

GlobalSign Enterprise Solutions

SSL Managed Service Quick Start Guide version 4.6

Managing EV, OV and IntranetSSL Certificates Across Your Organization Effectively



Copyright © 2011-2015 GlobalSign, Inc. All rights reserved.

GlobalSign, the GlobalSign logo and OneClickSSL are trademarks and registered trademarks of GlobalSign, Inc. or its affiliates in the United States and other countries.

All other trademarks are the property of their respective owners.

TABLE OF CONTENTS

- TABLE OF CONTENTS 2
- 1 INTRODUCTION 4
 - 1.1 LOGGING IN 4
 - 1.2 MANAGED SSL PAGE REFERENCE 4
 - 1.3 GETTING HELP..... 5
- 2 ORDERING CERTIFICATES 7
 - 2.1 Summary of MSSL Products..... 7
 - 2.1.1 Extended SSL 7
 - 2.1.2 OrganizationSSL 7
 - 2.1.3 IntranetSSL 7
 - 2.1.4 MSSL Product Feature Comparison 7
 - 2.2 Ordering MSSL Certificates..... 8
 - 2.2.1 ADDING SANS DURING THE ORDERING PROCESS..... 13
 - 2.3 ORDERING INTRANETSSL 14
 - 2.4 USING THE PUBLIC ORDERING PAGE..... 18
 - 2.4.1 ACTIVATING THE PUBLIC ORDERING PAGE..... 18
 - 2.4.2 CONFIGURING THE PUBLIC ORDERING PAGE 19
 - 2.5 APPROVING ORDERS 20
- 3 CLIENT CERTIFICATE AUTHENTICATION 22
- 4 MANAGING &REPORTING ON CERTIFICATES AND ORDERS 27
 - 4.1 SEARCHING FORCERTIFICATES 27
 - 4.1.1 SEARCH RESULTS..... 27
 - 4.2 CERTIFICATE ACTIONS 28
 - 4.2.1 REISSUE AN SSL CERTIFICATE 28
 - 4.2.2 RENEW AN SSL CERTIFICATE 28
 - 4.2.3 REVOKE A CERTIFICATE 28
 - 4.2.4 DOWNLOAD CERTIFICATE FILE..... 29
 - 4.2.5 CANCEL A CERTIFICATE 29
 - 4.2.6 CHANGE USER ASSOCIATED WITH CERTIFICATE..... 29
 - 4.2.7 ADD/REMOVE SANS 29
 - 4.2.8 DELETE AUTOCSR PKCS 12 30

4.3	CERTIFICATE DETAILS.....	30
4.3.1	ORDER SUMMARY.....	30
4.3.2	FULL ORDER DETAILS	30
4.3.3	USER &CONTACT DETAILS.....	31
4.3.4	GCC EMAIL LOG.....	31
4.3.5	GCC AUDIT LOG.....	31
5	MANAGE DOMAINS & PROFILES.....	32
5.1	SET USER PERMISSIONS.....	32
5.2	ADD NEW DOMAIN.....	33
5.3	EDIT PROFILE.....	33
5.4	UPGRADE TO EV LEVEL VETTING	33
6	ACCOUNT AND FINANCE PAGE	35
6.1	PAYMENT OPTION –DEPOSITING FUNDS INTO ACCOUNT	35
6.1.1	ADD DEPOSIT.....	35
6.1.2	HOW TO PAY FOR YOUR DEPOSIT.....	35
6.1.3	DEPLETED DEPOSITS.....	36
6.2	VIEW/REQUEST INVOICES	36
6.3	VIEW REQUESTS FOR PAYMENT (RFPs).....	36
6.4	VIEW STATEMENTS – OUTSTANDING FUNDS.....	37
6.5	ACCOUNT MANAGEMENT	37
6.5.1	AMENDCOMPANY DETAILS.....	37
6.5.2	VIEW ALL RECEIVED EMAILS	37
6.6	USER MANAGEMENT.....	38
6.6.1	USER ROLES.....	38
6.6.2	MANAGE USERS	38
7	USEFUL FUNCTIONS	40
7.1	CSR CHECKER	40

1 INTRODUCTION

The GlobalSign Certificate Centre (GCC) is a highly flexible, web-based certificate lifecycle management portal. The GCC centralizes Certificate management, including all types of GlobalSign Digital Certificates and allowing for multiple users. Managed SSL (MSSL) is a solution available via GCC.

1.1 LOGGING IN

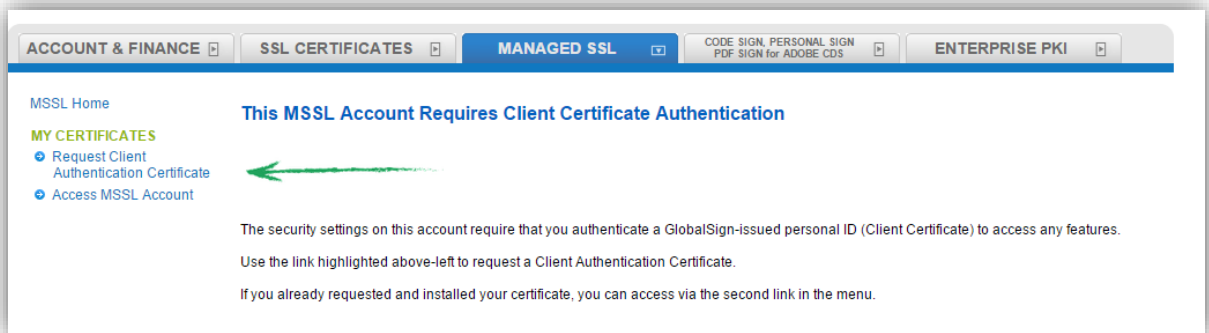
Once your Managed SSL Account has been approved, you can log into the GlobalSign Certificate Center (GCC) straight away to start managing the lifecycle of your SSL Certificates.

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 Authentications, then you will see a page similar to this when you log in. See section 3 for details.



If you have difficulties logging in or forget your password, please contact Support at www.globalsign.com/support.

You will only be able to order Certificates once the vetting of your organization and domain names has been completed. You can check your vetting status anytime by logging into your account.

1.2 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 on navigate and how to use the Managed SSL page. When ordering MSSL certificates please be sure you are in the **MANAGED SSL** tab.

Managed SSL - Home

MY CERTIFICATES

- Order Certificates
- Pending Approvals
- View Upcoming Renewals

FIND CERTIFICATES

- Search Order History

MY PROFILES

- Manage Domains and Profiles

TOOLS

- CSR Checker

RESOURCES

- MSSL Guide

My Domains and Profiles

Domain Name	Profile Name	Vetting Level
oliver.sslcerts.jp	globalsign	Organization SSL , Extended SSL
lina.sslcerts.com	globalsign	Organization SSL
sslcerts.jp	globalsign	Organization SSL , Extended SSL
tsg.sslcerts.jp	globalsign	Organization SSL
www.handshake-state1.com	globalsign	Organization SSL
ssl24.jp	globalsign	Organization SSL

References

1. **Account & Finance Tab** - This will redirect you to the Account & Finance Page where you can manage all your account information. See the section 5 for more information.
2. **Order Certificate** - You can order SSL certificates through the pre-vetted profiles here. See section 2 for more information.
3. **Pending Approvals** - You can view all the orders which are pending for approval. See section 2.5 for more information.
4. **Upcoming Renewals** - You can view here all certificates that are about to expire and are available for renewal. See section 4.2.2 for more information.
5. **Find Order** - You can search here all the SSL certificate orders made under your account and manage them. See section 4.1 for more information.
6. **Domains & Profiles** - This link will redirect you to the page where you can apply and manage all your profiles and domains. See section 5 for more information.
7. **CSR Checker** - This link will redirect you to the CSR checker page wherein GCC can parse and verify your CSR. See section 7.1 for more information.
8. **My Domains and Profiles** - List of profiles, domains and their vetting level. See section 5 for more information about this.

1.3 GETTING HELP

Every GlobalSign enterprise customer has a dedicated Account Manager who is on hand to help with any product and technical queries you may have about Managed SSL. GlobalSign also provides technical support through our Client Service departments around the world. www.globalsign.com/support

GlobalSign Americas

Tel: 1-877-775-4562

www.globalsign.comsales-us@globalsign.com**GlobalSign EU**

Tel: +32 16 891900

www.globalsign.eusales@globalsign.com**GlobalSign UK**

Tel: +44 1622 766766

www.globalsign.co.uksales@globalsign.com

GlobalSign FR

Tel: +33 1 82 88 01 24

www.globalsign.frventes@globalsign.com**GlobalSign DE**

Tel: +49 30 8878 9310

www.globalsign.deverkauf@globalsign.com**GlobalSign NL**

Tel: +31 20 8908021

www.globalsign.nlverkoop@globalsign.com

GlobalSign SG

Tel: +65 3158 0349

www.globalsign.sgsales-apac@globalsign.com**GlobalSign IN**

Tel: +91 11 41106000

www.globalsign.com/en-in/sales@globalsign.com

2 ORDERING CERTIFICATES

2.1 Summary of MSSL Products

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

2.1.1 Extended SSL

ExtendedSSL is the product name for GlobalSign's Extended Validation (EV) SSL offering and is issued in strict adherence 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 Organizational Vetted 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 a variety of SAN options 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: owa, autodiscover and mail
- Provide a CSR, or have GlobalSign generate the keys: You can enter a CSR or request that GlobalSign creates the keys and corresponding CSR on the fly (AutoCSR). Certificates requested using AutoCSR are returned in a packaged, encrypted PKCS#12 file containing both the Certificate file and private key.

2.1.3 IntranetSSL

The 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 as well as certificate validity period up to 5 years.

2.1.4 MSSL Product Feature Comparison

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

Function	ExtendedSSL	OrganizationSSL	IntranetSSL
Base Options			
• Wildcard	N	Y	Y
• Global IP	N	Y	Y
• Private (Internal Server name)	N	N	Y
Validity Period in request (years)	Up to 2	Up to 3	Up to 5
Maximum cert validity period (months)	27	39	60
Type of Order			
• New	Y	Y	Y
• Renewal	Y	Y	Y
• Transfer	Y	Y	N
Signing Algorithm (CA Hierarchy)			
• SHA-256	Y	Y	Y
• SHA-1	Y*	Y*	Y
• ECC P-256	N	N	Y
Unified Communications	Y	Y	N
SAN types			
• FQDN	Y	Y	Y
• SubDomain	Y	Y	Y
• Global IP Address	N	Y	Y
• Wildcard	N	Y	Y
• Internal SAN or Reserved IP address	N	N	Y
AutoCSR (RSA keys only, ECC is not supported)	N	Y	Y
CSR Key Types supported			
• RSA 2048-4096	Y	Y	Y
• ECC P-256	Y	Y	Y
• ECC P-384	Y	Y	Y
Site Seal	Y	Y	N

* SHA-1 options for EV and OV will end on December 14th 2015 due to Industry requirements. SHA-1 will continue to be an option for IntranetSSL since it is a non-public hierarchy and is exempt from Industry requirements.

2.2 Ordering MSSL Certificates

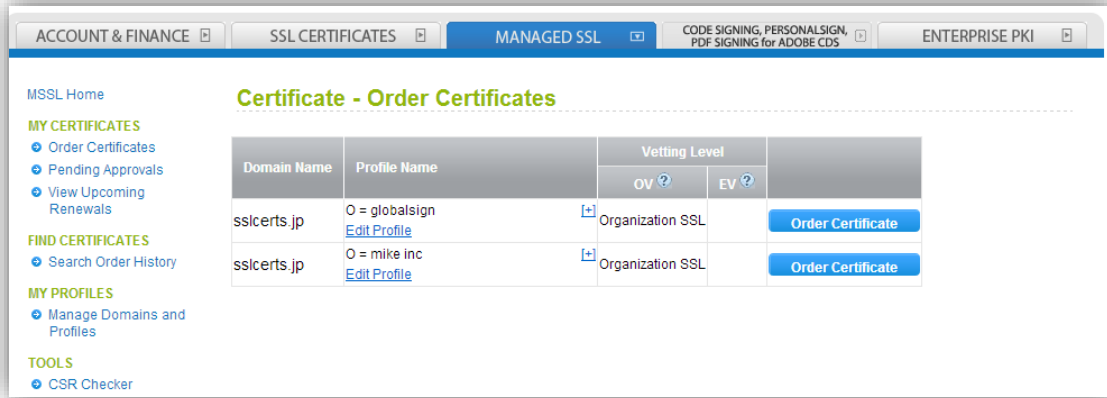
On the **Managed SSL** tab, click the **Order Certificate** widget.

The screenshot shows the 'Managed SSL - Home' interface. At the top, there are navigation tabs: 'ACCOUNT & FINANCE', 'SSL CERTIFICATES', 'MANAGED SSL' (highlighted with a red circle), 'CODE SIGNING, PERSONAL SIGN, PDF SIGNING for ADOBE CDS', and 'ENTERPRISE PKI'. Below the tabs, the page title is 'Managed SSL - Home'. On the left sidebar, there are sections for 'MY CERTIFICATES', 'FIND CERTIFICATES', 'MY PROFILES', and 'TOOLS'. The main content area features five widgets: 'Order Certificate' (circled in red), 'Pending Approvals', 'Upcoming Renewals', 'Find Order', and 'Domains & Profiles'. Below these widgets is a table titled 'My Domains and Profiles' with the following data:

Domain Name	Profile Name	Vetting Level
sslicerts.jp	globalsign	Organization SSL
sslicerts.jp	mike inc	Organization SSL

MSSL home screen

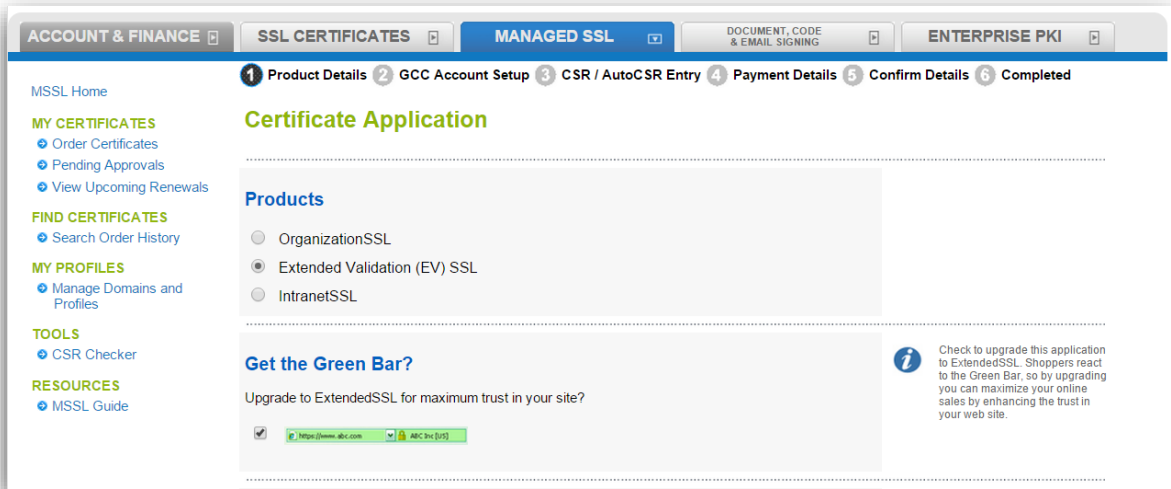
You will be presented with a list of domains vetted in your account along with the level of vetting that was applied to them (i.e., EV, OV and/or IntranetSSL).



Order Certificates screen

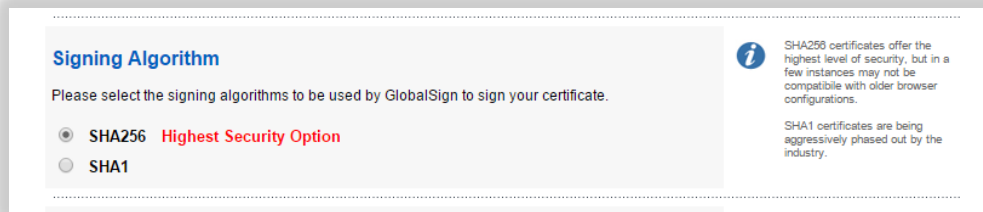
1. Click **Order Certificate** to begin the Certificate application process for one of your pre-vetted domains.

- The application workflow will display the product and options available based on that domain's vetting level.



Step 1 – select product details

- Specify the signing algorithm that will be used to sign the certificate. Using SHA-256 signing algorithm will give you the highest level of security. It will also have a maximum certificate validity of 3 years since SHA1 has a maximum of 1 year certificate validity and will be deprecated in December 2015. Browsers will display a warning “triangle” in their address bar for websites using SHA1 certificates in certain cases.



Note: you can ask GlobalSign support to set your account to issue SHA-256 certificates only and this will eliminate the SHA1 option on the above screen.

- 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. Ticking 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.

ACCOUNT & FINANCE | SSL CERTIFICATES | **MANAGED SSL** | CODE SIGNING, PERSONALSIGN, PDF SIGNING for ADOBE CDS | ENTERPRISE PKI

1 Product Details 2 **GCC Account Setup** 3 CSR / AutoCSR Entry 4 Payment Details 5 Confirm Details 6 Completed

Point of Contact for Certificate Delivery/Vetting Issues

Point of Contact #1

GCC Users: Lila Kee [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: * Lila

Last Name: * Kee

Telephone: * 5555555555

Email Address: * lila.kee@globalsign.com

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 2 – specify point of contact

- After specifying your certificate details, you will be prompted to enter the Certificate Signing Request (CSR). Follow the instruction on this link to generate your own Certificate Signing Request (CSR): <https://support.globalsign.com/customer/portal/articles/1229769>. If you do not have a CSR, you can use the AutoCSR delivery method and we will generate one for you. Many of the details needed for the AutoCSR will be pulled from the profile from which you're ordering. Fill in any remaining details and enter an alphanumeric password you will need when installing your Certificate.

Note: If you choose the AutoCSR delivery method, please make note of the AutoCSR password provided. You will need the full password to gain access to the PKCS#12 file we will send you.

Step 3 - CSR entry stage with AutoCSR option selected.

6. The next stage asks you to confirm the Secure Site Seal Information. This information will be displayed to anyone who clicks on the Site Seal displayed on your website.

Step 3 – confirm site seal details

7. Select the payment method you wish to use.
 - **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.
8. Finally, review the **Subscriber Agreement**, check the approval box, and you will be finished with the application process. Your Certificate will now be issued. 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.

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.

To add SANs to a certificate, select the **Add specific Subject Alternative Names (SANs)** option during the first step of the order process. You may add up to 100 SANs per certificate.

Add specific Subject Alternative Names (SANs)

Your Certificate will be issued to a specific Domain Name. When you buy a Certificate for `www.yourdomain.com`, we give you `yourdomain.com` as a free SAN. If you want to add further SANs and secure multiple sites, servers or IP addresses with a single Certificate, select Yes and enter the number of each SANs type you will add to the Certificate.

No Yes

Add multiple domain names
 Secure multiple Domain Names, they can be different to the Domain Names you will specify in the CSR / AutoCSR at \$0 each

Add multiple domain names with wildcard
 Secure all sub-domains on a single Fully Qualified Domain Name.
 e.g. a SAN in the certificate contains `*.ssl-globalsign.com` at \$0 each

Add multiple subdomains
 Secure subdomains of the Domain Name you will specify in the CSR / AutoCSR at \$0 each

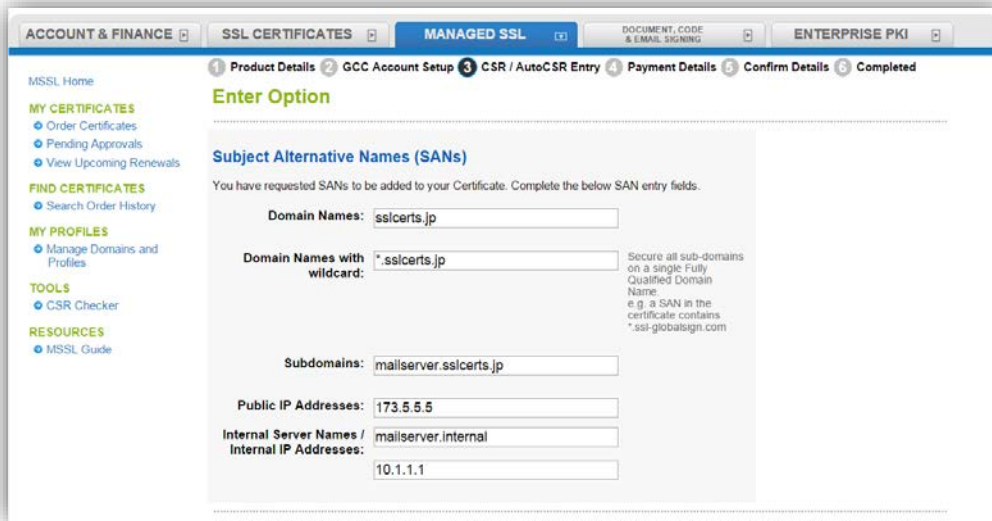
Add multiple public IP addresses
 Add Public IP Addresses (must be publicly accessible and owned by the applicant organization) at \$0 each

Add multiple internal server names or internal IP addresses
 Add Internal Addresses such as `10.1.1.1` or `localhost` at \$0 each

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.

SANs options and prices depend on the product and your account settings

Later in the ordering process you will be asked to specify the values for of the SANs you selected on the page above.



Example SANs entry fields for adding multiple SAN types

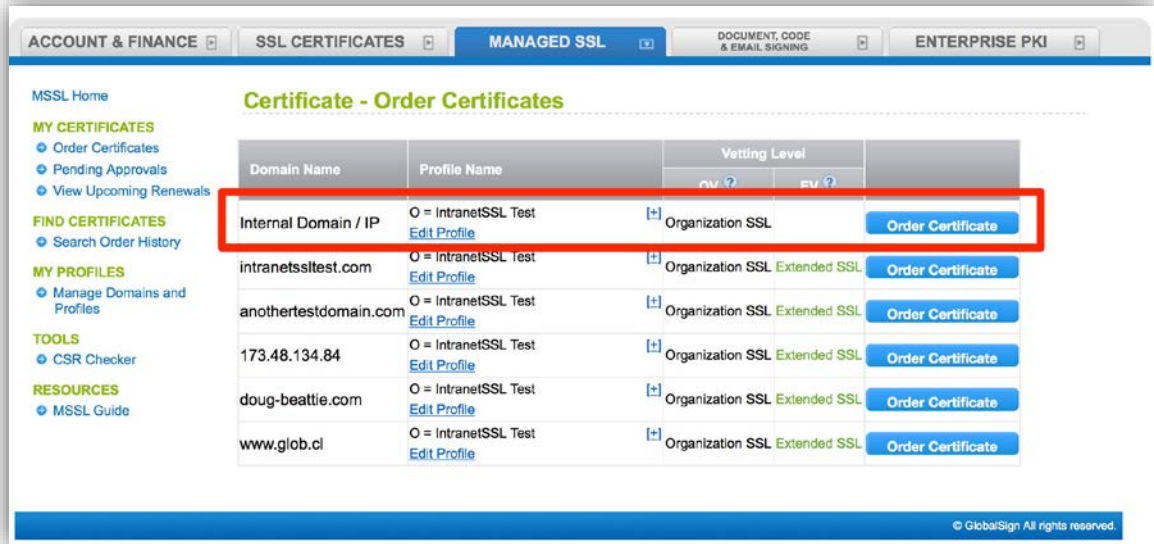
If you enter domains that are not pre-vetted, then you will receive an error message: **Domain or Profile is not valid or does not exist**. Please proceed to the **Manage Domains and Profiles** link under **My Profiles** to add a domain. Refer to section 5.2 for instructions on how to add domains.

2.3 ORDERING INTRANETSSL

1. On the **Managed SSL** tab, click the **Order Certificate** widget.



2. To order IntranetSSL Certificate with an internal server name or Reserved IP address in the CommonName, click on the **Order Certificate** button with the **Internal Domain / IP** domain name on the list. If you want an IntranetSSL with a FQDN in the CommonName, click the applicable **Order Certificate** button.



3. Specify the signing algorithm that will be used to sign the certificate. You can choose any of the following signing algorithm options: SHA1, SHA256 and ECC P-256.

Signing Algorithm

Please select the signing algorithms to be used by GlobalSign to sign your certificate.

- SHA256
- SHA1
- ECC P-256

i The selection of the Signing algorithm specifies the CA hierarchy and Root that will be used to sign this certificate. There are different Roots and Subordinate CAs for each of the signing algorithms.

4. Specify the validity period. You can choose up to 5 years certificate validity period, depending on your account configuration.

Validity Period

- half year \$0
- 1 year \$0
- 2 year \$0
- 3 year \$0
- 4 year \$0
- 5 year \$0

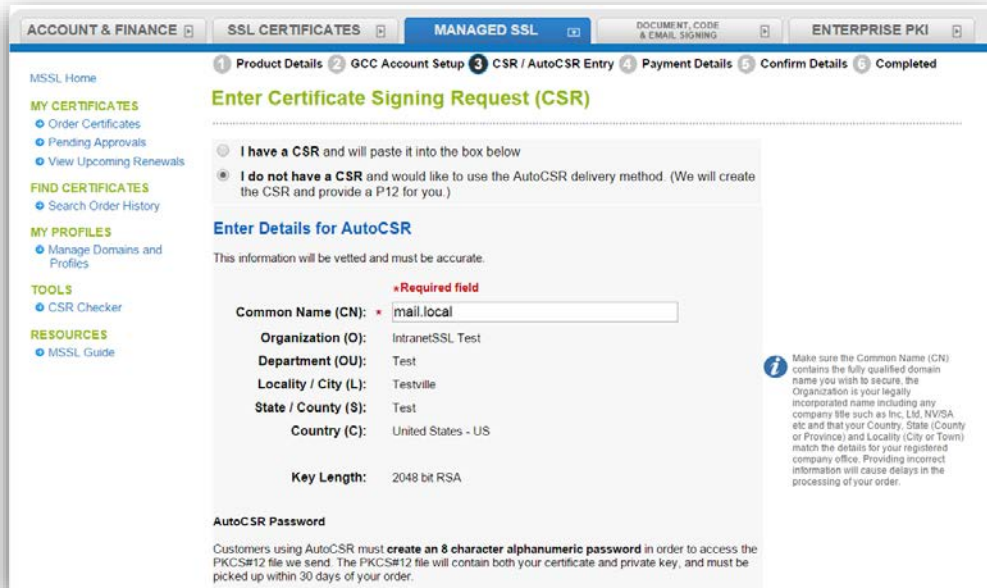
5. Specify the point of contact for certificate delivery or vetting issues. Note: you can Auto Fill these fields with the contact information for an existing GCC user. Ticking the **Is this the Point of Contact for communications** check box will enable GCC to send email notifications on the email address specified on the **Email Address** field.

The screenshot shows a web browser window with the GlobalSign Managed SSL portal. The navigation bar includes 'ACCOUNT & FINANCE', 'SSL CERTIFICATES', 'MANAGED SSL', 'CODE SIGNING, PERSONAL SIGN, PDF SIGNING for ADOBE CDS', and 'ENTERPRISE PKI'. The breadcrumb trail is: 1 Product Details, 2 GCC Account Setup, 3 CSR / AutoCSR Entry, 4 Payment Details, 5 Confirm Details, 6 Completed. The page title is 'Point of Contact for Certificate Delivery/Vetting Issues'. The form includes a 'GCC Users:' dropdown menu with 'Lila Kee' selected and an 'Auto Fill' button. Below this is a text box explaining the role of the point of contact. The form fields are: First Name (Lila), Last Name (Kee), Telephone (5555555555), Email Address (lila.kee@globalsign.com), Organization Name, and Department. There are checkboxes for 'Is this the Point of Contact for communications?' and a note about marking the contact as the point of communications for GlobalSign.

6. After specifying your certificate details, you will be prompted to enter the Certificate Signing Request (CSR). Follow the instruction on this link to generate your own Certificate Signing Request (CSR): <https://support.globalsign.com/customer/portal/articles/1229769>. If you do not have a CSR, you can use the AutoCSR delivery method and we will generate one for you. Many of the details needed for the AutoCSR will be pulled from the profile from which you're ordering. Fill in any remaining details and enter an alphanumeric password you will need when installing your Certificate.

If you initiated your order using the **Order Certificate** button next to **Internal Domain / IP**, then you must enter an internal server name or Reserved IP address into the CN. If you selected the **Order Certificate** button next to a domain, you must enter a CN that ends in this domain, as is the case when ordering ExtendedSSL and OrganizationSSL certificates.

Note: If you choose the AutoCSR delivery method, please make note of the AutoCSR password provided. You will need the full password to gain access to the PKCS#12 file we will send you.



7. Select the payment method you wish to use.
 - **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.

8. Finally, review the **Subscriber Agreement**, check the approval box, and you will be finished with the application process. Your Certificate will now be issued. 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.

2.4 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 anybody within your organization 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 ensure organizations issue Certificates only to legitimate applicants.

2.4.1 ACTIVATING THE PUBLIC ORDERING PAGE

To activate the POP for a pre-vetted domain, click the **Domains & Profiles** button in the bottom right of the Managed SSL home screen or select **Manage Domains & Profiles** under the **My Profiles** section of the left navigation menu. This will bring you to a screen that lists your domains and Certificate profiles.

Certificate Profile	Domain	Status	Actions	Status	Vetting Level		Profile Actions
					OV	EV	
O = globalsign OU = Tech	mike99.sslcerts.jp	Invalid					
S = Oosaka	mike98.sslcerts.jp	Invalid		Available	OV		Add New Domain Edit Profile
L = Nishinari-ku C = Japan - JP	sslcerts.jp	Available	remove set user permissions				Upgrade to EV Vetting Level Edit Public Order Page
O = mike inc OU = sales	sslcerts.jp	Available	remove set user permissions	Available	OV		Add New Domain Edit Profile
S = kanagawa L = kamakura C = Japan - JP							Upgrade to EV Vetting Level Activate Public Order Page

Manage Domains & Certificate Profiles screen

Find the Certificate Profile for which you would like to create a POP and select **Activate Public Order Page** in the rightmost column, **Profile Actions**. When the **Public Ordering Page** screen appears, check the box for **Activate Public Order Page** 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.

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

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

Similarly, you can deactivate the **Public Order Page** by navigating to the **Managed Domains & Profiles** page and selecting **Edit Public Order Page** in the rightmost column, **Profile Actions**. From there, simply uncheck the box next to **Activate Public Ordering Page** and click **Submit**.

2.4.2 CONFIGURING THE PUBLIC ORDERING PAGE

Selecting **Activate Public Order Page** 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.

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 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 <small>Allows applicant to trade-in competitor's Certificate- trade-ins get further benefits. Leave unchecked to set all applications to New Order only.</small>
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 Elicit Strategy <input type="radio"/> Fixed Payment Method <input checked="" type="radio"/> Specify When Ordering <input type="checkbox"/> Allow entry of Credit Cards for immediate charge

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 some flexibility or if you do not know the exact details at the time of configuration.
 - **Single Domain Certificate** – is issued to www.domain.com (and will contain domain.com in the SAN field) and can only be used on that FQDN.
 - **Wildcard SSL Certificate** – is issued to *.domain.com and can secure all sub-domains of domain.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 = 3 years, EV = 2 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** – To enhance security, you can choose to require a passphrase with an application request so an applicant will have to input the code before proceeding with an application. If you choose this option, please ensure that you communicate the passphrase to your POP recipient outside of the GlobalSign system. We do not recommend plain text e-mail 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 funds you have in your account, or allow the POP applicant to choose at the point of order. 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.

POP Configuration Options

Check with items to display on your Public Ordering Page

General Options Custom Fields

Custom Field	Field Title:	Required
	Employee Number	<input checked="" type="checkbox"/>

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 navigating to **Manage Domains & Profiles** from the **Managed SSL** menu to the left of your screen and clicking **Edit Public Order Page**.

2.5 APPROVING ORDERS

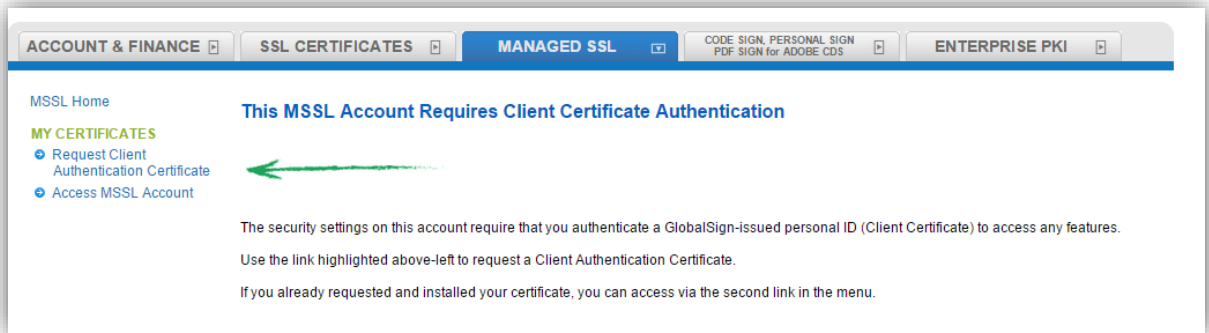
Applications made by Users **without** approval privileges or applications made using the **Public Ordering Page** must be approved by a User **with** approval privileges. When such applications are made, an email alert will be sent to the Account Administrator and the certificate will not be issued until the Administrator has approved the application.

Administrators and Users with approval rights can access their lists of pending orders by selecting **Pending Approvals** from the **My Certificates** section of the left navigation menu. Each order will have a checkbox next to it. Select the orders you would like to modify and click **Approve** or **Reject** depending on the required action.

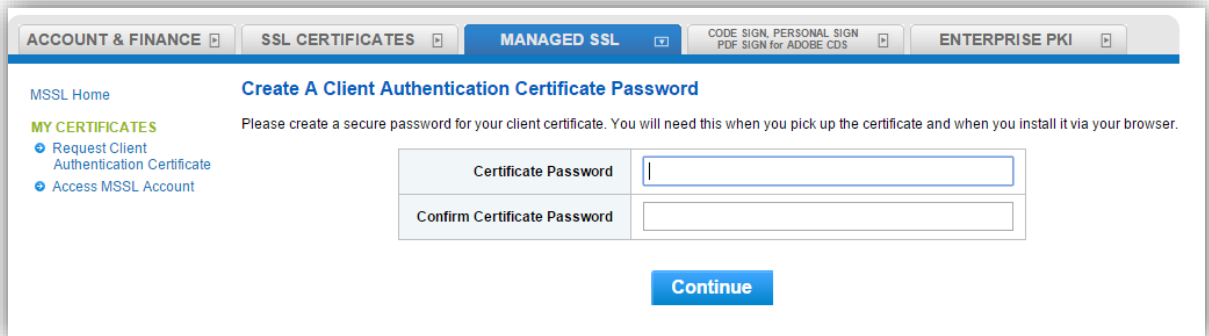
3 CLIENT CERTIFICATE AUTHENTICATION

You may request to have your GCC account upgraded to be Client Certificate Authentication enabled. If your account is enabled for client authentication you will not have access to the MSSL tab until you request and receive a client certificate.

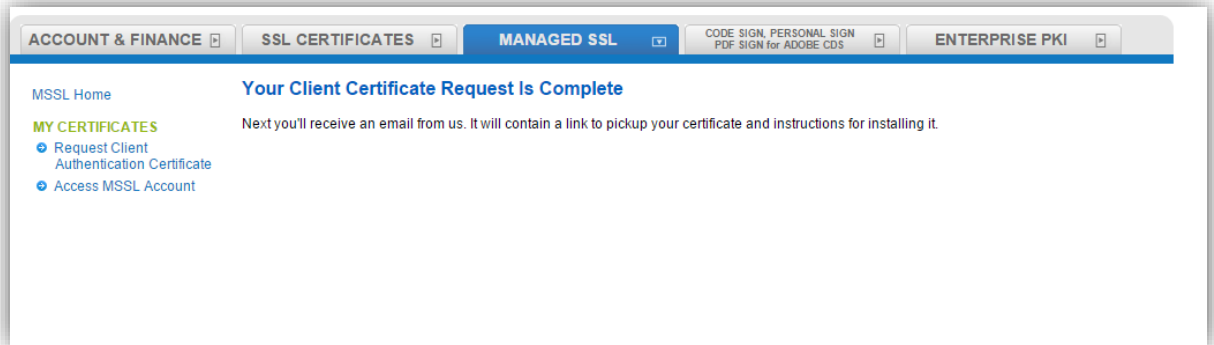
Once logged into your account, click on the **MSSL** tab. Click on the **Client Certificate Authentication** link located on the left side of the page.



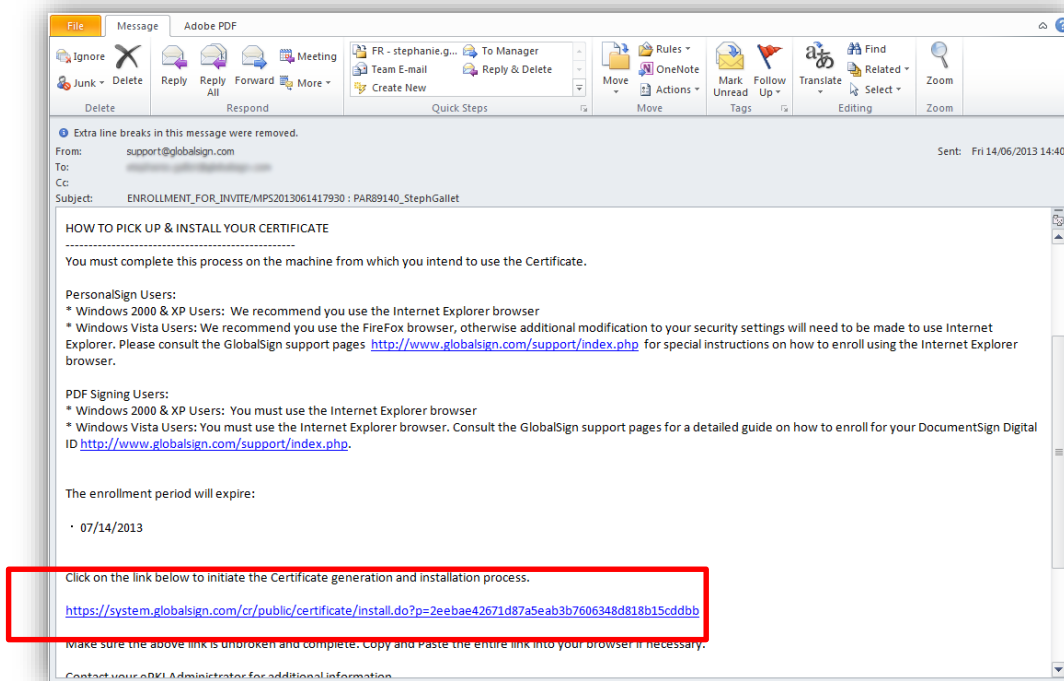
You will be asked to enter a secure password for the Client certificate and it will be used to pick up the Client Certificate later on.



Once you have entered the acceptable password for the client certificate, you will receive a confirmation message that you have completed the Client Certificate request and you will receive an email with a link for picking up the Client Certificate.



Click on the Certificate pick-up URL in the email sent to you in order to start installing your certificate.



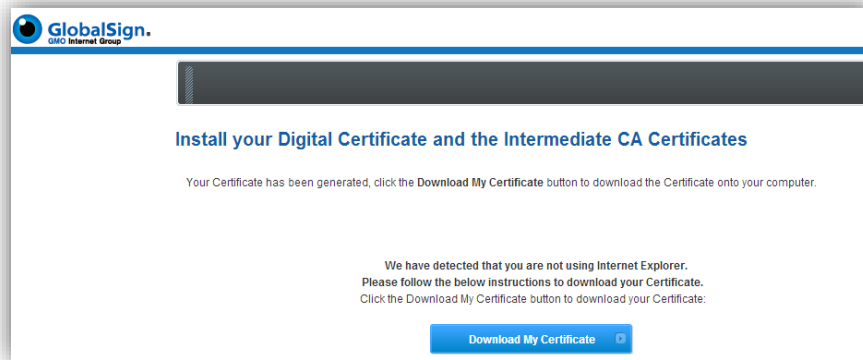
A pop-up window will appear, asking you to enter your **Pick-up Password**. Then click **Next**.

The screenshot shows the GlobalSign web interface. At the top left is the GlobalSign logo with the tagline "GMO Internet Group". Below the logo is a dark grey progress bar. The main content area contains the text: "You will now go through the Certificate generation and installation process." followed by the heading "Enter your Temporary Certificate Pick-up Password". Below the heading is a text input field with the placeholder text "Enter the Pickup Password to continue.". Underneath the input field is a link: "Forgotten the Pickup Password? [Contact Support](#) immediately for assistance.". At the bottom center is a blue button labeled "Next".

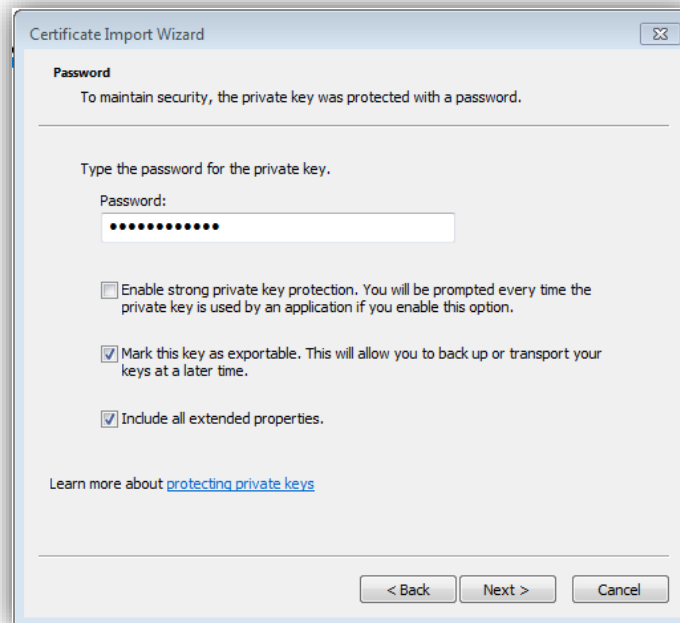
You will be requested to create a new password that we will refer to as **the Private Key password**. Next you will need to agree to the Subscriber Agreement and then click the **Next** button.

The screenshot shows the GlobalSign web interface. At the top left is the GlobalSign logo with the tagline "GMO Internet Group". Below the logo is a dark grey progress bar. The main content area contains two password input fields. The first field is labeled "Certificate Password Required" and has a note below it: "Password must be a minimum of 12 characters. Alpha-numeric values only (A-Z, 0-9)". The second field is labeled "Certificate Password (re-enter) Required". Below the password fields is the heading "ePKI Subscriber Agreement". Underneath is a scrollable text area containing the text: "GlobalSign Subscriber Agreement - Digital Certificates and Services - Version 2.5" followed by "PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE DIGITAL CERTIFICATE ISSUED TO YOU OR YOUR ORGANIZATION. BY APPLYING FOR A DIGITAL CERTIFICATE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY CANCEL THE ORDER WITHIN 7 DAYS OF THE APPLICATION FOR A FULL REFUND. IF YOU HAVE PROBLEMS UNDERSTANDING THIS". Below the text area is a checkbox labeled "I AGREE TO THE SUBSCRIBER AGREEMENT". At the bottom center is a grey button labeled "Next".

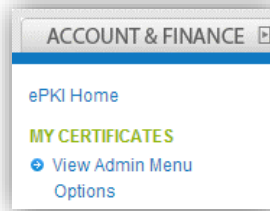
Click on the **Download My Certificate** button to download the Client Certificate.



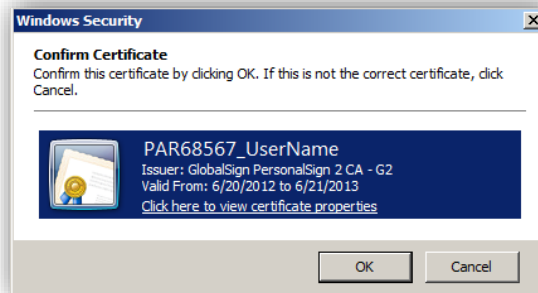
The Certificate Import Wizard will start when you open the .pfx document. Simply follow the steps by clicking **Next** button. On the second step, you will have to enter the **Private Key password** you created earlier and you will also be given the choice to select whether or not you wish the key to be exportable.



At the end of the process, a message will confirm that it was successful. You can then go back to your account, click **View Admin Menu Options** in the **My Certificates** menu.



You will be prompted to choose the Client Certificate that you just installed. You can verify the correct certificate as its common name will be your account login.



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



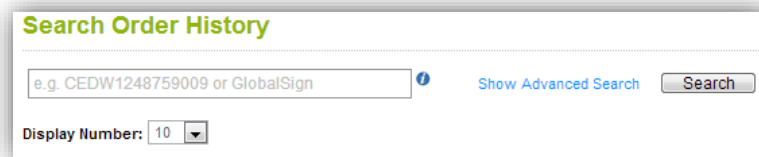
Note: Client certificates issued to EPKI administrators can also be used for the MSSL client certificate authentication.

4 MANAGING & REPORTING ON CERTIFICATES AND ORDERS

Order information is accessed via the **Managed SSL** tab of your GCC account.

4.1 SEARCHING FOR CERTIFICATES

Click the **Find Order** widget of the Managed SSL home screen or **Search Order History** under the **Find Certificates** section of the left navigation menu. This brings you to your reporting interface to access orders and certificates. The default basic search allows you to search by order number or common name.



The screenshot shows the 'Search Order History' interface. It features a search input field with the placeholder text 'e.g. CEDW1248759009 or GlobalSign'. To the right of the input field is a blue information icon and a 'Show Advanced Search' link. A 'Search' button is located to the right of the 'Show Advanced Search' link. Below the search input field is a 'Display Number' dropdown menu set to '10'.

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.



The screenshot shows the 'Search Order History' interface with advanced search options. It features a search input field with the placeholder text 'e.g. CEDW1248759009 or GlobalSign'. To the right of the input field is a blue information icon and a 'Hide Advanced Search' link. Below the search input field are several search criteria: 'Application Date is' with a dropdown arrow, 'between' with a dropdown arrow, 'i.e. mm/dd/yyyy' with a calendar icon, 'and', 'i.e. mm/dd/yyyy' with a calendar icon, 'Any User' with a dropdown arrow, 'Any Status' with a dropdown arrow, and 'Any Product' with a dropdown arrow. At the bottom left is a checkbox labeled 'Include SSL'. A 'Search' button is located at the bottom right.

Advanced Search Options

The **Include SSL** option in the advanced search allows you to search for all managed and non-managed SSL Certificates associated with your account. On occasion Managed SSL users may place an order through the **SSL Certificates** tab rather than the **Managed SSL** tab. Checking the **Include SSL** option will allow you to see any non-managed certificates that may have been ordered in the past so you know to renew them under the managed tab in the future.

4.1.1 SEARCH RESULTS


Clicking **Search** after defining your search parameters brings up a results page that displays summary information about your orders that fit the defined criteria. When the list of certificates appears, you will notice several **quick action** icons next to each order (e.g., revoke, reissue, Get Cert). If the certificate is within the renewal period, a renew option will also appear. See the **Certificate Actions** section below for details about certificate activity.

If you checked the option to include non-managed SSL Certificates in your search results, they will be highlighted in green.

4.2 CERTIFICATE ACTIONS

4.2.1 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 **Search Order History** 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  **Reissue**.

Please note that although you can elect 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.

4.2.2 RENEW AN SSL CERTIFICATE

You can find a list of certificates within the renewal range, ninety days before expiration, with the **Upcoming Renewals** widget in the Managed SSL home screen or by clicking **View Upcoming Renewals** in the **My Certificates** side menu. Simply click the **Renew** button that appears next to the certificate.

You can also renew certificates using the search function.


1. Click **Search Order History** 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  **Renew**. 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 associated with the order 90 days prior to the expiration of the certificate. See the **User & Contact Details** section below to for information on modifying contacts.

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


4.2.3 REVOKE A CERTIFICATE

If your server and / or private keys have been compromised then you will want to revoke the certificate. This will cause any visitors to the associated website to receive a pop up warning of the certificate status and instructing them not to trust the site. This will add the certificate serial number to the GlobalSign CRL and OCSP servers, which are then propagated across the Internet.

1. Click **Search Order History** 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  **Revoke**.

4.2.4 DOWNLOAD CERTIFICATE FILE

If your order was an AutoCSR, then this will download the .p12 file (containing the private key + certificate). If you used a standard CSR during application, this will download the intermediates + end entity certificate.

1. Click **Search Order History** and use the search function to find the certificate for which you need to download the file.
2. Once the certificate appears in the search results, click the **Get Cert** button .

4.2.5 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 **Search Order History** and use the search function to find the certificate you need to cancel.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. Make sure you are on the **Order Summary** tab and click **Cancel** under the **Certificate Actions** menu in the right column.

4.2.6 CHANGE USER ASSOCIATED WITH CERTIFICATE

This assignment dictates who will receive renewal notices associated with the certificate. Whoever 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 **Search Order History** and use the search function to find the certificate you need to modify.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. Make sure you are on the **Order Summary** tab and click **Change User** under the **Certificate Actions** menu in the right column.

4.2.7 ADD/REMOVE SANS

This option will enable you to change the Subject Alternative Names configuration of your certificate. SANs allow the addition of other domain name, subdomains, or hostnames into a single SSL Certificate. The type of SAN option available here is dependent on the certificate type.

1. Click **Search Order History** and use the search function to find the certificate you need to modify.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. Make sure you are on the **Order Summary** tab, and click **Add/Remove SANs** under the

Certificate Actions menu in the right column.

4.2.8 DELETE AUTOCSR PKCS 12

This option allows you to delete the .p12 file for this Certificate from our servers. Please ensure that you have a backup of it before performing this action as it cannot be undone.

1. Click **Search Order History** and use the search function to find the desired certificate.
2. Once the certificate appears in the search results, click the **Edit** button to bring up the **Order Details** screen.
3. Make sure you are on the **Order Summary** tab, and click **Delete AutoCSR PKCS 12** under the **Certificate Actions** menu in the right column.

Please Note: Keys will automatically be deleted in 30 days.

4.3 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.

Order Details for CEPO1108249494	
Order Summary Full Order Details User & Contact Details GCC Email Log GCC Audit Log	
Common Name:	globalsign.com
Issued To:	GMO GlobalSign Ltd
Status:	Certificate Issued
Product:	OrganizationSSL(MSSL AutoCSR)
Price:	GBP 1,512,001.20
Issued on:	08/24/2011 13:12(GMT+00:00)
Expires on:	08/24/2013 13:11(GMT+00:00)
Order Contact:	Richard Hancock
Send Renewal Reminder Emails:	<input checked="" type="checkbox"/>
Optional Notes:	
Update	

Certificate Actions:

- [Reissue](#)
- [Revoke](#)
- [Cancel](#)
- [Cancel & Replace Order](#)
- [Change User](#)
- [Add/Remove SANs](#)
- [Delete AutoCSR \(PKCS#12\)](#)

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

4.3.1 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. Key actions relating to the certificate lifecycle are performed from this screen. For more information on these actions please see **Certificate Actions** above.

4.3.2 FULL ORDER DETAILS

The **Full Order Details** tab provides all information relating to a particular order, such as download status of the .p12 file, the second half of the .p12 password, and any SAN options. You can also

copy and paste the CSR and issued Certificate from this screen, should the need arise.

4.3.3 USER & CONTACT DETAILS

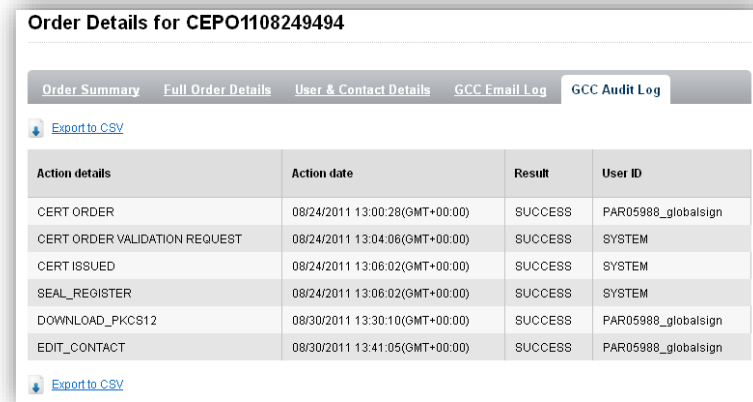
This screen allows you to view and edit the user with whom this order is associated. Please note that any changes made here **will not** be domain-wide and only apply to this particular order. Click **Update** to save any changes.

4.3.4 GCC EMAIL LOG

From here you will see all the 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).

4.3.5 GCC AUDIT LOG

Here are all the actions associated with this 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 eased management of certificates for all domains owned by one account. Accounts can be comprised of one **single organization** or an **umbrella entity** (MSSL Pro only), containing multiple companies, branches, and departments. These subdivisions are collectively known as **profiles** and contain their own set of domains. Each subsidiary can have its own profile DN data and related domains with appropriate users within the subsidiary only ordering for their own company, while still centralizing management and billing for the parent account.

In order to upgrade your MSSL account to Pro, where you can have multiple profiles with separate DN information, please contact your Account Manager. Please note, **only** MSSL Pro customers are able to have more than one profile within their account.

Click **Manage Domain & Profiles** under the **My Profiles** section in the left navigation menu to access domain management. Here you'll find a snapshot of your domains and several management functions.

Manage Domains & Certificate Profiles

Add or remove domains associated with your vetted profiles. Set User Permissions for granular control of which users have access to ordering for each domain.

Certificate Profile	Domain	Status	Actions	Status	Vetting Level		Profile Actions
					OV	EV	
O = GMO GlobalSign Ltd S = Kent L = Maidstone C = United Kingdom - GB	globalsign.com	Available	remove set user permissions				Add New Domain Edit Profile Upgrade to EV/Vetting Level Activate Public Order Page
	globalsign.co.uk	Available	remove set user permissions	Available	OV		
	globalsign.net	Available	remove set user permissions				

Snapshot of domains and management options

5.1 SET USER PERMISSIONS

Click **Set User Permissions** in the **Actions** column next to the domain you would like to modify. This will 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 what rights each user 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

5.2 ADD NEW DOMAIN

Click **Add New Domain** in the **Profile Actions** column to add another domain to a profile. For **Pro Accounts**, please be careful that you are in the correct profile when using this as the certificates for the new domain will be issued with the DN of the profile you select.

Add New Domain

Please enter a TLD (Top Level Domain) to be associated with the profile listed below. A vetting process to verify ownership of the domain by the relevant entity will begin after finishing the application.

Certificate Profile

- O = Marchi Inc
- S = NH
- L = Portsmouth
- C = United States - US

Do not include the www or other subdomains - Managed SSL operates by validating your top level domain. By entering a TLD such as [domain.com](#) you will be able to purchase [www.domain.com](#) or [secure.domain.com](#) from your account without the need for additional validation steps.

Domain Name

Submit **Cancel**

Add new domain to existing Certificate profile.

Our Vetting Team will be alerted when a new domain has been added to your profile. You can monitor the status of your new domain request from the **Manage Domains & Certificate Profiles page**. After your ownership of this domain has been verified by the team, you will receive an email alert and will be able to issue Certificates to that domain.

5.3 EDIT PROFILE

Click **Edit Profile** in the **Profile Actions** column to amend details contained within your profile. Please note: if your profile is active this action will **suspend** the account until our Vetting Department have verified the new information and re-activated it. Changes are not retrospective.

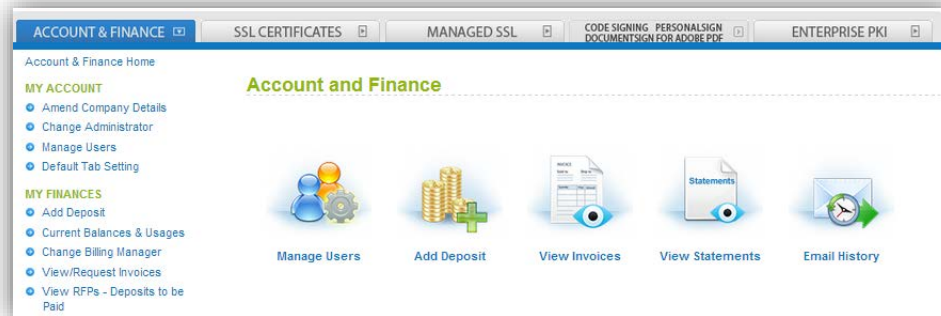
5.4 UPGRADE TO EV LEVEL VETTING

Click **Upgrade to EV Vetting Level** in the **Profile Actions** column to upgrade a profile vetted to the Organization Validated (OV) level 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 us to efficiently vet the account. Please have details, such as company number, appropriately 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 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.

To help speed up the process, please make sure that we are able to independently verify the data you submit. For example, you should enter the full legal name of your company (e.g., “My Company & Sons, Inc.” instead of “My Company”). Contact your Account Manager for assistance.

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

6.1 PAYMENT OPTION –DEPOSITING FUNDS INTO ACCOUNT

Using the account funds option gives you a discount. To be able to pay for certificates using deposited funds, you must first deposit funds into your account by clicking **Add Deposit** in the **My Finances** section of the menu on the left side of your screen.

6.1.1 ADD DEPOSIT

If you simply want to add a set amount of funds to your account, not based on a specific order, you can choose to add a deposit at any time. Click **Add Deposit** under the **My Finances** section of the left navigation menu to input the exact amount of money that you wish to add to your account. Once you have specified the amount, 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 checked="" 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

6.1.2 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.

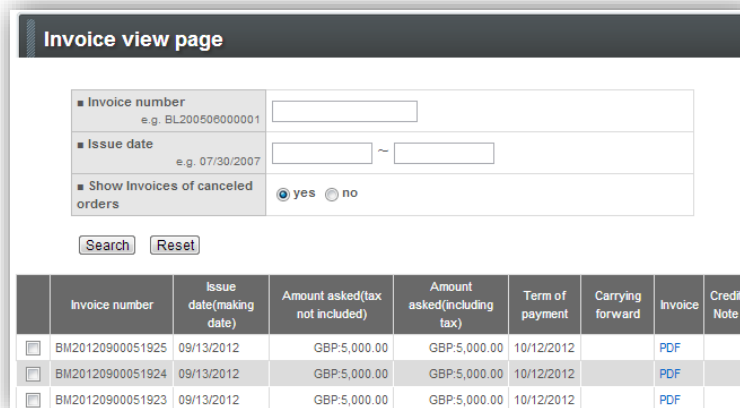
When buying certificates using the funds you have deposited, be sure to select **Deposit** as the **Payment Option** at the payment point in the purchasing process.

6.1.3 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. If you buy using Pay As You Go, you can pay by credit card for individual certificates as the certificate is issued. Please note that your pricing will be reset to standard Pay As You Go levels; therefore in order to maintain current discount levels, you should always add an additional deposit.

6.2 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 in association with your account. **Invoices will appear here 8 days after the issuance of the Certificate.** You can search by invoice number and date to quickly find a given invoice.



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' and '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, 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 automatically generated invoice for every certificate seven days after delivery date. If you have already paid your deposit, the invoice is provided for information purposes only.

6.3 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.

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	PA201003295061	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.

6.4 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.

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

Snapshot of any outstanding funds in your account

6.5 ACCOUNT MANAGEMENT

These functions are available on the **Account & Finance** tab of your GCC account.

6.5.1 AMENDCOMPANY 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.

6.5.2 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.

6.6 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

6.6.1 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** – Managers’ administration rights and abilities are determined by the Account Administrator. Certificate rights, such as application, approval, and revocation, as well as account rights, such as adding funds to the account bulk balance and creating Staff in Charge users, can be assigned on an individual basis. In the event of more than one manager per account, they cannot see each other’s orders. In the event of manager one, for example, being out of the office and a certificate ordered by him needing to be re-issued, only the administrator could perform that task as other managers would not have access to that order.
- **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.

6.6.2 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	01822 768766		richard.hancock@globalsign.com	Sandling Road	Hancock	Richard	Administrator
Edit	PAR05988_global99	Test User			ME14 2LP	KentMaidstoneSpringfield House	12345		richard.hancock@globalsign.com	Sandling Road	User	Test	Staff in charge

[New registration](#)

Manage Users screen

6.6.2.1 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.

6.6.2.2 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. Globalsign Inc
■ Department	<input type="text"/> e.g. Marketing
■ First Name	Test
■ Middle Name	<input type="text"/>
■ Last Name	User

Modify user information

6.6.2.3 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**.

6.6.2.4 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.

7 USEFUL FUNCTIONS

7.1 CSR CHECKER

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

Click CSR Checker under the **Tools** section of the left navigation 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).