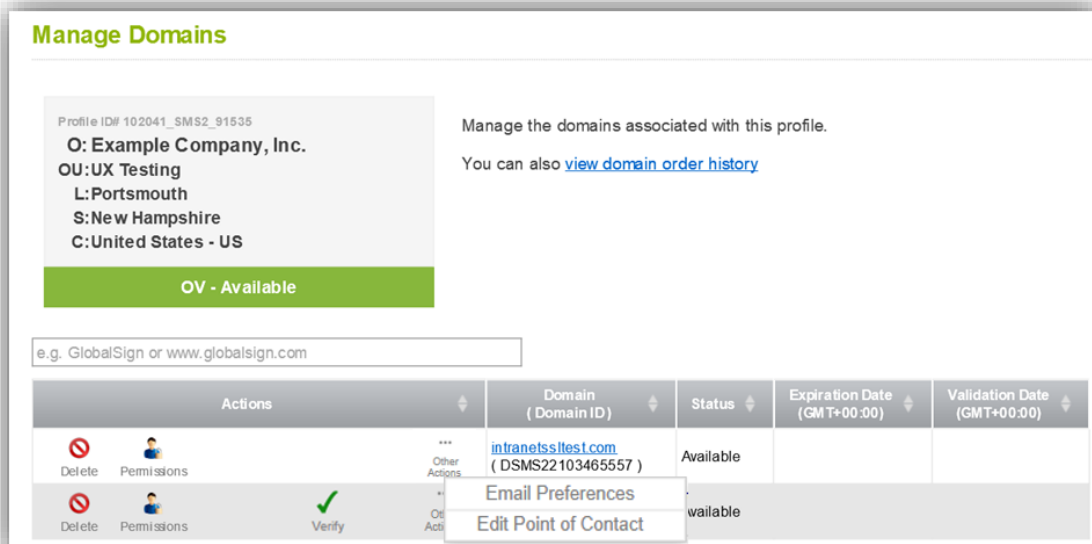
- **Place Orders** – the user can place orders for a particular domain.
- **Approve Orders** – the user can approve orders placed by him/herself or others users for a particular domain.
- **Revoke Certificates** – the user can revoke Certificates issued to a particular domain.

3. **Renew:** Click the **Renew** icon to renew expiring domains (the renewal option is available up to 90 days prior to expiration).
4. **Verify:** Click the **Verify** icon to verify a domain submitted with the **DNS TXT** or **HTTP Verification**.



Verify my Domain Screen

5. **Domain ID:** Click on the domain name (hyperlink) to view details including profile details, basic domain details, point of contact and an action log specific to that domain.
6. **Other Actions:** Hover over the **Other Actions** icon to show the **Email Preferences** and **Edit Point of Contact** icons.



- **Email Preferences:** Click the **Email Preferences** icon to open the **Manage Renewal Reminder Emails** window. The user can enable / disable the renewal reminder per domain by checking off either On / Off for **Renewal Reminder Emails**. The renewal notice will go to the person that placed the domain order and optionally to the Domain Point of Contact if the “Is this the Point of Contact for communications” checkbox is checked. You can check the person that placed the domain order by clicking domains on the **Manage Domain** page. This brings up the **Domain Details** page and you can find User ID starting with **PAR** for the domain order in **Action History**.

Manage Renewal Reminder Emails

Renewal reminder emails may be enabled/disabled on a domain-by-domain basis to control email volume around renewal time.

Domain name: example.ssllerts.jp

Renewal Reminder Emails: On Off

Close

Note: Renewal Reminder Emails are set **default On**.

- **Edit Point of Contact:** Click the **Edit Point of Contact** icon to bring up the **Point of Contact** window. The user can edit the PoC information for domain submitted at 5.2.1.2.

Point of Contact

Point of Contact #1

GCC Users: America Portsmouth **Auto Fill**

By ordering this domain you will receive all vetting and renewal-related emails. If you wish to specify an additional POC to also receive these communications, you may do so here.

*** Required field**

First Name: * America

Last Name: * Portsmouth

Telephone: * +44(0)1622 766766

Email Address: * america.portsmouth@globalsign.com

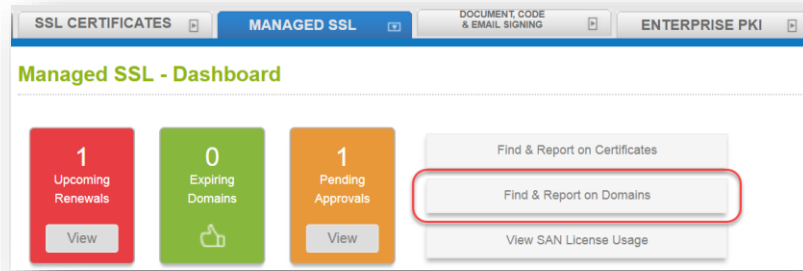
Is this the Point of Contact for communications?: Check the box and to mark this contact as the point of communications for GlobalSign to contact should there be issues with the vetting or renewal of this domain.

Save **Close**

Note: The **Email Preferences** and **Edit Point of Contact** icons are only shown to the user who has **Place Orders** permission enabled at 5.2.3.2.

5.2.4 SEARCHING FOR DOMAINS

You can search for domains associated with any profile by clicking **Find & Report on Domains**, located on Managed SSL home screen.



Find & Report of Domains – Reporting Function

This brings you to the reporting interface to search for domain orders. Click **Show Advanced Search** for additional search criteria, such as order date and vetting status. You can also access the domain management actions from this screen, including: renew, verify, delete, permissions etc.

5.2.5 ACTIVATE POP or EDIT POP

If the Public Ordering Page (POP) has not been activated, then you can active it by hovering over the **Other Actions** icon and selecting Activate Public Ordering Page. If it was previously activated, you can select Edit Public Ordering Page.

5.2.6 EV APPLICATION

Hover over the **Other Actions** icon and click the EV Application Form which contains all of the relevant EV data GlobalSign has verified and configured for this profile.

5.3

UPGRADE TO EV LEVEL VETTING

Hover over the **Other Actions** icon and click **Upgrade to EV** to upgrade a profile to the Extended Validation (EV) level. Appropriate vetting will take place and the account will be re-activated once completed.

While upgrading, you will be asked for some additional information to enable GlobalSign to efficiently vet the account. Please have details, such as company number, authorized personnel and place of business available. You will also need to print off an EV request form provided during the application process and submit it to our Vetting Team. Upon receipt of the request form, the Vetting Team will send a subscriber agreement to your designated authorized person for signing.

In addition to upgrading the Profile, the domain(s) will also need to be vetted to the EV level. Until this is completed, the domains may be used only for OV Certificate issuance. To upgrade one or more of the domains in the profile, click the **“Manage Domains”** icon and then to **“Manage Domains”**. Click the **“Upgrade to EV”** Action icon and follow the instructions.

6 ACCOUNT AND FINANCE PAGE

All financial activity is controlled and monitored from the **Account & Finance** tab of your GCC account.



Account and Finance Home Screen

LICENSING OPTIONS

GlobalSign offers flexible purchasing and licensing options to suit your business needs.

6.1

6.1.1 BULK PURCHASE

The most common method for purchasing certificates is via a bulk purchase. This allows full flexibility regarding validity periods and with ordering options like additional SANs or Wildcard Certificates. The cost of the certificate (including selected certificate options) are deducted from your bulk balance which is valid for 1 year. You can add more funds at any time through the Account & Finance tab and pay with Credit Card, PO and/or arrange different payment terms. Greater bulk balance purchases result in greater discounts. Contact your dedicated Account Manager for details.

6.1.2 PAY AS YOU GO

If you're not sure of your annual needs, you can use our Pay-As-You-Go (PAYG) model and each order will be charged to your registered credit card. This is ideal for low volume customers who do not want to commit to a bulk purchase.

6.1.3 CERTIFICATE LICENSING

Per certificate licensing makes it easy to manage annual costs based on your projected usage. We'll work with you to define the exact parameters and product mix and then set a price for your annual certificate needs which align with your budgetary cycles. Please contact your Account Manager for details and attractive pricing.

6.1.4 SAN LICENSING

If you are using your certificates to secure server inventories that change on a regular basis where 1-year certificates would not be cost effective, then you can opt for MSSL SAN Licensing. This allows you to specify the **maximum number of unique SANs you need active at any given time**.

When you have a certificate with a SAN that is no longer needed, you can use the Add/Delete SAN option to remove it and optionally add a new one. You can also **Cancel** and/or **Revoke** orders and the SAN licenses will be returned to your inventory for reuse. Note: The standard 7-day cancellation policy does not apply with SAN licensing orders; you cancel certificates at any time, even after 7 days and the SANs that were used are returned to the available pool.

Ordering a certificate with a SAN that already is active does not count against your SAN license so

you can **obtain multiple certificates for the same SANs without consuming more licenses**. This is excellent for customers that need to secure changing development servers and for customers that offer trial accounts so they can effectively provide security without wasting 1-year certificates.

An MSSL SAN license is based on a set threshold of unique active SANs for your account. The threshold is set for either OV, EV, or both EV and OV Certificates, as well as IntranetSSL Certificates. We process Wildcard SANs as 5 SAN licenses for optimal flexibility.

PAYMENT OPTION –DEPOSITING FUNDS INTO ACCOUNT

By using the account funds option, you are eligible for discounts. To be able to pay for certificates using deposited funds, you must first deposit funds into your account. Navigate to the **ACCOUNT & FINANCE** tab and click the **Add Deposit** menu item, under the **MY FINANCES** section on the left side.

6.2

6.2.1 ADD DEPOSIT

If you simply want to add a set amount of funds to your account, you can choose to add a deposit at any time. Click **Add Deposit** and input the amount of money that you wish to add to your account (minimum of \$200). Confirm the amount and you will be taken to the payment process.

Direct purchase of deposit	
Account Balance	GBP:0.00
Deposit money	1000
Purchase order Number <small>To appear on your invoice</small>	
Select Payment Method	
Payment details	<input checked="" type="radio"/> Bank Transfer: <input type="radio"/> Payment in Arrears – Invoice to be paid as per applicable payment terms <input type="radio"/> Credit card
<input type="button" value="Confirm"/>	

Add Deposit Option

6.2.2 HOW TO PAY FOR YOUR DEPOSIT

Complete the steps for **Add Deposit** as detailed above to add funds to your account. You have two payment options to settle the deposit amount.

- **Bank Transfer – Payment in Arrears**
Select to pay for deposit via Purchase Order. Funds will be added to your account after our finance department receives the Purchase Order via email.
- **Credit Card**
You will be asked to provide the details for the selected Credit Card before the Deposit amount is added. The credit card is charged immediately.

When buying certificates using the funds you have deposited, be sure to select **Deposit** as the **Payment Option** at the payment point in the purchasing process.

6.2.3 DEPLETED DEPOSITS

If you deplete your current deposit, you should add additional deposit or alternatively you may

downgrade to a Pay-As-You-Go account. In order to maintain current discount levels, you should add an additional deposit.

VIEW/REQUEST INVOICES

Click **View/Request Invoices** under the **MY FINANCES** section of the left navigation menu to view all the invoices that have been generated. **Invoices will appear here 8 days after the issuance of the certificate.** You can search by invoice number and date to quickly find a specific invoice.

6.3

The screenshot shows the 'Invoice view page' with search filters and a table of invoices. The search filters include: Invoice number (e.g. BL200506000001), Issue date (e.g. 07/30/2007), and Show Invoices of canceled orders (radio buttons for yes/no). Below the filters are 'Search' and 'Reset' buttons. The table below lists three invoices with columns for Invoice number, Issue date, Amount asked (tax not included), Amount asked (including tax), Term of payment, Carrying forward, Invoice (PDF link), and Credit Note.

	Invoice number	Issue date(making date)	Amount asked(tax not included)	Amount asked(including tax)	Term of payment	Carrying forward	Invoice	Credit Note
<input type="checkbox"/>	BM20120900051925	09/13/2012	GBP:5,000.00	GBP:5,000.00	10/12/2012		PDF	
<input type="checkbox"/>	BM20120900051924	09/13/2012	GBP:5,000.00	GBP:5,000.00	10/12/2012		PDF	
<input type="checkbox"/>	BM20120900051923	09/13/2012	GBP:5,000.00	GBP:5,000.00	10/12/2012		PDF	

List of available invoices, with option to download to PDF

Customers paying via deposit will still receive an auto-generated invoice for every certificate seven days after issuance. If you have already paid your deposit, the invoice is provided for information purposes only.

6.4

VIEW REQUESTS FOR PAYMENT (RFPs)

Click **View RFPs – Deposits to be Paid** under the **MY FINANCES** section of the left navigation menu to display any Requests for Payments (RFPs) that you have associated with your account. Please note, the status will **always** say “Payment expected by check or bank transfer” whether it has been paid or not. For your convenience, search parameters are included to make it easy to find specific RFPs.

The screenshot shows the 'Request for Payment' page with search filters and a table of RFPs. The search filters include: Order Date (e.g. 07/30/2007), Approval date (e.g. 07/30/2007), Status (dropdown menu set to 'All'), and Order Number. Below the filters are 'Search' and 'Reset' buttons. The table below lists two RFPs with columns for PDF, Order Number, Order Date, Approval date, Deposit amount, Status, and Delete.

PDF	Order Number	Order Date	Approval date	Deposit amount	Status	Delete
PDF	PA200911122079	11/11/2009(GMT+00:00)	11/11/2009(GMT+00:00)	€5,000.00	Payment expected by cheque or by bank transfer	Delete
PDF	PA201003295081	03/29/2010(GMT+00:00)	03/29/2010(GMT+00:00)	€10,000.00	Payment expected by cheque or by bank transfer	Delete

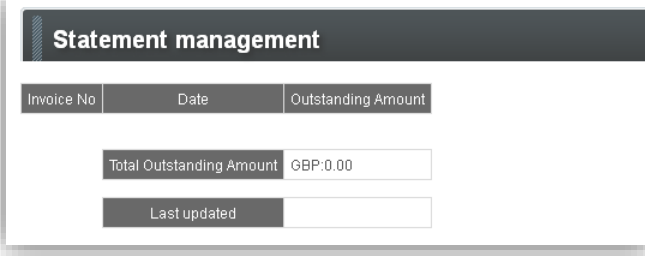
List of available RFPs, with option to download to PDF

Customers placing a deposit into their GCC account will receive a Payment Request for advance payment unless the deposit was paid by credit card at the point of ordering.

VIEW STATEMENTS – OUTSTANDING FUNDS

Click **View Statements** under the **My Finances** section of the left navigation menu to view a snapshot of how much money is outstanding within your account. This is the sum of all certificate values minus what you have paid GlobalSign.

6.5



Invoice No	Date	Outstanding Amount
Total Outstanding Amount		GBP:0.00
Last updated		

Snapshot of any outstanding funds in your account

ACCOUNT MANAGEMENT

6.6

These functions are available on the **ACCOUNT & FINANCE** tab of your GCC account.

6.6.1 AMEND COMPANY DETAILS

Click **Amend Company Details** under the **My Account** section of the left navigation menu to edit any of your company details, including name, address, contact details, VAT number, etc.

6.6.2 VIEW ALL RECEIVED EMAILS

Click the **Email History** widget on the **ACCOUNT & FINANCE** home screen view all GCC emails that have been sent in relation to **all orders** that have been placed within your account. You also have the ability to resend any of the emails if they have not been received or were caught in spam filters, etc.

6.7

USER MANAGEMENT

It is important to determine the structure and the permission levels you wish to create as an Account Administrator before you begin to create a delegated administration hierarchy within the GCC system, although it is possible to edit the permissions for users in the future. User management is accessed via the **Account & Finance** tab of your GCC account.



Account & Finance Home Screen

6.7.1 USER ROLES

You may add additional users to your MSSL account. Depending on their privileges, newly created Users may place new certificate orders, add deposit funds, or perform reporting. Users are defined in roles:

- **Account Administrator** – This type of user has full control over the account with ability to order any type of certificate, amend account/profile information and create new Managers and Staff in Charge. An administrator can also see any orders placed by other users within the system and can perform actions on them such as re-issue, cancel, revoke etc.
- **Manager** – Manager rights and abilities are similar to the Account Administrator. The Admin can restrict or permit Managers to add funds to the account bulk balance. Manager roles can only create additional Staff in Charge users.
- **Staff in Charge** – Users at this level have their administration rights (e.g. certificate application, approval, or revocation and adding funds to account bulk balance) defined by the Account Administrator or the Manager. Unlike Account Administrators and Managers, Staff in Charge cannot create additional users.

6.7.2 MANAGE USERS

Go to the **Account & Finance** tab then click **Manage Users** under the **My Account** section of the side menu to add or edit users of your account.

Manage Users													
Edit	User ID	Full name	Department name	Official position	Zip code	Address	TEL	FAX No.	Email address	Location(building name)	Surname	First name	User permissions
Edit	PAR05988_globalsign	Richard Hancock			ME14 2LP	KentMaidstoneSpringfield House	01622 766766		richard.hancock@globalsign.com	Sandling Road	Hancock	Richard	Administrator
Edit	PAR05988_global199	Test User			ME14 2LP	KentMaidstoneSpringfield House	12345		richard.hancock@globalsign.com	Sandling Road	User	Test	Staff in charge

[New registration](#)

Manage Users Screen

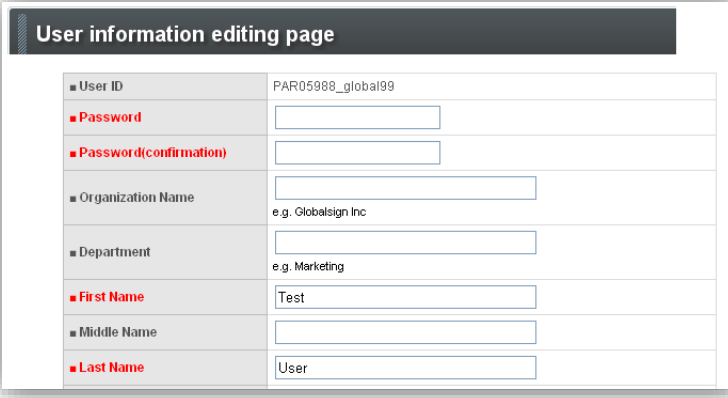
6.7.2.1 NEW USERS

Click **New Registration** on the **Manage Users** screen to add a new user to your account. You can assign users to any of three roles previously described (Administrator, Manager, Staff in Charge). You

can also designate whether the individual will have the ability to approve certificates or add funds to the account.

6.7.2.2 EDIT USERS

Click **Edit** next to the user you would like to modify. From here you can reset passwords, privilege levels, status and contact information.



User information editing page	
■ User ID	PAR05988_global99
■ Password	<input type="text"/>
■ Password(confirmation)	<input type="text"/>
■ Organization Name	<input type="text"/> e.g. Globesign Inc
■ Department	<input type="text"/> e.g. Marketing
■ First Name	<input type="text"/> Test
■ Middle Name	<input type="text"/>
■ Last Name	<input type="text"/> User

Modify User Information

6.7.2.3 CHANGE ADMINISTRATOR

Click **Change Administrator** under the **My Account** section to **promote** another user within the account to the administrator level. Please note: the user must already exist before you can make him/her an **Administrator**.

6.7.2.4 CHANGE BILLING MANAGER

There is only one **Billing Manager** per account. Click **Change Billing Manager** under the **My Finances** section to make another account user the dedicated billing contact. This ensures the correct person receives invoice notices.

6.8

TAB MANAGEMENT

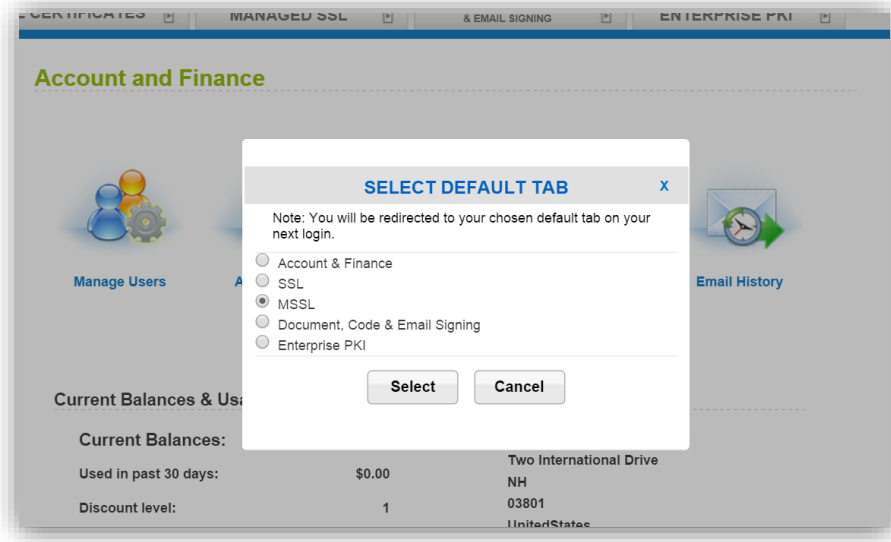
Within the GCC interface there are multiple tabs shown at the top for the management of all of GlobalSign's products you have. This provides one centralized location for all certificate management actions.

6.8.1 SETTING THE DEFAULT TAB

As a convenience, upon logging in for the first time, GCC allows you to set which of these tabs you would like to be the default tab that is shown as your initial starting point when accessing your account.

While on the **Account & Finance Tab**, on the left navigation menu under **My Account**, click **Default Tab Setting** to open the **Select Default Tab** dialog. Note, if it is your first time logging in to your GCC account the Select Default Tab dialog will appear automatically.

Using the radio buttons next to each option select your default tab. Click **Select**. Your default tab is now set and will appear after your next login to your GCC account.

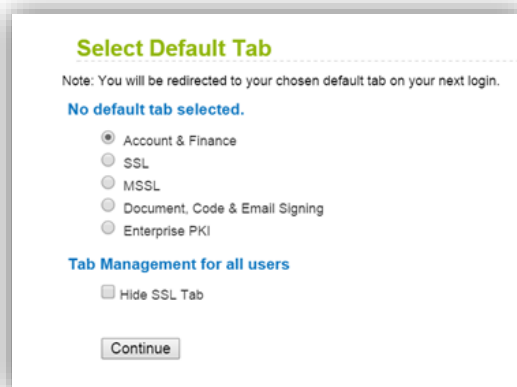


Select Default Tab (First GCC Login)

6.8.2 HIDING THE SSL TAB

Managed SSL allows you to benefit from the instant issuance of certificates from pre-vetted domains. Occasionally, orders are mistakenly placed through the **SSL CERTIFICATES** tab resulting in issuance delays due to the individual/ manual vetting process. To prevent users from accidentally ordering through the wrong Account tab, Account Administrators can hide the SSL Certificates tab for all users.

To hide the SSL tab for all users, log in as the Account Administrator and make sure the **ACCOUNT & FINANCE** tab is selected. On the left navigation menu under **My Account**, click **Default Tab Setting**. Check the box next to **Hide SSL Tab**. Click **Continue**. For this change to take full effect, each user must **logout of GCC and log back in**.



Hide SSL Tab Option

7 USEFUL FUNCTIONS

CSR CHECKER

This tool is available on the **Managed SSL** tab of your GCC account.

Click CSR Checker on the left menu to use the online tool to debug any CSR issues. If you try to place an order and the CSR is giving you problems, run it through this tool and it should highlight any syntactical errors you may have (e.g. C=UK instead of C=GB)

7.1

8 GLOBALSIGN CONTACT INFORMATION

GlobalSign Americas

Tel: 1-877-775-4562

www.globalsign.com

sales-us@globalsign.com

GlobalSign EU

Tel: +32 16 891900

www.globalsign.eu

sales@globalsign.com

GlobalSign UK

Tel: +44 1622 766766

www.globalsign.co.uk

sales@globalsign.com

GlobalSign FR

Tel: +33 9 75 18 32 00

www.globalsign.fr

ventes@globalsign.com

GlobalSign DE

Tel: +49 800 723 798 0

www.globalsign.de

verkauf@globalsign.com

GlobalSign NL

Tel: +31 85 8882424

www.globalsign.nl

verkoop@globalsign.com
