

GlobalSign Enterprise Solutions

Google Apps Authentication User Guide

Using EPKI for 'Google Apps for Business' Single Sign-on and Secure Document Sharing



Table of Contents

Table of Contents	2
Introduction	3
Solution Requirements	3
Step 1 – Authentication Server Setup	3
Step 2 – Apache CSR Generation	4
Step 3 – Obtaining a Certificate	5
Step 4 – Installation of the Certificate to the Server	10
Step 5 – Apache SSL Settings	10
Step 6 – Creating a Key Pair for Google Apps	10
Step 7 – Google Apps Settings	10
Step 8 – LDAP Settings (Via LDIF)	12
Step 9 – Accessing Google Apps for Business	14
Appendix A – Password Synchronization – Advanced Design	15
GlobalSign Contact Information	19

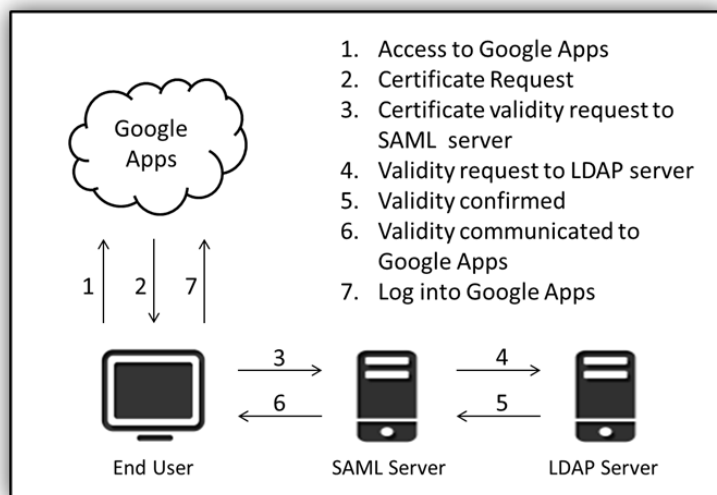
Introduction

As more and more organizations experience the business benefits of cloud-based applications, such as Google Apps, organizations should consider implementing strong two-factor authentication for users accessing sensitive data stored outside the trusted network. Google Apps for Business by default allows users to login via username/password. This can be a security issue for companies where users' passwords can be attacked. Google offers alternative methods for accessing their services to enhance security as well as improving the user experience. Here we will explain setting up and using the SAML Single Sign-on (SSO) Service for Google Apps web based applications.

Security Assertion Mark-up Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content.

Google Apps SSO service is based on SAML v2; there are a number of clients available for communicating with Google using this specification. Here we will focus on using the GHeimdall open source solution together with an LDAP server for providing access rights. GHeimdall enables you to authenticate Google Apps users by your own authenticate back end.

Overview of the Setup for Google SSO Login



Solution Requirements

The following components will be required for this solution:

- Google Apps for Business Account
- LDAP Directory Server (e.g. Apache Directory Server)
- SAML Authentication Server
 - GHeimdall2-repos
 - Gdata (Google Apps Provisioning API)
 - GHeimdall2 (<http://code.google.com/p/gheimdall2/>)
 - Apache
 - Python

Step 1 – Authentication Server Setup

To configure the Authentication Server you will need to adjust your LDAP directory server settings as well as adjust the GHeimdall configuration file and Apache configuration file.

LDAP Directory Server Settings

Define the settings for the directory server within the SAML authentication system as well as the filter to apply for user authentication.

LDAP URI	ldap://localhost/
----------	-------------------

LDAP basedn	dc=globalsign,dc=com
LDAP filter	(mail=%s@orgname.*)

GHeimdall Location and Configuration File

After installing GHeimdall, the configuration tree will be as follows:

Location	Description
/etc/gheimdall2/	Authentication key pair location
/etc/gheimdall2/gheimdall2.conf	GHeimdall Config File

GHeimdall2 Preferences (gheimdall2.conf):

Parameters	Value	Remarks
apps_domain	orgname.com	Google Apps Domain Name
always_remember_me	False	"Remember me the next time" to enable / disable check box
privkey_filename	/etc/gheimdall2/privkey-nopass.pem	Secret key to use Google Apps SSO service
auth_engine	ldapauth	Authentication modules
use_header_auth	True	Set whether to perform authentication using HTTP headers
auth_header_key	HTTP_SSL_CLIENT_S_DN_E_MAIL	If the header name to authenticate with the HTTP header
use_change_passwd	True	Enable / disable the Change Password feature
use_reset_passwd	False	Enable / disable the password reset feature
passwd_regex	^[~]{8,}\$	Change the password restrictions
domain_admin	adminname	Google Apps administrator User
admin_passwd	*****	Google Apps administrator password
hash_function_name	SHA-1	Google Apps password hash format

Apache Used Folders and Configuration File

Configuration file, directory	Description
/etc/httpd/conf/httpd.conf	Apache Configuration File
/etc/pki/tls/certs	SSL certificate store directory
/etc/httpd/conf.d/ssl.conf	SSL Configuration File

Step 2 – Apache CSR Generation

If you use HTTPS to access the SAML authentication system from the client, the server will require an SSL certificate authentication system. If you already have a certificate to use for the application, please proceed to [Step 4 – Installation of the Certificate to the Server](#).

1. Follow the CSR generation procedure in the next step to get the SSL server certificate.

```
$ /usr/bin/openssl genrsa -rand _rand.dat -des3 2048 > ssl.key  
  
$ /usr/bin/openssl rsa -in ssl.key -out ssl.key-nopass  
  
$ /usr/bin/openssl req -new -key ssl.key-nopass -out csr.pem  
  
$ chmod 0700 ssl.key*
```

2. Set the following items for the certificate Distinguished Name (DN). Note, you should replace the following details with the details specific to your organization.

Item	Value
Country Name (2 letter code) [GB]:	GB
Organization Name (eg, company) [My Company Ltd]:	OrgName
Organizational Unit Name (eg, section) []:	Domain Control Validated
Common Name (eg, your name or your server's hostname) []:	server.orgname.com
Email Address []:	

Step 3 – Obtaining a Certificate

The next step is to obtain a GlobalSign Organizational Vetted (OV) certificate from the CSR you created in the previous steps.

1. Go to <http://www.globalsign.com/ssl/> and click **Buy Now** under the Organizational High Assurance SSL option.

OrganizationSSL

High Assurance SSL

\$1.25M warranty
7 Day Refund
Organization identity included
Higher levels of trust

[Learn more](#)

[Buy Now](#) | [Renew](#)

2. Select your region and click **Select and Continue** to go to the next step.

Select Region:

Please Select your Region ▼

To best serve all our worldwide customers, GlobalSign has numerous of Global offices. Please select your Country or Region to ensure you receive the best support from our staff in the most appropriate local office.

[Select and Continue](#) [Go Back](#)

3. Your order will then be processed and the Certificate Application will appear. Complete all required information of the application and click Next. Note, this is not the vetted certificate information. Click **Continue** once you have completed the application.

1 Product Details

2 GCC Account Setup

3 CSR / AutoCSR Entry

4 Payment Details

5 Confirm Details

6 Completed

OrganizationSSL Certificate Application

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.

Signing Algorithm

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

i SHA1 certificates are limited to a 3 year maximum validity period. Microsoft will stop trusting these certificates in January 2017, so any SHA1

4. Next you will enter in your account details. These details will be vetted and included as the certified identity within your issued certificate.


Important – make sure the details entered are correct as GlobalSign will vet the details you include.

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

GlobalSign Certificate Center (GCC)

Setup GCC Account Details & Contacts

Registered Organization details

*** Required field**  Your registered address is the official address that your business is registered at. Generally it will form part of the public record.

Organization Name: *

Address: * Line 1
 Line 2

Town / City: *

State / County: *

Zip Code / Postal Code:

Country: *

Telephone: * Include dialling code

Fax: Include dialling code

DUNS (Dun &

You will also need to choose a username and password. An account number (PAR####) will be appended to the username you choose.

GCC Account Contact

The GCC Account Contact will receive the issued Certificate and Renewal Notices when the Certificate approaches expiration. This Contact person will also be the primary contact associated with the GCC account and will have full admin rights.

If you wish for a second Contact to also receive the Certificate, you can specify a new contact point in the section for Point of Contact.

Select GCC User ID: *

Select GCC Password: *

Confirm GCC Password: * Re-enter password to confirm.

Optional – add an additional point of contact (this is commonly used when you are applying on behalf of someone else).

Point of Contact for Certificate delivery / vetting issues

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.

For OrganizationSSL & ExtendedSSL applications GlobalSign will place a verification telephone call to the Organization being issued the Certificate. The Point of Contact should be someone within the Organization and they should expect the verification call.

This person, if different to your GCC Account Contact, will not have access to your GCC account.

- ☒ Point of Contact is same as GCC Account Contact
- ☐ Specify a different Point of Contact

Click **Continue**.

5. Enter in your Certificate Signing Request (CSR). The next step varies depending on whether you will provide a self-generated CSR or not. If you choose the AutoCSR option, it is recommended to write down the private key password that you create. For security purposes, this password is not kept on file. If this password is lost, you must reissue your certificate in order to create a new one. Click **Continue**.

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

Enter Certificate Signing Request (CSR)

If you **have** a CSR please complete the section below. If you **do not have** a CSR or do not know how to create one on your web server, don't worry, just choose one of the alternative methods below.

- ☒ Yes, I already have a CSR and will paste it into the input box below (default)
- ☐ I do not have a CSR, so I will use the AutoCSR delivery method (we generate the CSR for you)

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

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDYTCCAsoCAQAwYUxHjAcBgNVBAMTFXd3dy5jZXJ0YXV0aG9yaXR5LmNvbTEb
MBkGA1UECxmSVGVzY2huaWNhCBTdKBwb3J0MRYwFAYDVQQKEw1HbG91YXN0dW
IFVLMRIwEAYDVQQHEw1NYW1kc3RvbWUxDTALBgNVBAQTEct1bnQxQzAJBgNVBAYT
AkdCMIGIMAOCQGSqSIB3DQEBQUAA4GNADCB1QKBgQDQXWmVPB13EUGuJ3QzVpefH
Rz4cV5jOERxZCDF39d/tYgYJTC8su3xOGVREC9T9tTwjSHKcv4WOpIrTc7+CXLqz
hgatGgNzZr1GNt1LAHIAbwTwna7FwQ3r1RZdpL0Hy4AzzeWfNbq1H1eEh3WvPRb
CFbzGmDQqQS44tmrwmOWIDAQABoIIImTAAgBqBzBgEEAYI3DQIDMQWc3UuMS4y
NjAwLjIwewYKKwYBBAGCNwIBDjFtMGswDAHIAbw4AQH/BAQDAgTwMEQGCsGSIb3
DQEJDwQ3MDUwDgYIKoZIhvcNAwICAQCAIA4GCCqGSIb3DQMEAgIAgDAHBGUrDgMC
BzAKBgqgqhkiG9w0DBzATBgNVHSUEDAKBggrBgEFBQcDATCB/QYKKwYBBAGCNwOC
AjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAGSAZqB0ACAAUgBTAEIAIABTAEMAaABh
AG4AbgB1AGwAIABDIAHIAeQBAwAHIAbwBzAHIAIAYQSwAGAAQBAQBAIAAAUABYAG8AdgBp
AGQAZQBYA4GJAJNjHxOpKtL7BFcmT5oF0MmDDU0ehAjWa+Am/1oT4HsX4zjuasD
htaAzk21snAHIAbwRv1DyUq6vuHKLUIV1UMKXpQhm/MVBE6cQqJia4TedO/bxV6
+XbB5JrTksJEkps/cq7LmWHgOPiYnyhtx04McBbaFKGZ5vhPmOKLIVAAAAA
AAAwDQYJKoZIhvcNAQEFBQADgYEAIGqvWuAT42pOauAHIAbw00vgasOoT0bY89pt
FQ3wtEo6ko276FDd6NhoFj74URXJDNCK9XE4c4b0h1Scdhm87RqffFRJEeBT6MkP
vvK70L3n0QmgKoLW+TndK60FnQauf8wSD3pvdgSrd7gWsfzKW3mYiaHz6eqi07B
rNkWPUE=
```


6. You will be presented with the option to obtain a Site Seal. 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. This is optional. Once you have completed the form or decided not to obtain a Site Seal click **Continue**.

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

Enter Secure Site Seal Profile Information

Your Profile 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:



Information added on this page will be displayed in your company profile. To display only the verified information present within your issued Certificate, do not add anything else in this page. If you wish to add other information, such as Contact Telephone & Fax numbers, or your trading address, please complete as appropriate. Note: your Organization Name, City, State & Country are verified details and present within your Certificate. They may not be amended.

Organization Name: GlobalSign Inc.

Street Address 1:

Street Address 2:

City:

State or County:

Zip code / Postal Code:

7. Complete the payment details. Click **Continue**.
8. Confirm the details you entered and agree to the **Terms of Service** and **Subscriber Agreement**. Click **Complete**.

Terms of Service

GlobalSign Certificate Center (GCC) - Terms of Service
US Version
Version 1.4

☐ *I agree to the Terms of Service [download PDF](#)

Subscriber Agreement

GlobalSign Subscriber Agreement - Version 3.0
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE

☐ *I agree to the Subscriber Agreement [download PDF](#)

Once you have successfully ordered your Organizational Vetted (OV) Certificate, your application will be sent to our vetting team. Vetting your application details can take up to **2-3 business days**. Once the vetting process is complete, your certificate will be emailed to you and available for download from your account. Once the vetting process is complete please proceed to [Step 4 – Installation of the Certificate to the Server](#).

Step 4 – Installation of the Certificate to the Server

The SSL server certificate, key and intermediary certificates are each stored on the server, in a location referenced from the Apache SSL Configuration file.

Location	Description
/etc/httpd/conf/ssl.crt/server.orgname.com.crt	SSL Certificate
/etc/httpd/conf/ssl.key/server.orgname.com.key	Private Key (without password)
/etc/httpd/conf/ssl.crt/int.crt	Intermediate Certificates File

Note, if you use a private key with a pass phrase, starting/restarting Apache requires the private key password to be entered each time.

Step 5 – Apache SSL Settings

Setting up SSL on Apache requires adding the location of the certificate, key and intermediary certificates to the Apache configuration file. Note, that this may be located in its own file or in some cases will be in the httpd.conf file.

Apache SSL Configuration File

Location	Description
/etc/http/conf.d/ssl.conf	SSL Configuration File

Apache SSL Settings

Parameters	Values
SSLCertificateFile	/etc/httpd/conf/ssl.crt/server.orgname.com.crt
SSLCertificateKeyFile	/etc/httpd/conf/ssl.key/server.orgname.com.key
SSLCertificateChainFile	/etc/httpd/conf/ssl.crt/int.crt

Step 6 – Creating a Key Pair for Google Apps

In order to use Google Apps, you will require a key pair for authenticating your system to Google Apps SSO service. We will create the key pair using OpenSSL.

Complete the key pair generation.

```
# openssl genrsa -des3 -out privkey.pem 2048
# openssl rsa -in privkey.pem -out privkey-nopass.pem
# openssl rsa -in privkey-nopass.pem -pubout -outform DER -out publickey.der
```

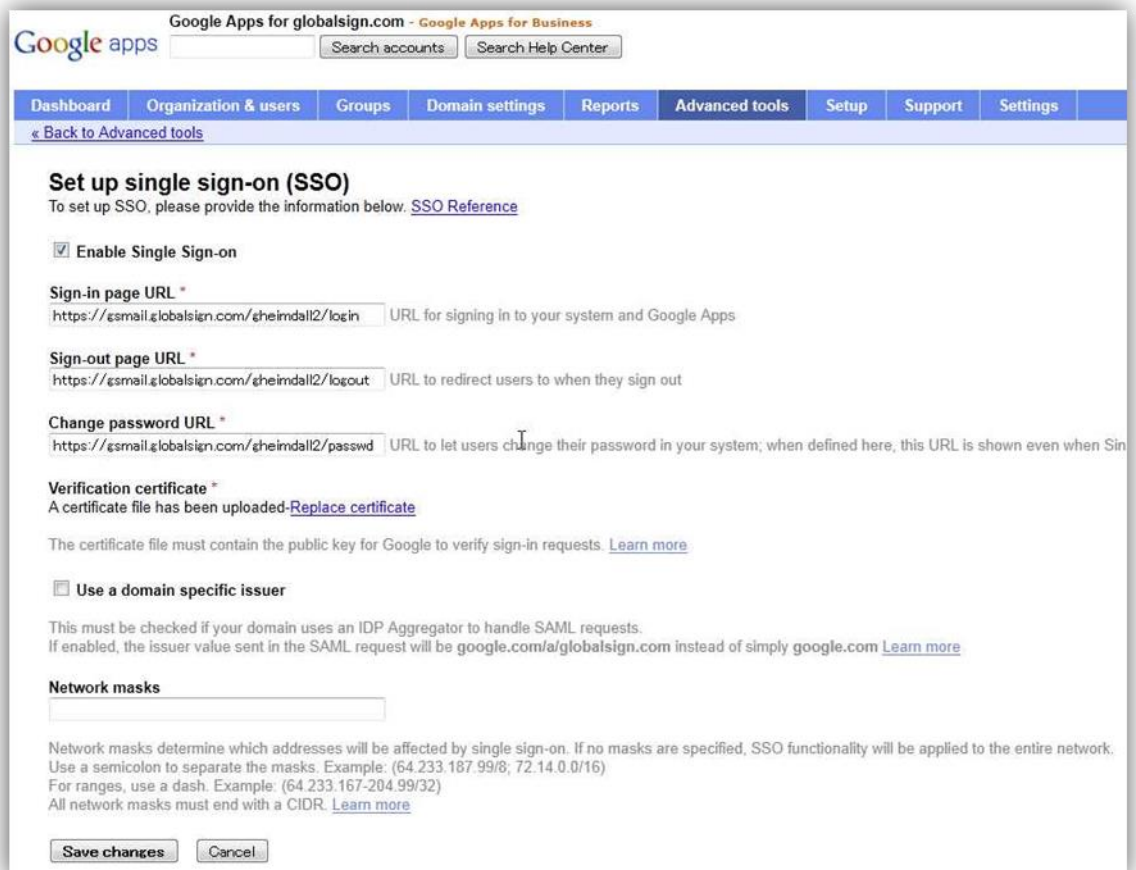
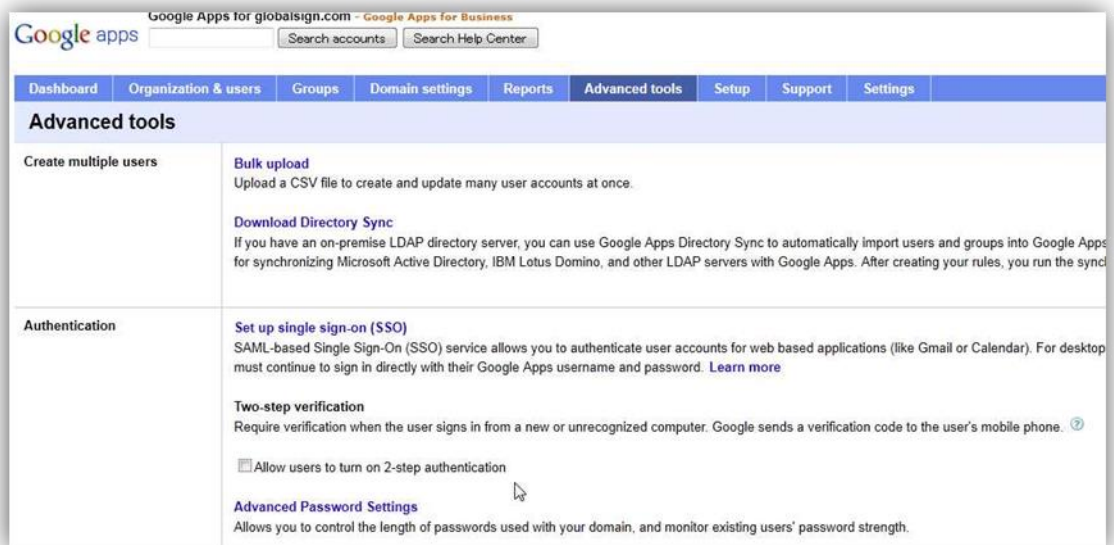
The private key should be stored on your server and the public key should be uploaded to the Google Apps control panel.

Step 7 – Google Apps Settings

It is now time to configure your Google Apps Settings to allow the single sign-on:

1. Go to the Google Apps web control panel.

2. Select **Advanced Tools** and **Single Sign-on** to set all settings to enable SSO.



Overview of the Google Apps SSO Settings:

Parameters	Values
SSO Valid	ON
Login URL	https://server.orgname.com/gheimdall2/login
Logout URL	https://server.orgname.com/gheimdall2/logout
Password URL	https://server.orgname.com/gheimdall2/passwd

Certificates	Browse to file location of publickey.der (created at step 1 above)
--------------	--

Step 8 – LDAP Settings (Via LDIF)

Next, the EPKI Administrator uploads the public certificates associated with authorized users to a directory that the SAML server with query for authorization decisions. EPKI provides a method to generate a LDIF (Lightweight Directory Access Protocol) report for upload to an LDAP directory. This LDAP directory will be used to authorize users to log on to the corporate Google Apps account using their certificate for authentication.

If you are looking for more information about using your EPKI account please refer to the instructions found in the EPKI Administrator Guide: <https://www.globalsign.com/support/ordering-guides/globalsign-epki-admin-guide.pdf>

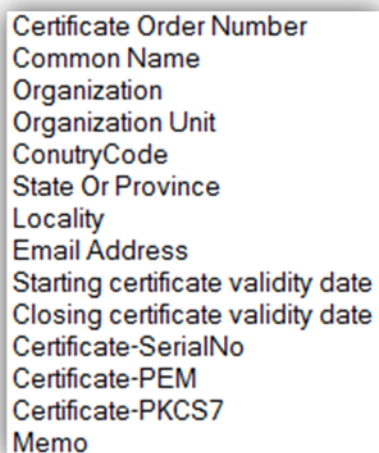
1. **Extracting LDIF From EPKI Console** – LDIF reports can be formatted by the EPKI administrator via the **Configure LDIF** link found under **Other Functions** in the EPKI management console.



Please note that the initial LDIF default format has been established by GlobalSign. The EPKI Administrator must modify the LDIF Template based on the 'Profile' the LDIF query will run against.

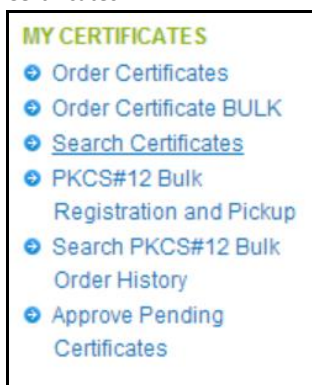


The LDIF message format can be modified by clicking on a variety of substitution variables available in the far right pane. To save changes click **Next** and then **Complete**.



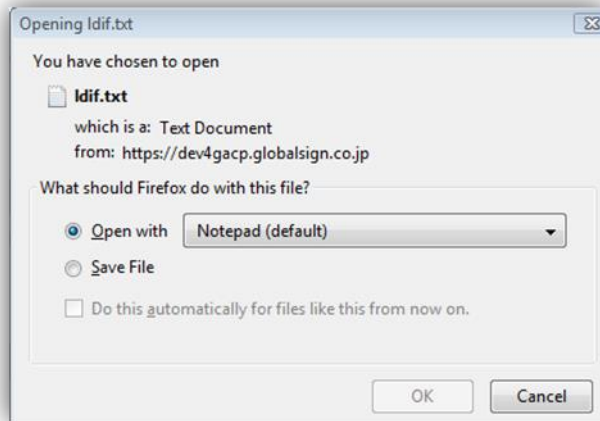
You can reset the format back to the default values anytime by clicking **Reset Message** as illustrated below.

2. **Generating a LDIF Report** – LDIF reports are generated from the **Search Certificates** link found under **My Certificates**.

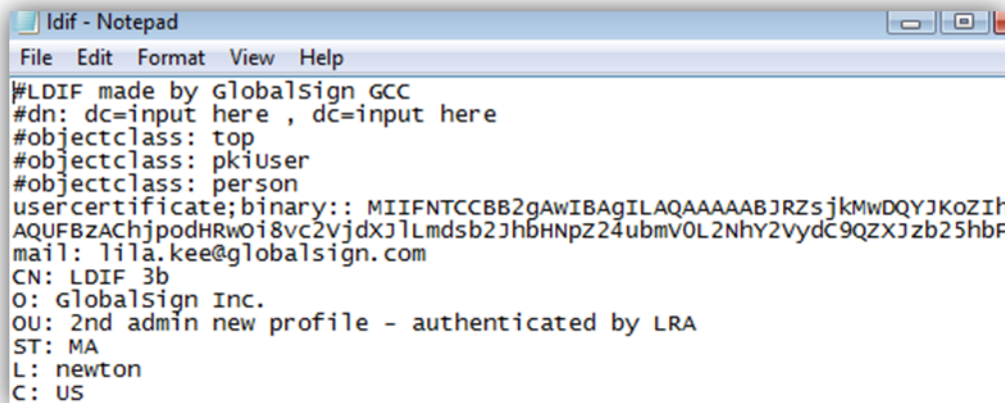


Select the appropriate date range, profile ID (if you have more than one) and set the **Certificate Status** as **Issue Completed** via the drop down menu. Note, if a certificate has been reissued the replacement certificate will have a status of issued and will be included in the LDIF report. The original, replaced certificate will not be included in the query since its status will change to reissued. Only non-revoked and unexpired certificates will be included. Then click on the LDIF button to download the report.

Open the file with your preferred application.



Below is an example entry:



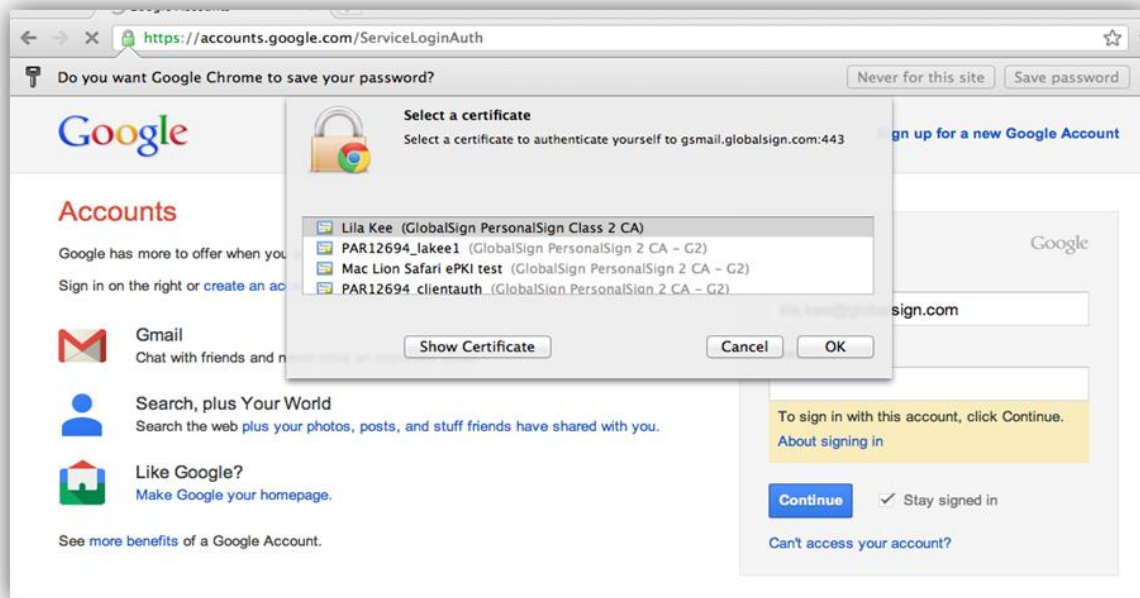
Upload this to your LDAP directory according to your product specific instructions. For example, for OpenLDAP the LDIF would be added using a command as such:

ldapadd -H ldap://ldap.orgname.com -x -D "cn=orgname,dc=example,dc=com" -f Idif.txt -w secret

Step 9 – Accessing Google Apps for Business

Users should now have access to Google Apps via their usual link (<https://docs.google.com/a/orgname.com>). On first access, the user will be asked to present a certificate together with their password, and will be asked whether they wish to link this certificate to their account. As long as the certificate and password are linked in the LDAP, they will be allowed access and future logins will be via their certificate. If allowed by the administrator, users will also be able to update their password.

From here users can share docs with others in the usual way.



Appendix A – Password Synchronization – Advanced Design

There is an optional password sync/manage process which is also controlled by GHeimdall. GHeimdall will update the Google's user's password from the local directory server. The Google user password and the GHeimdall user password can be set to remain in sync.

GHeimdall Configuration

Defining the necessary configuration information in GHeimdall is carried out in two locations.

1. **GHeimdall Template** – modify the template GHeimdall2. For modifications please refer to the relevant screen configuration of GHeimdall2. Below is the templates directory:

Location	Description
/etc/gheimdall2/static/	css, image file storage directory
/etc/gheimdall2/templates/	Web page template file

2. **Authentication Related** – modify the settings file to configure GHeimdall for your Organizational needs. Required settings include your domain name, your private key location, authentication type, password settings, certificate authentication field, LDAP information and template path.

GHeimdall2 Settings (/etc/gheimdall2/gheimdall2.conf) (additions to default):

```

--- gheimdall2.conf.dist
+++ gheimdall2.conf

@@ -13,6 +13,6 @@

# Domain name for Google apps

-apps_domain = 'example.com'
+apps_domain = 'orgname.com'

```

```

# private key

-privkey_filename = '/some/where/privkey-nopass.pem'

+privkey_filename = '/etc/gheimdall2/privkey-nopass.pem'


@@ -22,3 +22,3 @@

# auth_engine to use

-auth_engine = 'sample'

+auth_engine = 'ldapauth'


@@ -54,4 +54,6 @@

# passwd policy

-passwd_regex = '^.{8,}$'

+# passwd_regex = '^.{8,}$'

# passwd_regex = '^.*(?!.{8,})(?!.*\d)(?!.*[a-z])(?!.*[A-Z])(?!.*[@#$%^&+=]).*$'

+# passwd_regex = '(?!.*\d)(?!.*[a-z])(?!.*[A-Z])^[ -~]{8,}$'

+passwd_regex = '^[ -~]{8,}$'


@@ -61,3 +63,3 @@

# Set to True if you use auth with specific header value

-use_header_auth = False

+use_header_auth = True


@@ -72,8 +74,9 @@

# The header name for header authentication.

-auth_header_key = 'SSL-CLIENT-S-DN-CN'

+#auth_header_key = 'SSL-CLIENT-S-DN-CN'

#auth_header_key = 'REMOTE_USER'

+auth_header_key = 'HTTP_SSL_CLIENT_S_DN_EMAIL'


# Google Apps admin user name and password. (If you want to sync passwords.)

-domain_admin = 'admin'

-admin_passwd = 'password'

```



```

+domain_admin = 'admin'

+admin_passwd = '*****'

@@ -83,7 +86,7 @@

# ldap stuff

-ldap_uri = 'ldap://ldap.example.com/'

-ldap_basedn = 'dc=example,dc=com'

-ldap_filter = 'uid=%s'

-ldap_rootdn = 'cn=admin,dc=example,dc=com'

-ldap_rootpw = 'password'

+ldap_uri = 'ldap://172.0.0.0/'

+ldap_basedn = 'dc=globalsign,dc=com'

+ldap_filter = '(mail=%s@orgname.*)'

+ldap_rootdn = 'cn=admin,dc=orgname,dc=com'

+ldap_rootpw = '*****'

ldap_passwd_hash_style = '{SHA}'

@@ -100,3 +103,3 @@

# Corresponds with an error on SSL Client Auth

-use_subprocess_for_signing = False

+use_subprocess_for_signing = True

@@ -111,3 +114,3 @@

[[response_creators]]

-google.com = "default"

+google.com = "uselocalpart"

```

GHeimdall2 Settings (/usr/lib/python2.4/site-packages/gheimdall2/settings.py)

Additions to default – here you will change the settings from warnings only to info and add the correct link to the template location:

```

file_logger = logging.FileHandler("/var/log/gheimdall2/error.log")

-file_logger.setLevel(logging.WARN)

+file_logger.setLevel(logging.INFO)

formatter = logging.Formatter('%(asctime)s: %(pathname)s: %(lineno)d: %(name)s: %(levelname)s: %(message)s')

```

@@ -45,3 +45,3 @@

```
logging.getLogger("").addHandler(file_logger)

-logging.getLogger().setLevel(logging.WARN)

+logging.getLogger().setLevel(logging.INFO)
```

@@ -123,3 +123,7 @@

```
# Don't forget to use absolute paths, not relative paths.

- os.path.join(os.path.dirname(os.path.abspath(__file__)), 'templates'),

+ '/etc/gheimdall2/templates',

+)

+

+LOCALE_PATHS = (

+ '/etc/gheimdall2/locale',

)
```

Apache & GHeimdall Related Settings (additions to default)

For your Apache server you will add the webserver, certificate and encryption details for our local server. At this stage you will also add the client certificate details which Google will use to connect to the service.

```
+Listen 443
+<VirtualHost _default_:443>
+ServerName server.orgname.com:443
+ErrorLog logs/ssl_error_log
+TransferLog logs/ssl_access_log
+LogLevel warn
+SSLEngine on
+SSLProtocol all -SSLv2
+SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
+SSLCertificateFile /etc/httpd/conf/ssl.crt/server.orgname.com.crt
+SSLCertificateKeyFile /etc/httpd/conf/ssl.key/server.orgname.com.key
+SSLCertificateChainFile /etc/httpd/conf/ssl.crt/int.crt
+SetEnvIf User-Agent ".*MSIE.*" \
+    nokeepalive ssl-unclean-shutdown \
+    downgrade-1.0 force-response-1.0
+CustomLog logs/ssl_request_log \
+    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
+</VirtualHost>
+
+<Location "/gheimdall2/">
@@ -8,5 +27,11 @@
    PythonDebug On
+    SSLCACertificatePath /etc/pki/tls/certs
+    SSLVerifyClient require
+    SSLVerifyDepth 3
+    # SSLRequire (%{SSL_CLIENT_S_DN_O} in {"OrgName"})
+    SSLRequire (%{SSL_CLIENT_S_DN_O} in {"OrgName"}) or (%{SSL_CLIENT_S_DN_Email} in {"adminname@orgname.com"})
+    RequestHeader set SSL_CLIENT_S_DN_Email %{SSL_CLIENT_S_DN_Email}s
+</Location>
-Alias /gheimdall2/static/ "/usr/lib/python2.4/site-packages/gheimdall2/static/"
-<Directory "/usr/lib/python2.4/site-packages/gheimdall2/static/">
+Alias /gheimdall2/static/ "/etc/gheimdall2/static/"
+<Directory "/etc/gheimdall2/static/">
    Options Indexes MultiViews
```

GHeimdall2Rotating Logging Setting (/etc/logrotate.d/gheimdall2)

```
/var/log/gheimdall2/*log {  
    weekly  
    create 0755 apache apache  
    missingok  
    notifempty  
    sharedscripts  
}
```

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 1 82 88 01 24

www.globalsign.fr

ventes@globalsign.com

GlobalSign DE

Tel: +49 30 8878 9310

www.globalsign.de

verkauf@globalsign.com

GlobalSign NL

Tel: +31 20 8908021

www.globalsign.nl

verkoop@globalsign.com
