

High Quality Education For All

Computer Services Documentation



Shibboleth Documentation

{Shibboleth & Google Apps Integration}

John Paul Szkudlapski June 2010

Note: These case studies, prepared by member organisations of the UK federation, are provided for information purposes only and reflect the particular arrangements and experience of those concerned.

Introduction

This document provides information intended to help those installing and configuring Shibboleth to work with Google Apps (Education Edition). It assumes that you are using Microsoft Active Directory as an authentication method for your users.

There are six parts to getting Google Apps to work correctly with Shibboleth:

- 1) DNS/FQDN Configuration
- 2) Initial Sign Up to Google Apps
- 3) Configuration of Google Apps (pre-Shibboleth)
- 4) Setting up Active Directory Synchronisation
- 5) Setting Up Shibboleth
- 6) Altering Google Apps to use Shibboleth as an authentication method

Part 1 – DNS/FQDN Configuration

For the purposes of this document we are going to set up a new fully qualified domain name (FQDN) of 'shibmail.bsfc.ac.uk'.

Step A – Register DNS Entries

Register your new FQDN by adding the following DNS information for your required DNS entry (again in this example we are using shibmail.bsfc.ac.uk):

Registering all the information below at once will save you having to carry out other steps later on.

shihmail	IN	MX	10	asomy Laooale.com
Shibhali			10	aspinkilguugieleun
	IN	MX	20	alt1.aspmx.l.google.com
	IN	MX	20	alt2.aspmx.l.google.com
	IN	MX	30	aspmx2.googlemail.com
	IN	MX	30	aspmx3.googlemail.com
	IN	MX	30	aspmx4.googlemail.com
	IN	MX	30	aspmx5.googlemail.com
\$ORIGIN shibmail.bsfc	.ac.uk			
googlefffffff9489253a	IN	CNA	ME g	oogle.com
mail	IN	CNA	ME g	hs.google.com
			-	

This will normally take 24 hours to become effective.

Part 2 – Initial Sign Up to Google Apps

Navigate to the Google Apps signup page:

http://www.google.com/a/cpanel/education/new

Enter your domain name *shibmail.bsfc.ac.uk*

On the next screen ("Sign up for Google Apps Education Edition – Step 2 of 3"), complete the information on the page and click next.

On the next screen ("Sign up for Google Apps Education Edition – Step 3 of 3"), create an administrator account with an associated password – this will be used to administer GoogleApps:

Username

mailadmin

You will then be passed over to the "Welcome to Google Apps" page:

Google Apps for shibmail.bsfc.ac.uk - Education Edition		mailedmin@shibmail.bsfc.ac.uk Take 6dmin Survey Inition Help Sk			Sign				
Google apps		Sean	ch accounts	Search Help	Center				
Dashboard Univ	in ant groups	Unmain settings	Advanced form	Sapport	Services	ntinger			
Welcome to	o Google Ap	ps							
To activate your an administrations ca	count, you need to n manage Google	verify that you own sh Apps for your domain	ibmail balc ac uk . V	enfication does	not disrupt y	our existing services,	and ensures that on)	y authorized	
Select one of	of the methods bei	low for verification in	structions						
O Upload Recom	an HTINL file to shi mended if you can	bmail.bsfc.ac.uk upload files to shibm	all balc ac ult						
Change CNAME	shibmail.belic.ac.i records are create	uk CNAME record ed with your domain h	oet						
Continue	10								

Select "Change shibmail.bsfc.ac.uk CNAME record" and click "Continue".

At the next screen ("Change CNAME records to verify that you own shibmail.bsfc.ac.uk"), click "I've completed the steps above":

 Change CNAME records to verify that you own shibmail.bsfc.ac.uk

 Follow the steps below to verify your domain ownership.

 1. Sign in to your domain hosting service and locate the DNS management page. The location veries by service, but can typically be found under Domain Management or Advanced Settings.

 2. Use the following unique string to create a new CNAME record for the shibmail.bsfc.ac.uk domain: googlefffffff9489253a

 3. Point the CNAME record to: google.com

 4. Once you have made the changes, you can verify that the record exists by doing a CNAME lookup for http://www.opogle.com

 Point the steps above
 I will verify later

If your DNS has not propagated, you will need to wait 24 hours before you continue.

After your DNS has propagated, log back into the site via the link:

https://www.google.com/a/shibmail.bsfc.ac.uk/

Log in as Administrator (in our case mailadmin), and return to "Verify the domain ownership".

Part 3 – Configuration of Google Apps (pre-Shibboleth)

In our system we want to be able to use our FQDN rather than Google's built-in one (http://mail.google.com/a/shibmail.bsfc.ac.uk), so we are going to alter the settings to point at mail.shibmail.bsfc.ac.uk.

GoogleMail

Goto "Service Settings" on the main menu and select "Email".

There are various options that can be set here, but for the purposes of this document I am only going to set the most relevant.

Under "Web address", click "Change URL" and select the 2nd option. As you can see from the screenshot, the default URL for e-mail will now be:

http://mail.shibmail.bsfc.ac.uk

Change URL for Email

Select a simple, easy-to-remember address that redirects to the login page for Email. Change URLs for all domain services

http://mail.google.com/a/shibmail.bsfc.ac.uk (default)
http://mail
.shibmail.bsfc.ac.uk/ (custom)

To enable your custom URLs, you must create CNAME records with your domain host.

Continue »

Click on "Continue"; you will be presented with a "Changing CNAME record" page. As you have already completed this step you can click 'I've completed these steps'.

Return to the Email page ("Service Settings" \rightarrow "Email") and near the bottom of the screen there is a section called "Email Activation". Click on the "Instructions on how to activate Email".

A new page will appear ("How to activate e-mail"). As we are going to use Active Directory to synchronise the users, we can ignore section 1.

In section 2 ("Set up email delivery"), click on the link "Change MX Records".

As you have already completed these steps, click on "I have completed these steps".

We also set the following options in the Email page (these may not be relevant for everyone):

Name Format We un-ticked "Allow users to customize this setting".

Email white list We entered the external IP range of the institutional network.

Part 4 – Setting up Active Directory Synchronisation

There are three steps to achieving this:

Step A – Setting Google Apps to use an external provisioning API.

Step B – Setting the 'new' e-mail address for all your users in Active Directory.

Step C – Setting up the synchronisation with Active Directory.

Step A – Google Apps – Enable Provisioning API

Log into Google Apps as the Administrator, click on 'Users and groups', and then click on 'Settings'.

Put a tick in the box next to 'Enable provisioning API' and click 'Save changes' at the bottom of the page.

Step B – Setting the e-mail address in the Users' Profile

In Active Directory you will need to set the "E-Mail" field with the users' new e-mail address (as this is used as part of the synchronisation routine). I suggest you speak to your network team about this one (as I do both jobs, I didn't think it was necessary to have a conversation with myself).

In our setup, we only have the Students configured to use Google Apps, so only the users inside our Active Directory OU (and subsequent sub-OUs) are synchronised to Google Apps:

OU=Students 2009 Entry 2008 Entry 2007 Entry Adult Education

To do this quickly, select all of your users and put this into their e-mail fields:

%username%@shibmail.bsfc.ac.uk

This automatically sets the e-mail field for each as username@shibmail.bsfc.ac.uk

Step C – Setting up Active Directory Synchronisation

You need to install an application called "Google Apps Directory Sync" onto a server in your domain; we have it installed on the same server as our Shibboleth installation.

It can be downloaded from:

http://dl.google.com/dirsync/dirsync-win32.exe

A tutorial is available here:

http://www.postini.com/webdocs/training/en/

DirSync_GoogleApps/DirSync_GoogleApps.html

Once the software is installed, run the config-manager to create and test the config file:

1	<u>y</u>			·	
/ C	oogle Apps Directory Sync -	E:\GoogleApps\studentmail.ami			_ D X
Ble	<u>Windows</u> Help				
Co - = =	Ngure Ganaral Sattings Google Apps – Sattings – Exclusion Rules LDAP Sattings – LDAP Connection – Users – Connection – User Sync	Google Apps Directory Before you first use Google App 1. Log in to your Google 2. Click Users and Grou 3. Check the box labelet 4. Click Save Changes Bpecify which categories of obj	Sync General Settings as Directory Sync, anable the Provisionin Apps domain as an administrator. sa from the top menu, then click the Sett I Enable Provisioning API. ects to synchronize Learn More.	g API in your Google Apps Dashboand inga tab.	Google
	Groups Group Search Rules Exclusion Rules Notifications	Synchronize: Only the items checked above vell	🕑 Users be synchronized.	Groups	

Below I list the left-hand sections, along with the settings that we used. We currently don't sync the AD Groups, so I have left this part out.

Note that the attributes released to Google Apps below include those described as "personal data". For the implications of doing this please refer to the UK federation document *Recommendations for Use of Personal Data*, accessible from <u>http://www.ukfederation.org.uk/content/Documents/FedDocs</u>.

General Settings Synchronize

Users

Google Apps \rightarrow Settings

Admin E-mail Address mailadmin@shibmail.bsfc.ac.uk

Admin Password xxxxxxx

Domain Name shibmail.bsfc.ac.uk

I also entered the address of our Microsoft ISA Server to allow connections out (*HTTP proxy*)

Google Apps \rightarrow Exclusion Rules

Click "Add Rule"	
Туре	USER_NAME
Match Type	EXACT
Rule	mailadmin

Note: This "mailadmin" account is the administrator account that we set up for Google Apps. If you don't specifically exclude it, then when you synchronise your users, it will get deleted because it does not exist on your AD structure.

LDAP Settings \rightarrow LDAP Connection

Connection Type	Standard LDAP
Hostname	bsfcdomain.bsfc.ac.uk
Port:	389
Base DN	We only sync our "Students" OU
OU=Student	s,DC=bsfcdomain,DC=bsfc,DC=ac,DC=uk
Authentication Type	Simple

	Cimpio
Authorised User	xxxxxx@bsfcdomain.bsfc.ac.uk
Password	XXXXXXXX

Note: This is the same user as the one we use in Shibboleth; it is basically a read-only account allowed to do LDAP lookups.

Users \rightarrow Attributes

Server Type MS Active Directory

Email Address Attribute mail

Ensure that all of your student accounts have their Google Apps e-mail address specified in the 'E-Mail tab of their profile'.

Users \rightarrow Extended Attributes

Given Name Attribute	givenName
Family Name Attribute	sn
Password Encryption	SHA1

Users \rightarrow User Sync

Click 'Add Rule'	
Scope	Sub-tree
Rule	<i>objectclass=perso</i> n

Notifications

Send notifications from csgoogle@bsfc.ac.uk

SMTP Relay Host

User Name

Password

We created an account for these notifications to be sent to our admin contact, so that one can see the status of the synchronisation.

Delete Limits

Do not synchronise if the delete limit would be exceeded:

Delete no more than: 60% of users

Log Files

File name	sync.log
Log Level	INFO
Maximum Log Size	1GB

Once you have got to this stage, it is a good idea to save the configuration file. We saved our configuration files into a folder called "C:\GoogleApps" on our Shibboleth Server.

After you have saved the file, move into the **Test** section.

If you click on "Simulate Sync" the process will run based on your configuration file, but will not write anything out to Google Apps.

You should notice that the "Sync Log" will show:

Proposed Changes

Delete:	0
Modify:	0
Create:	xxxx (number of users to create)

You now need to create a scheduled task that runs periodically to update Google Apps based on the changes within AD (user additions/deletions). We have ours set to run at 2am every day.

Create a new scheduled task

New Scheduled Task Nam	ne GoogleAppsSync
Run	"C:\Program Files\Google Apps Directory Sync\sync- cmd.exe" -a -c C:\GoogleApps\studentmail.xml
Run As	We have a dedicated account to run tasks
Schedule	
Scheduled Task	Weekly
Start Time	02:00
Schedule Task Weekly	
Every	1 weeks
On	Mon, Tue, Wed, Thu, Fri, Sun

The next time this task runs, it will populate Google Apps with all of your students, as can be seen from the following screenshot:

	and a man g contra	Contraction of the Automation	Contraction of the local division of the loc	1.11.11.11.1			
ers	and groups						
Inara	Groups Battings						
Voci o	allocation sufficient						
AF	Access is enabled. Any la	ipdates you make via this	control panel will not	thransfer to you	ir user managemi	ent system. Lean more	
	a trade and some some some some some some some some	NAMES AND ADDRESS OF THE OWNER	Verse Transactor I				
Teat	n mente up to 2000-user ac	many users at once - 1 counts for this domain.	Email additions				
The	Delin mane -						1 E d E
Da	lictic galars						1 - 5 of 5
	Name	<u>Usemano</u> *		5	latun	Email Quote	1 - 5 of 5
	Name Pamela Cook	<u>Usemano</u> ♥ 000754@shibmail	heft acuk	5 N	tetury lewly created	Email Quate	1 - 5 of 5 <u>Last signed in</u> Never lagged in
	Name Pamela Cook Michel Witt	Usemamo¥ 000754@shibmail 2937@shibmail.bs	hsfcacuk Atacuk	5 N N	tetus lewly created lewly created	Email Guide	1 - 5 of 5 <u>Linst signed in</u> Never logged in Never logged in
	Name Pamela Cook Michel Witt Jonatrun Petman	Usemano ¥ 000754@shibmail 2937@shibmailos 9618021@shibma	hsfcacuk Acacuk il bakacuk	5 N N	<mark>latus</mark> lewly created lewly created lewly created	Ethal Guota 10%	1 - 5 of 5 <u>Einst signed in</u> Never logged in Never logged in
	Name Pamela Cook Michel Witt Jenathun Petman Tem Holmes	Usemano ¥ 000754@shibmail 2937@shibmailis 9818021@shibmai 8822575@shibmai	hsfc.ac.uk Pc.ac.uk il bafc.ac.uk il bafc.ac.uk	5 N N N	latur; lewly created lewly created lewly created lewly created	Email Quota 0% 0% 0%	1 - 5 of 5 <u>Enst signed in</u> Never logged in Never logged in Never logged in Never logged in
	Name Pamela Cook Michel Witt Jenathun Petman Tem Holmes John Schudiapah	Usemano ¥ 000754@shibmail 2937@shibmailis 9818021@shibmai 9822575@shibmai mailadmin@shibm	hafc ac uk Ac ac uk Al bafc ac uk Al bafc ac uk Nali bafc ac uk	5 N N N	tatur; lewly created lewly created lewly created lewly created dministrator	Email Queta 0% 0% 0% 10% 0%	1 - 5 of 5 Last signed in Never logged in Never logged in Never logged in Never logged in 7 34 pm

Part 5 – Setting up Shibboleth

Google has a handy document on how to set up Google Apps with Shibboleth:

http://code.google.com/apis/apps/articles/shibboleth2.0.html

First we need to configure Google Apps to use Shibboleth; then we need to make some alterations to our Shibboleth installation.

Take a backup of the configuration files before you make any alterations.

Step A – Configure Google Apps to use Shibboleth

To set the SSO configuration you can navigate to the page from either of two locations:

Advanced Tools \rightarrow Set up single sign-on (SSO)

or

Users and Groups \rightarrow Settings \rightarrow Set up single sign-on (SSO)

Below are the configuration options that we have set:

Enable Single Sign-on Ticked

Sign-in page URL

We direct the Sign-in page URL to be our Shibboleth IdP:

https://sso.bsfc.ac.uk/idp/profile/SAML2/Redirect/SSO

Sign-out page URL

At present we direct the users to a static HTML page whenever they sign out of Google Apps:

http://studentapps.bsfc.ac.uk/logoutmail.html

Change password URL

At present we have not implemented a web-based change password option for our Active Directory so we redirected this to a static HTML page:

http://studentapps.bsfc.ac.uk/logoutmail.html

Verification Certificate

Upload the 'idp.crt' certificate from your Shibboleth Install, e.g.: C:\Shibboleth\Shib2\Shib2ldp\credentials\idp.crt

You may need to copy this temporarily to a publicly accessible location.

In this example I am using the 20 year self-signed certificate (idp.crt) to protect the 8443 port. However, if you are going to use another certificate (such as a Janet Certificate Service certificate) to protect the 8443 port, then you should specify it here instead.

Scroll down to the bottom of the page and click "Save Changes".

Step B – Change Shibboleth IdP Files

 a) Create a new file called google-metadata.xml (located at %idp_home%/metadata/) and containing the following text:

Change YOURDOMAIN. COM to reflect your domain; in our case this would read:

```
Location="https://www.google.com/a/shibmail.bsfc.ac.uk/acs" />
```

b) Then edit the file %idp_home%/conf/relying-party.xml and add the following code just after the DefaultRelyingParty element:

Note that the certificate specified via IdPCredential in your relying-party.xml configuration file must match the "Verification certificate" specified in Step A above.

Change YOUR-ENTITY-ID to reflect your IdP name; in our case this would read:

```
provider="https://sso.bsfc.ac.uk/idp/shibboleth"
```

c) Still in the file %idp_home%/conf/relaying-party.xml, add the following code:

```
<!-- Google Metadata -->
<MetadataProvider id="GoogleMD" xsi:type="FilesystemMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata"
metadataFile="IDP_HOME/metadata/google-metadata.xml"
maintainExpiredMetadata="true" />
```

Change IDP_HOME/ to reflect the location of your Shibboleth Installation; in our case this would read:

```
metadataFile="C:\Shibboleth\Shib2\Shib2Idp/metadata/google-metadata.xml"
```

d) Edit the file %idp_home%/conf/attribute-resolver.xml and add the following code:

e) Finally, edit the file %idp_home%/conf/attribute-filter.xml and add the following code:

```
<AttributeFilterPolicy>
        <PolicyRequirementRule xsi:type="basic:AttributeRequesterString"
value="google.com" />
        <AttributeRule attributeID="principal">
            <PermitValueRule xsi:type="basic:ANY" />
            </AttributeRule>
</AttributeFilterPolicy>
```

You need to restart Tomcat for these settings to become effective.

If you now access your Google Apps install via

mail.shibmail.bsfc.ac.uk

You will automatically be directed to your Shibboleth IdP login screen:

	BIRKENHEAD SIXTH-FORM-COLLEGE High Quality Education for All	BSFC Computer Services Single Sign-on Service	
	User Name: Password:		
		Login	
The res Birke	source that you have attemp nhead Sixth Form College (oted to access requires that you login Computer Network username and par	with your ssword.
lf you ar	e having any trouble logging	g in, please contact the Computer Se	rvices staff

If you now log in as a user, you will automatically be redirected to your Google Apps mail page:

Coogle	Stea mailadmin@shibmail.bsfc.ac.uk <u>Managa thia domain</u> Settings H	alo I Sign a
Mail Compose, Mail	<u>Windows T ** Duppt Access</u> - microsolt com/everybodyshusmess - Making Muhile Computing On The Ge S assurptions and **	
bibox (2)	Anothive Report spann Delete Nove tor Labers Nove actions Ration	1-2 012
Staned 😭	Belect, All, None, Read, Unread, Blarred, Unstarred	
Sent Mail	Gmail Team Access Gmail on your mobile phone - The days of needing your comp	Mar 23
Ealow in Miss Priority 4.more+ Contacts Tests	Get started with Gmail - Gmail is hult on the ideo that email can be into	Mar 23
- Chat		
Search, add, or invite	Select: Al, None, Read, Unread, Starred, Unstarred	
John Szkudlapski Set status here	Archive Report spam Delete Nove for Labels? None actions? <u>Referch</u>	1 - 2 of 2
(j)	Add phone numbers, notes and more for the people in your <u>Contact The</u> <u>Learn more</u> You are currently using 0 MB (0%) of your 7437 MB:	

Disclaimer

This case study is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.