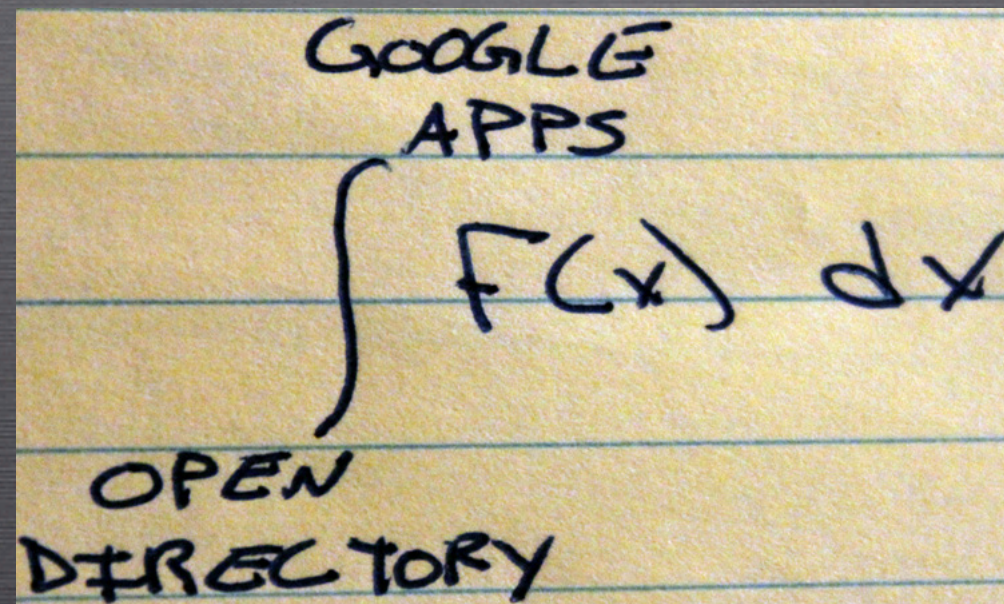


# GOOGLE APPS AND OPEN DIRECTORY



RANDY SAEKS

TWITTER: @RSAEKS

[HTTP://WWW.TECHRECESS.COM](http://www.techrecess.com)



# AGENDA

---

- Quick Google Apps Overview
- Structure Setup
- Preparing OD
- Configuration
- Lessons
- Q&A&S



# RESOURCES

---

<http://techrecess.com/mactech>



# YOU ARE ...

---

OS X Server Administrators

Lead Geek

Network Managers

Directory Service Admins

Technology Nerd

Organizational Technology Leaders

Whatever gets put on my desk

Keeping Current-ers

Single-handed reason local coffee shop is still open



# ... AND HERE

---

we are going to deploy  
Google Applications

I want to learn more about  
ways to leverage Open  
Directory

we are looking to deploy  
Google Applications

I want to bring a solution  
back to work

A professional looking  
to learn more

of another reason



# GOOGLE APPS OVERVIEW

---

- Standard, Premier and Education are major editions.
- Differences relate to cost and storage.

	Cost	Storage	Limitations
Education	\$0	7GB email	Need to be Edu. or 501(c)3
Standard	\$0		50 accounts Does not to SSO
Premier	\$50 per user per year	25GB email	



# SERVICES

---

Mail	Sites	Moderator	Video
Google Chat	Calendar	Docs	Mobile
Google Labs	Marketplace Tools	Extends ability of Google Apps with other services	



# GOOGLE APPLICATIONS

---

- Emphasizes Collaboration
- Service Control
- Remote Access
- Sharing and permissions



# CALENDAR

---

- Web-based calendar
- Mobile device synchronization
- Supports iCal, Outlook, CalDAV



# CHAT

---

- Jabber protocol
- Organizational IM capability
- Voice & Video Supported
- Offline messaging & archiving



# DOCS

---

- Documents
- Presentations
- Spreadsheets
- Forms
- Drawing



# Docs

---

- Word / Excel support (.docx, xlsx)
- PowerPoint (.pps, ppt)
- Other common formats (.rtf, .csv, odt)
- Template support
- Store & share other files



# FORMS

---

- Simple survey mechanism
- Results collected in spreadsheet



# EMAIL

---

- Provides domain eMail services
- Many users already know GMail
- POP, IMAP, web
- Sync to devices



# SITES

---

- Access Controls
  - Users, groups, domain, public
- Share Knowledge in a wiki typed setup



# SITES



District 30  
applications

Browse sites in d30.me

[« Back to dashboard](#)

Browse by popular categories

**(uncategorized)**

[art](#) (1)

[classroom](#) (1)

[club](#) (1)

[current events](#) (1)

[health](#) (1)

[music](#) (1)

[school](#) (1)

[school sports t.v](#) (1)

[spanish](#) (1)

[sports](#) (1)

[t.v](#) (1)

## Uncategorized sites

[Eighth Grade Social Studies](#) Shared with everyone in d30.me

[Fletcher Free Press](#) Shared with everyone in the world

[Michalakos' Site](#) Shared with 20 people

[Miss Lund's Classroom](#) Shared with everyone in the world

[Monarch Award Literature Blog](#) Shared with 80 people Library Lit Blog 2nd grade

[Mrs. Connolly's Connection](#) Shared with everyone in the world

[Mrs. Sachman's Classroom](#) Shared with 2 people

[Mrs. Zdonek's Site](#) Shared with everyone in the world An online learning community

[Murnick](#) Shared with everyone in the world

[Onsrud's News Network](#) Shared with everyone in the world

[test site](#) Shared with 1 person

[Rezac's Embeds](#) Shared with everyone in d30.me

[Welcome to Ms. Freehill's Class](#) Shared with everyone in the world



# SITES

---

▼ Home

Helen Keller Reflection

Assignments

▼ Science Blog

Plants

Second Science Blog Question

Sitemap

Edit sidebar

[Home >](#)

## Helen Keller Reflection

Now that we have learned about Helen Keller and we have finished the book, what are some of your thoughts?

### What do you think was the most challenging thing in Helen's life? If you were Helen, what would you find challenging?

Write at least 5 sentences (substantial sentences) answering these questions or explaining your thoughts about the book. Make sure to check your spelling before you post.  
Comment on at least 2 other students posts--try to comment on a post that doesn't have a lot of comments.

New post

#### [HELEN KELLER](#)

posted Oct 20, 2010 1:47 PM by lindy v

One big challenge in Helen Keller's life was when Annie came. Helen didn't know who Annie was and she was scared. When you are blind and deaf your life is dark and silent. Helen took a big step in life by learning new words with your hands. If I were Helen Keller I would be proud of myself for catching up so fast. Helen Keller was actually an ordinary girl.

[\(Edit post\)](#) | [1 comment](#)



# SITES

---

[Home](#) > [Helen Keller Reflection](#) >

## Being blind, and deaf

posted Oct 20, 2010 1:46 PM by marcus g

If I were blind, and deaf, the most challenging thing would be having to walk and see. And the most challenging thing about being deaf, is having to hear when anybody calls and you still can't hear. Type a comment if you agree or disagree with me.

 **Attachments (0)**

### Comments (2)

**madeleine h** - Oct 20, 2010 1:59 PM - [Remove](#)

Marcus, I think you are right, if you where blind and deaf you would not be able to hear people.

**daniel r** - Oct 27, 2010 1:49 PM - [Remove](#)

I think you are right about it because it's really hard to see and hear everything.



# TECH OVERVIEW

---

- SAML
- GADS



# DOMAIN STRUCTURES

---

- Single Domain
- Single Domain with sub-organizations
- Multiple Domains



# SINGLE DOMAIN - FLAT STRUCTURE

---

One domain to manage ...	Loss of control to differentiate service access
Need to tweak OD for password syncing ...	Allows OD password to work with Google Apps
No tweaks needed for SAML ...	I've got nothing



# SINGLE DOMAIN WITH SUB-ORGANIZATIONS

---

One domain to manage ...	Control services on (sub) organization(s) level
Need to tweak OD for password syncing ...	Allows OD password to work with Google Apps
Need to tweak OD for SAML ...	Only one SAML install required
Only need one SSO configuration ...	Caveats with GADS



# MULTIPLE DOMAINS

---

Multiple domains to manage ...	Control services on domain level
Need to tweak OD for password syncing ...	Allows OD password to work with Google Apps
No tweaks needed for SAML ...	Again, nothing
Need SSO configuration per domain ...	Flexibility in SSO configuration and options



# REQUIREMENTS

---



# ONE OR MULTIPLE DOMAINS WITH SAML

---

- Configure SAML Identity Provider (IdP)
- Determine attribute mapping for identifying user in Google Apps
- Accounts need to exist in Google Apps



# SUBDOMAINS WITH SAML

---

- Configure a SAML Identity Provider (IdP)
- Determine attribute mapping for identifying user in Google Apps
  - This needs to be the full user ID
- Accounts need to exist in Google Apps



# DOMAINS USING GADS

---

- Password Server External Command
- Attribute for SHA1 hash of password
- Configure GADS
  - Users can be created in Google Apps
- Determine GADS run frequency



# CONFIGURATION

---



# SYNCING OD PASSWORDS VIA GADS

---

- What do we need to do?
  - Get password on user record
  - Send to Google

Oh, and in a secure manner



# CAPTURING THE CHANGE

---

/Library/Preferences/com.apple.passwordserver

▼ Root	Dictionary	↕ 17 key/value pairs
BadTrialDelay	Number	↕ 0
▶ Debug Log Options	Dictionary	↕ 2 key/value pairs
DeleteWaitInMinutes	Number	↕ 2
ExternalCommand	String	↕ record_password.sh
KerberosCacheLimit	Number	↕ 95,000
▶ ListenerInterfaces	Array	↕ 3 ordered objects
▶ ListenerPorts	Array	↕ 2 ordered objects
PassiveReplicationOnly	Boolean	↕ NO
Preference File Version	Number	↕ 3
ProvideReplicationOnly	Boolean	↕ NO

External Command relative to /usr/sbin/authserver/tools/



# GETTING PASSWORD ON USER RECORD

---

```
# Get password from stdin. This will be the password change running through password server.
read password

# Hash the password using the SHA1 method and store into "password".

password=`echo -n $password | /usr/bin/openssl dgst -sha1 -hex`

# Create LDIF file for LDAP modification. This will import the value into LDAP attribute "pager".
# If you wish to change the attribute, change both instances of pager. Also, make sure to keep the
# \n inplace as currently formatted.
#
# REQUIRED CHANGES: specify your domain below, replacing dc=YOUR,dc=DOMAIN

LDIFMOD="/usr/sbin/authserver/tools/modify.ldif"
touch $LDIFMOD
echo -e "dn: uid=$1,cn=users,dc=YOUR,dc=DOMAIN\nchangetype: modify\nreplace: pager\npager: $password" > $LDIFMOD

# ldapmodify command to import previously generated LDIF file back into directory.
# You will need to specify an account with admin rights to your LDAP database here.
#
# REQUIRED CHANGES: admin username for uid=SOMEADMIN.
#                      Domain information replaing dc=YOUR,dc=DOMAIN
#                      password for user with write access for PASSWORD

ldapmodify -xD uid=SOMEADMIN,cn=users,dc=YOUR,dc=DOMAIN -w PASSWORD -f $LDIFMOD -v

# Remove LDIF file for security purposes.

rm $LDIFMOD
```



# SENDING CHANGE TO GOOGLE APPS

---

- Google Apps Directory Sync
  - Windows XP, Vista, Solaris, Linux
- Configurable on a schedule
- Execute from password change script



# SENDING CHANGE TO GOOGLE APPS

Workgroup Manager: d30odm.district30.k12.il.us

Server Admin Accounts Preferences New User Delete Refresh New Window Search

Authenticated as rsaeks to directory: /LDAPv3/127.0.0.1

Basic Privileges Advanced Groups Home Mail Print Info Windows Inspector

Filter: Record Size: 257.06 KB

Name	Size	Value
EmailAddress	21 bytes	rsaeks@district30.org
FirstName	7 bytes	Randall
GeneratedUID	36 bytes	9CF805AA-DF1E-479D-
HomeDirectory	94 bytes	<home_dir> <url>afp://
IMHandle	39 bytes	JABBER:rsaeks@chat.district30.k12.il.u
JPEGPhoto	254.69 KB	<Non-Text Value>
Keywords	7 bytes	lsadmin
LastName	5 bytes	Saeks
MCXFlags	275 bytes	<?xml version="1.0"
NFSHomeDirectory	74 bytes	/Network/Servers/
PagerNumber	40 bytes	e1a150def3211726a894bc0b7977f54
Password	8 bytes	*****
PhoneNumber	12 bytes	847 400 8957
PostalCode	5 bytes	60062
PrimaryGroupID	2 bytes	80
PrintServiceUserData	698 bytes	<?xml version="1.0"

Options... Edit... New Value... New Attribute...

Presets: Maple Staff Revert Save

1 of 1 user selected



# SECURITY WARNING!

---

- Protect file system access to script!
- Use Directory Access Controls (DACs)





# GOOGLE APPS DIRECTORY SYNC

## Google Apps Directory Sync General Settings



Before you first use Google Apps Directory Sync, enable the Provisioning API in your Google Apps control panel:

1. Log in to your Google Apps administrator control panel.
2. Click **Users and Groups** from the top menu, and then click the **Settings** tab.
3. Check the box labeled **Enable Provisioning API**.
4. Click **Save Changes**.

Specify which categories of objects to synchronize. [Learn More](#)

### Synchronization of Google Organizations (from LDAP Org Units)

- ☐ Sync LDAP Org Units, and move users into Google Organizations, as specified in the User Sync Rules
- ☐ Do not create or delete Google Organizations, but move users between existing Organizations, as specified in the User Sync Rules
- ☒ Ignore any Google Organization information  
(Any new users are created in the default Google Organization)

Synchronize:



Users



Groups



Profiles



Contacts



# DOMAIN SETTING

Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml

File Windows Help

Configure

- General Settings
- Google Apps
  - Settings
  - Exclusion Rules
- LDAP Settings
  - LDAP Connection
  - Org Units
    - Search Rules
    - Exclusion Rules
  - Mappings
  - Users
    - Attributes
    - Extended Attributes
  - User Sync
    - Exclusion Rules
  - Groups
    - Group Search Rules
    - Exclusion Rules
  - User Profiles
    - Attributes
  - User Profiles Sync
    - Exclusion Rules
  - Shared Contacts
    - Attributes
  - Contacts Sync
    - Exclusion Rules
- Notifications
- Delete Limits
- Log Files

Test

- Simulate Sync

## Google Apps Settings

Enter connection information for your Google Apps account. You can synchronize to all the domains your Google Account is configured to administer. [Learn More](#)

Admin Email Address:   
for example, admin@example.com

Admin Password:

Primary Domain Name:

☐ Replace domain names in LDAP email addresses (of users and groups) with this domain name.

If your firewall uses a proxy to access external websites, enter the information for the SSL Proxy. If you use different proxies for HTTP and HTTPS connections, also enter the HTTP Proxy information.

SSL Proxy (used to connect to Google Apps)	HTTP Proxy (if different from the SSL proxy)
Host Name: <input type="text"/>	Host Name: <input type="text"/>
Port: <input type="text"/>	Port: <input type="text"/>
User Name (if required): <input type="text"/>	User Name (if required): <input type="text"/>
Password (if required): <input type="text"/>	Password (if required): <input type="text"/>

← Previous

→ Next



# EXCLUSION RULES

Google Apps Directory Sync - Untitled-1.xml

File Windows Help

Configure

- General Settings
- Google Apps
  - Settings
  - Exclusion Rules
- LDAP Settings
  - LDAP Connection
- Org Units
  - Search Rules
  - Exclusion Rules
  - Mappings
- Users
  - Attributes
  - Extended Attributes
  - User Sync
    - Exclusion Rules
- Groups
  - Group Search Rules
  - Exclusion Rules
- User Profiles
  - Attributes
  - User Profiles Sync
    - Exclusion Rules
- Shared Contacts
  - Attributes
  - Contacts Sync
    - Exclusion Rules
- Notifications
- Delete Limits
- Log Files

Test

- Simulate Sync

## Exclusion Rules for Google Apps

Unless you set up Exclusion Rules, Directory Sync removes any users and groups that are not on your LDAP server. To exclude a user or group from synchronization, add an exclusion rule for it. If you have multiple users or groups that match a pattern, you can enter a substring or regular expression, or add a separate rule for each item. [Learn More](#)

Type	Match Type	Rule
USER_NAME	SUBSTRING	@test.domain

☒ Add Exclusion Rule

Specify a user address, group name, or member address to exclude. An excluded member address is not removed from Google Apps groups. For examples, click the "Learn More" link on the previous page.

Type:  Match Type:

Exclusion Rule:

OK Cancel Apply

Previous Add Rule Next



# LDAP CONNECTION

Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\MacIT.xml

File Windows Help

Configure

- General Settings
- Google Apps
  - Settings
  - Exclusion Rules
- LDAP Settings
  - LDAP Connection**
  - Org Units
    - Search Rules
    - Exclusion Rules
    - Mappings
  - Users
    - Attributes
    - Extended Attributes
    - User Sync
      - Exclusion Rules
  - Groups
    - Group Search Rules
    - Exclusion Rules
  - User Profiles
    - Attributes
    - User Profiles Sync
      - Exclusion Rules
  - Shared Contacts
    - Attributes
    - Contacts Sync
      - Exclusion Rules
- Notifications
- Delete Limits
- Log Files

Test

- Simulate Sync

**LDAP Connection**

Specify information for how to connect to your LDAP directory server. [Learn More](#)

Connection Type: Standard LDAP

Host Name: 10.15.4.190

Port: 389

Base DN: dc=d30odm,dc=local

Authentication Type: Anonymous

Authorized User:

Password:

Previous Test Connection Next



# LDAP ATTRIBUTES, PT I

The screenshot shows the 'LDAP User Attributes' configuration window in Google Apps Directory Sync. The window title is 'Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml'. The left sidebar contains a tree view with categories: 'Configure' (General Settings, Google Apps, LDAP Settings, Org Units, Users, Groups, User Profiles, Shared Contacts, Notifications, Delete Limits, Log Files) and 'Test' (Simulate Sync). The 'Users' category is expanded, and 'Attributes' is selected. The main content area is titled 'LDAP User Attributes' and includes the Google logo. It contains instructions: 'Select your LDAP Server Type, and enter the LDAP attribute names to use in the synchronization. If your LDAP server stores aliases in multiple attributes, enter attribute names one at a time, and click Add for each. For mailing lists, enter the attribute that contains the email address, such as "mail". [Learn More](#)'. Below the instructions are two input fields: 'Server Type' (a dropdown menu set to 'OpenLDAP') and 'Email Address Attribute' (a text box containing 'mail'). To the right of these is a section for 'Alias Address Attributes' with a text box, an 'Add' button, and a 'Remove' button. Below the 'Add' button is a large, empty list box with scrollbars. At the bottom of the window are three buttons: 'Previous', 'Use Defaults', and 'Next'.

Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml

File Windows Help

Configure

- General Settings
- Google Apps
  - Settings
  - Exclusion Rules
- LDAP Settings
  - LDAP Connection
  - Org Units
  - Users
    - Attributes**
    - Extended Attributes
    - User Sync
      - Exclusion Rules
  - Groups
    - Group Search Rules
    - Exclusion Rules
  - User Profiles
    - Attributes
    - User Profiles Sync
      - Exclusion Rules
  - Shared Contacts
    - Attributes
    - Contacts Sync
      - Exclusion Rules
- Notifications
- Delete Limits
- Log Files

Test

- Simulate Sync

**LDAP User Attributes**

Select your LDAP Server Type, and enter the LDAP attribute names to use in the synchronization. If your LDAP server stores aliases in multiple attributes, enter attribute names one at a time, and click Add for each. For mailing lists, enter the attribute that contains the email address, such as "mail". [Learn More](#)

Server Type: OpenLDAP

Email Address Attribute: mail

Alias Address Attributes:

Add

Remove

Previous Use Defaults Next



# LDAP ATTRIBUTES, PT II

## LDAP Extended Attributes



Enter optional LDAP attributes to synchronize additional user settings in Google Apps. Note that some password encoding formats are not supported. [Learn More](#)

Given Name Attribute:

Family Name Attribute:

Mailbox Quota Size Attribute:

### User Password Sync

Synchronize Passwords ☐ Only for new users ☒ For new and existing users

Password Attribute:

Password Encryption Method: ☒ SHA1 ☐ MD5 ☐ Plaintext

☐ Force new users to change password.

Default password for new users:

### Google Apps Users Deletion / Suspension Policy

- ☐ Delete only active Google Apps users not found in LDAP (suspended users are retained).
- ☐ Delete active and suspended Google Apps users not found in LDAP.
- ☒ Suspend Google Apps users not found in LDAP, instead of deleting them.

[← Previous](#)

[→ Next](#)



# USER SYNC OPTIONS, PT I

The screenshot shows the 'Google Apps Directory Sync' application window. The title bar reads 'Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml'. The menu bar includes 'File', 'Windows', and 'Help'. On the left is a blue sidebar with a tree view containing categories like 'Configure' (General Settings, Google Apps, LDAP Settings, Org Units, Users, Groups, User Profiles, Shared Contacts, Notifications, Delete Limits, Log Files) and 'Test' (Simulate Sync). The 'Users' category is expanded, and 'User Sync' is selected.

The main pane is titled 'LDAP User Sync' and features the Google logo. It contains a descriptive paragraph and a table of sync rules. A dialog box titled 'Edit LDAP User Sync Rule' is open in the foreground.

**LDAP User Sync**

Specify which users to import and synchronize. Other users are deleted or suspended. These rules use LDAP query notation. To match all users, enter(objectclass=user). Search rules apply in the order they appear in the table. [Learn More](#)

Active / Suspended User...	Org Name/Org Mapping ...	Scope	Filter	Base DN Override				
Active	[derived]	SUBTREE	(objectclass=inetOrgPer...	cn=users,dc=d30odm,d...	+	+		

**Edit LDAP User Sync Rule**

Import users that match this LDAP rule. For examples, click the "Learn More" link on the previous page.

☐ Suspend these users in Google Apps

Scope: Sub-tree

Rule: (objectclass=inetOrgPerson)

Base DN: cn=users,dc=d30odm,dc=local  
(leave blank to use the Base DN from the "LDAP Connection" page)

OK Cancel Apply

Previous Next



# USER SYNC OPTIONS, PT II

☒ Add LDAP User Sync Rule

Import users that match this LDAP rule. For examples, click the "Learn More" link on the previous page.

Place users in the following Google Apps Org Unit:

☒ Org Unit based on Org Units Mappings and DN

☐ Org Unit Name:

☐ Org Unit Name defined by this LDAP attribute:

☐ Use default filter

Scope:

Rule:

Base DN:

(leave blank to use the Base DN from the "LDAP Connection" page)



# DELETE LIMITS

The screenshot shows the 'Delete Limits' configuration window of the Google Apps Directory Sync application. The window title is 'Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml'. The left sidebar contains a tree view with categories: 'Configure' (General Settings, Google Apps, LDAP Settings, Groups, User Profiles, Shared Contacts, Notifications, Delete Limits, Log Files) and 'Test' (Simulate Sync). The 'Delete Limits' option is highlighted. The main content area has the Google logo and a heading 'Delete Limits'. Below the heading is a paragraph explaining the delete limits: 'Specify limits on delete operations. Check the appropriate boxes and enter values for the checked items to activate delete limits. If no delete limits are specified the default becomes 5%. If sync operation would reach the delete limit, no actions are performed and the sync operation terminates. [Learn More](#)'. The configuration section is titled 'Do not synchronize if the delete limit would be exceeded:' and contains two radio button options. The first option, 'Delete no more than 5 % of organizations or users.', is unselected. The second option, 'Delete no more than 1 organizations or users.', is selected. At the bottom of the window are 'Previous' and 'Next' navigation buttons.

Google Apps Directory Sync - C:\Program Files\Google Apps Directory Sync\WacIT.xml

File Windows Help

Configure

- General Settings
- Google Apps
  - Settings
  - Exclusion Rules
- LDAP Settings
  - LDAP Connection
  - Org Units
  - Users
    - Attributes
    - Extended Attributes
  - User Sync
    - Exclusion Rules
- Groups
  - Group Search Rules
    - Exclusion Rules
- User Profiles
  - Attributes
  - User Profiles Sync
    - Exclusion Rules
- Shared Contacts
  - Attributes
  - Contacts Sync
    - Exclusion Rules
- Notifications
- Delete Limits**
- Log Files

Test

- Simulate Sync

**Delete Limits**

Specify limits on delete operations. Check the appropriate boxes and enter values for the checked items to activate delete limits. If no delete limits are specified the default becomes 5%. If sync operation would reach the delete limit, no actions are performed and the sync operation terminates. [Learn More](#)

Do not synchronize if the delete limit would be exceeded:

☐ Delete no more than 5 % of organizations or users.

☒ Delete no more than 1 organizations or users.

Previous Next



# OTHER SYNC SETTINGS

---

- Groups
- Profile data
- Shared Contact data
- Email notifications of sync status



# SYNC

---

- Run manually
- Run via schedule task or cron job
- Command in password change script



# SAML

---

- Similar to Kerberos for web
- Requires an IdP (OD) and SP (Google)
- Extensible to other products using this architecture



# PRE-REQUISITES

---



# PRE-REQUISITES

---

- Users present in Google Apps



# PRE-REQUISITES

---

- Users present in Google Apps
  - Import via CSV
  - Use Provisioning Toolkit to create and delete users from LDAP.



# CSV IMPORT

---

eMail Address	First Name	Last Name	Password
<u>UserAy@example.com</u>	User	Ay	,alas
<u>UserBee@example.com</u>	User	Bee	honey
<u>UserSea@example.com</u>	User	Sea	OldMan&



# PROVISIONING TOOLKIT

---

- VMWare image
- Does the heavy work for you
- Queries LDAP to creates accounts
- Specifies default password



# PROVISIONING TOOLKIT

---

- Required Configuration Information:
  - Google Apps Domain
  - Database Type (LDAP)
  - LDAP server and mappings
  - Default Password for users



# GOOGLE APPS PROVISIONING TOOLKIT

---

- Free Download from SADA Systems  
Link on <http://techrecess.com/mactech>



# PROVISIONING TOOLKIT CONFIGURATION

---

```
***** GoogleApps Domain Variables *****#
//domain name
$domain = 'YOUR.DOMAIN';
#domain administrator account and password
$admin = 'SOME_Admin';
$password = 'SOME_Password';

//Permanently delete user accounts
$allow_account_deletion = 'no';

***** Database Settings *****#
DEFINE('DB_TYPE', 'ldap');

***** LDAP Settings *****#
// ldap server
DEFINE('LDAP_SERVER', 'LDAPHOST'); // use ldaps://hostname/ for connetion over SSL
// ldap port
DEFINE('LDAP_PORT', '389'); // 389 is default
// ldap protocol option
DEFINE('LDAP_PROTOCOL', '3'); // 3 is default
// ldap referrals option
DEFINE('LDAP_REFERRALS', '0'); // 0 is default
// bind rdn
DEFINE('LDAP_BIND_RDN', 'uid=SOMEUSER,cn=users,DC=d30odm,DC=local');
// bind password
DEFINE('LDAP_BIND_PASSWORD', 'SOMEPassword');
// base dn for search
DEFINE('LDAP_BASE_DN', 'CN=users,DC=d30odm,DC=local');
// search filter
// example: '(&(objectclass=person)(mailnickname=*)(cn=*)(sn=*))'
DEFINE('LDAP_FILTER', '(uid=rsaeks)');
// username
DEFINE('LDAP_USERNAME', 'uid');
// first name
DEFINE('LDAP_FIRSTNAME', 'givenname');
// last name
DEFINE('LDAP_LASTNAME', 'sn');
```



# PROVISIONING TOOLKIT

## CONFIGURATION, CONT

---

```
// Define how Password will be generated when LDAP is used
// Valid entries:
// default: One default password for all users, defined in the DEFAULT_PASSWORD variable
// field: One field or a combination of fields, defined in the $field variable bellow
DEFINE('LDAP_PASSWORD', 'default');

DEFINE('LDAP_DEFAULT_PASSWORD', 'default_password'); // Default password for all users if LDAP_PASSWORD = 'default' is 'default_password'

if (LDAP_PASSWORD == 'field') {
    // Add LDAP field names to the array bellow if you wish to use a readable field or a combination of readable fields. List in order to be combined.
    // Alternative, you can generate $field by writting a custom function.
    $field = array('sn');
}
```



# PROVISIONING TOOLKIT CONFIGURATION, CONT

---

```
// Define how Password will be generated when LDAP is used
// Valid entries:
// default: One default password for all users, defined in the DEFAULT_PASSWORD variable
// field: One field or a combination of fields, defined in the $field variable bellow
DEFINE('LDAP_PASSWORD', 'default');

DEFINE('LDAP_DEFAULT_PASSWORD', 'default_password'); // Default password for all users if LDAP_PASSWORD = 'default' is 'default_password'

if (LDAP_PASSWORD == 'field') {
    // Add LDAP field names to the array bellow if you wish to use a readable field or a combination of readable fields. List in order to be combined.
    // Alternative, you can generate $field by writting a custom function.
    $field = array('sn');
}
```

- Once toolkit is configured, navigate to <http://ip/GoogleAppsToolKit/admin/>
- Walks you through process with options



# SIMPLESAMLPHP

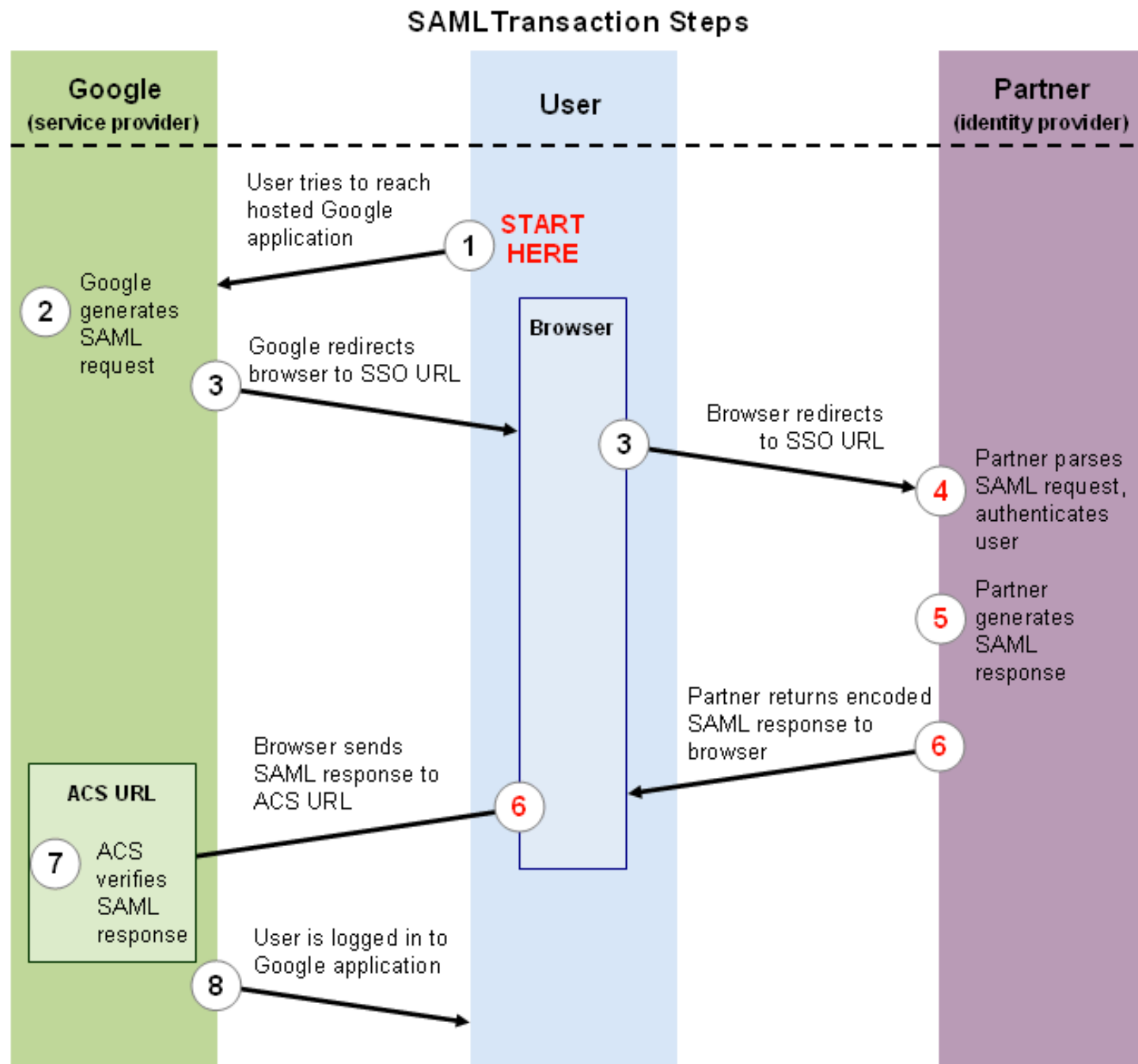
---

- Open-source PHP SAML solution
- Download from:
  - <http://simplesamlphp.org/>



# SAML OVERVIEW

Figure 1: Logging in to Google Apps using SAML





# INSTALLATION

---

- Unpack files
- Create web alias in Server Admin (SA)
- Enable php module in SA



# /CONFIG/CONFIG.PHP

---

- Set Administrative Password
- Hash Value
- Technical Contact
- Enabled Services
  - 'enable.saml20-idp' => true,



# /CONFIG/CONFIG.PHP

```
* This password will give access to the installation page of simpleSAMLphp with
* metadata listing and diagnostics pages.
*/
'auth.adminpassword'      => 'SECUREPASS',
'admin.protectindexpage'  => false,
'admin.protectmetadata'   => false,

/**
 * This is a secret salt used by simpleSAMLphp when it needs to generate a secure hash
 * of a value. It must be changed from its default value to a secret value. The value of
 * 'secretsalt' can be any valid string of any length.
 *
 * A possible way to generate a random salt is by running the following command from a unix shell:
 * tr -c -d '0123456789abcdefghijklmnopqrstuvwxyz' </dev/urandom | dd bs=32 count=1 2>/dev/null;echo
 */
'secretsalt' => 'hf29fmsl01nfla02na',

/*
 * Some information about the technical persons running this installation.
 * The email address will be used as the recipient address for error reports, and
 * also as the technical contact in generated metadata.
 */
'technicalcontact_name'   => 'Randy Saeks',
'technicalcontact_email' => 'rsaeks@district.org',

/*
 * Enable
 *
 * Which functionality in simpleSAMLphp do you want to enable. Normally you would enable only
 * one of the functionalities below, but in some cases you could run multiple functionalities.
 * In example when you are setting up a federation bridge.
 */
'enable.saml20-sp'        => false,
'enable.saml20-idp'       => true,
'enable.shib13-sp'        => false,
'enable.shib13-idp'       => false,
'enable.wsfed-sp'         => false,
'enable.openid-provider' => false,
'enable.authmemcookie'    => false,
```



# ENABLE SAML LDAP

---

- Navigate to modules directory > LDAP
- Enable by placing file

```
touch /path/to/saml/modules/ldap/enable
```



# SECURING THE TRUST

---

- Generate RSA keys
- Upload .crt to Google Apps



# /CONFIG/LDAP.PHP

---

- Specify dn pattern
- LDAP host
- attributes to retrieve

```
'auth.ldap.dnpattern'    => 'uid=%username%,cn=users,dc=d30odm,dc=local',  
'auth.ldap.hostname'    => '10.15.4.190',  
'auth.ldap.attributes'  => null,  
'auth.ldap.enable_tls'  => false,
```



# **/METADATA/SAML20-IDP- HOSTED.PHP**

---



# /METADATA/SAML20-IDP- HOSTED.PHP

---

- Define Entity ID
- Define Host
- Specify Certificates previously created

```
$metadata = array(  
  
    // The SAML entity ID is the index of this config.  
    'd30svcs.district30.org' => array(  
  
        // The hostname of the server (VHOST) that this SAML entity will use.  
        'host'                => 'd30svcs.district30.org',  
  
        // X.509 key and certificate. Relative to the cert directory.  
        'privatekey'          => 'googleappsidp.pem',  
        'certificate'          => 'googleappsidp.crt',  
  
        // Authentication plugin to use. login.php is the default one that uses LDAP.  
        'auth'                 => 'auth/login.php',  
        'authority'            => 'login'  
    )  
);
```



# /METADATA/SAML2O-SP-REMOTE.PHP

---

- Create metadata array
- Define ACS
- Set nameid format
- Define nameid attribute

```
$metadata['google.com'] = array(  
    'AssertionConsumerService' => 'https://www.google.com/a/district30.org/acs',  
    'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:email',  
    'singlesaml.nameidattribute' => 'mail', /* uid for rsaeks: mail for rsaeks@district30.org */  
    'singlesaml.attributes' => false  
);
```



# NAMEID ATTRIBUTE

---

- Defines attribute passed to Google Apps once user and password verified
- Can be any LDAP attribute
- Single domain setups can use uid
- Subdomains should use attribute specifying user@domain



# SECURITY WARNING!

---

- Limit your Directory Admins
- nameidattribute will be your linked Google Apps Account





# CONFIGURING GOOGLE APPS FOR SAML

---

- Advanced Tools in cpanel -> SSO
- Sign-In page
- Sign-Out page
  - Can specify a redirect with ?  
RelayState=URL
- Network Mask (Good for testing!)



# CONFIGURING GOOGLE APPS FOR SAML

Dashboard	Organization & users	Groups	Domain settings	Advanced tools	Support	Service settings ▾
-----------	----------------------	--------	-----------------	----------------	---------	--------------------

« [Back to Advanced tools](#)

## Set up single sign-on (SSO)

To set up SSO, please provide the information below. [SSO Reference](#)

☒ **Enable Single Sign-on**

**Sign-in page URL \***  
 URL for signing in to your system and Google Apps

**Sign-out page URL \***  
 URL to redirect users to when they sign out

**Change password URL \***  
 URL to let users change their password in your system

**Verification certificate \***  
A certificate file has been uploaded-[Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. [Learn more](#)

☐ **Use a domain specific issuer**

This must be checked if your domain uses an IDP Aggregator to handle SAML requests.  
If enabled, the issuer value sent in the SAML request will be **google.com/a/district30.org** instead of simply **google.com** [Learn more](#)

**Network masks**

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network.  
Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16)  
For ranges, use a dash. Example: (64.233.167-204.99/32)  
All network masks must end with a CIDR. [Learn more](#)



# TESTING

---

- Include small IP range to test
- Login with one machine prior to enabling SSO
- Test with secondary machine



# LESSONS

---



# IN RELATION TO SETUP

---

- Having a test domain
- Determine service implementation and enablement schedule
- Access methods



# IN RELATION TO PASSWORDS

---

- Access methods determine passwords
- Find a web-based password reset
  - Built into 10.6 Server.



# IN RELATION TO USERS

---

- Establish a migration schedule
- Ample bandwidth for mail migration
- Calendar management