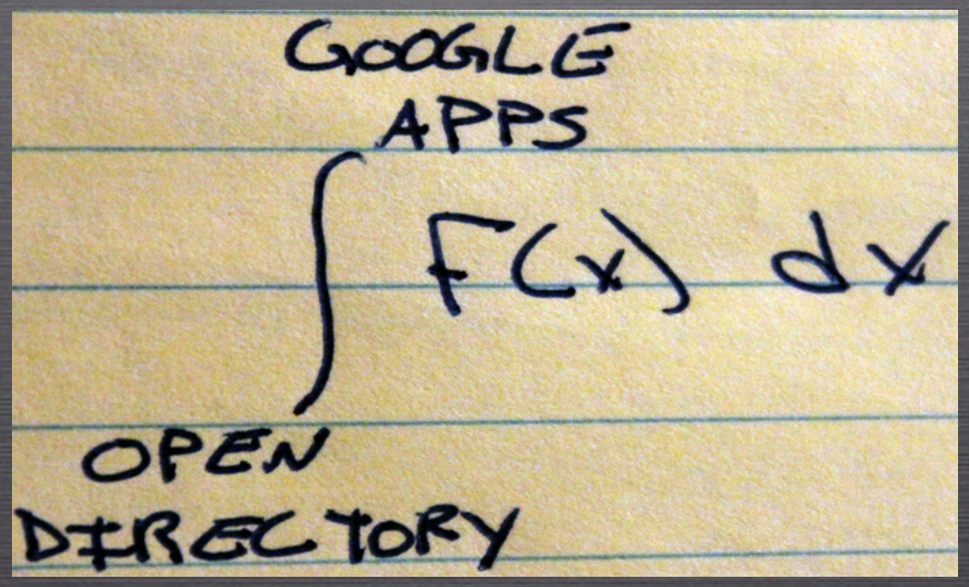
Google Apps and Open Directory



Randy Saeks

Twitter: @rsaeks

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

Keeping Current-ers

Whatever gets put on my desk

Single-handed reason local coffee shop is still open

... AND HERE

we are going to deploy Google Applications

we are looking to deploy Google Applications

A professional looking to learn more

I want to learn more about ways to leverage Open Directory

I want to bring a solution back to work

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

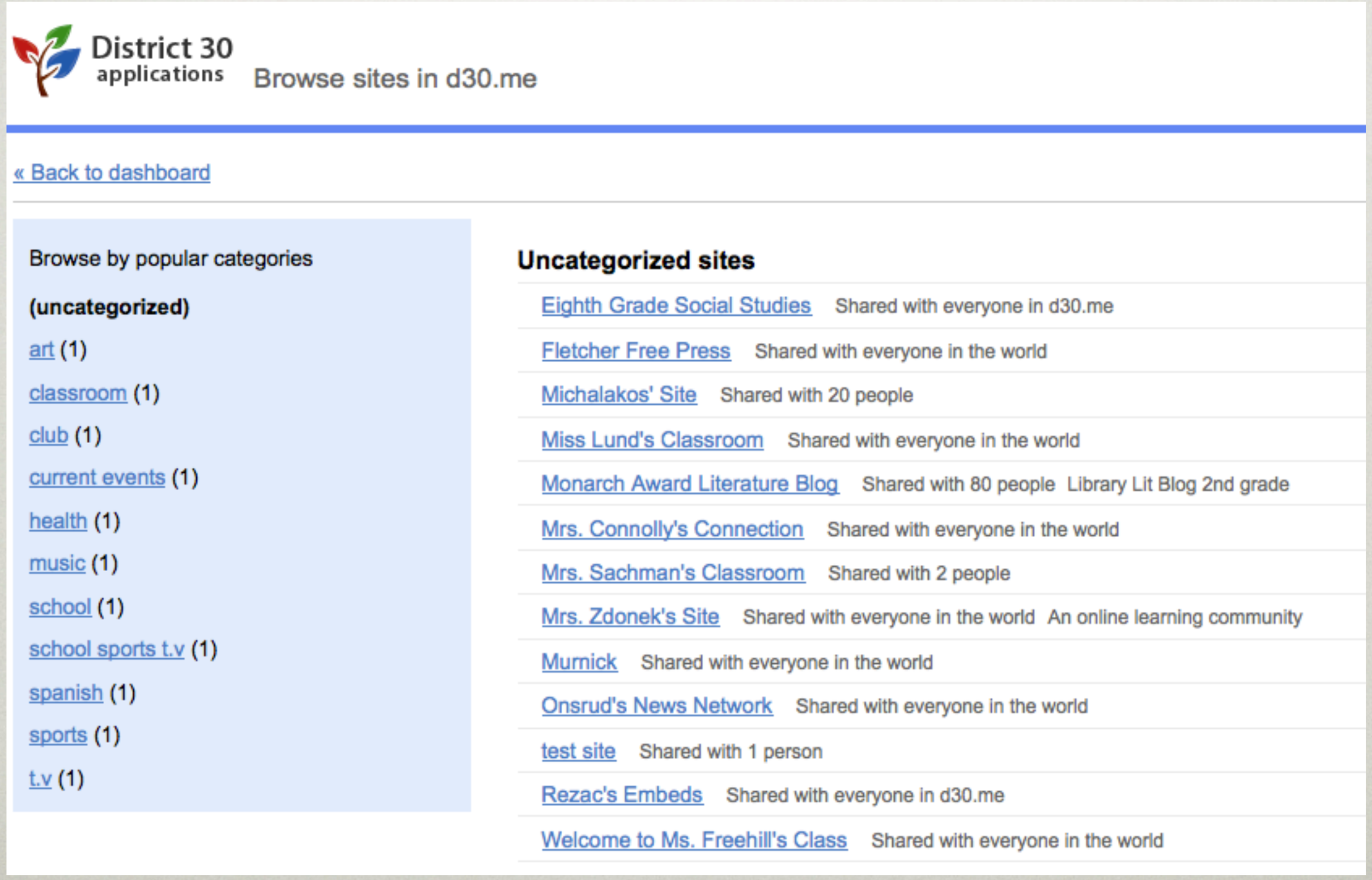
EMail

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

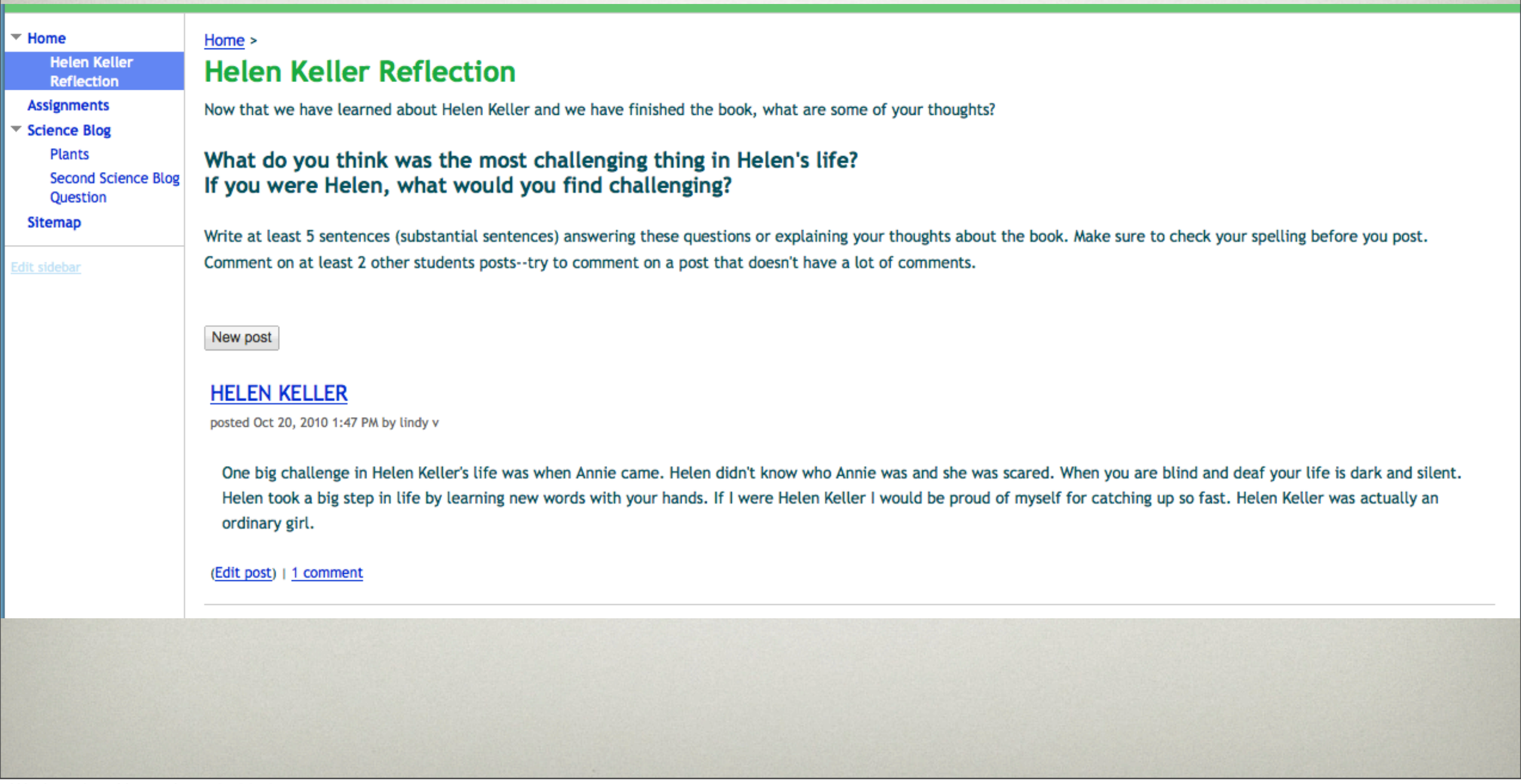
Sites

- 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

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/

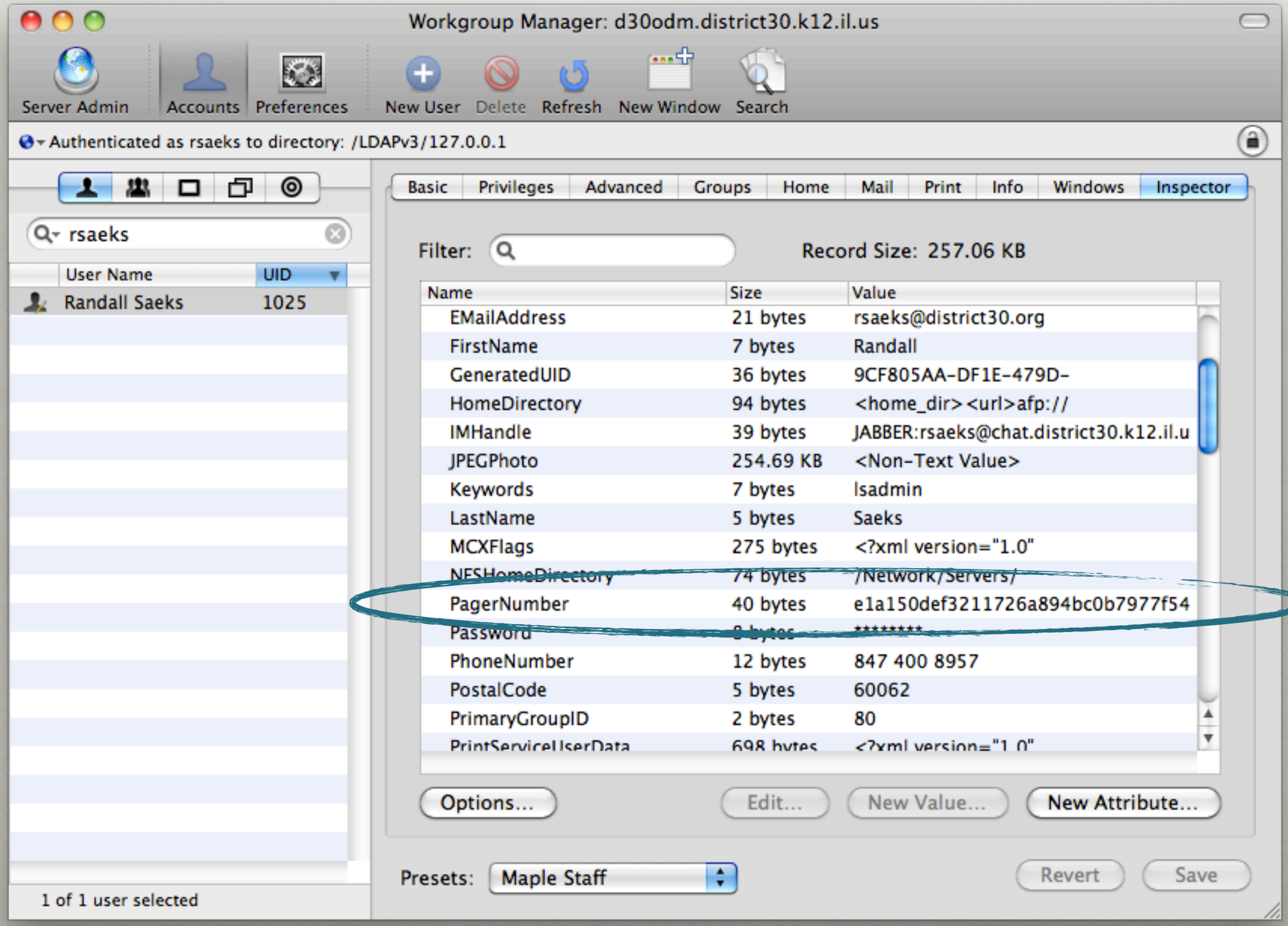
Getting Password on User Record

```
# 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.

srm $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



Security Warning!

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

Google Apps Directory Sync

Google Apps Directory Sync General Settings

Google

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**.

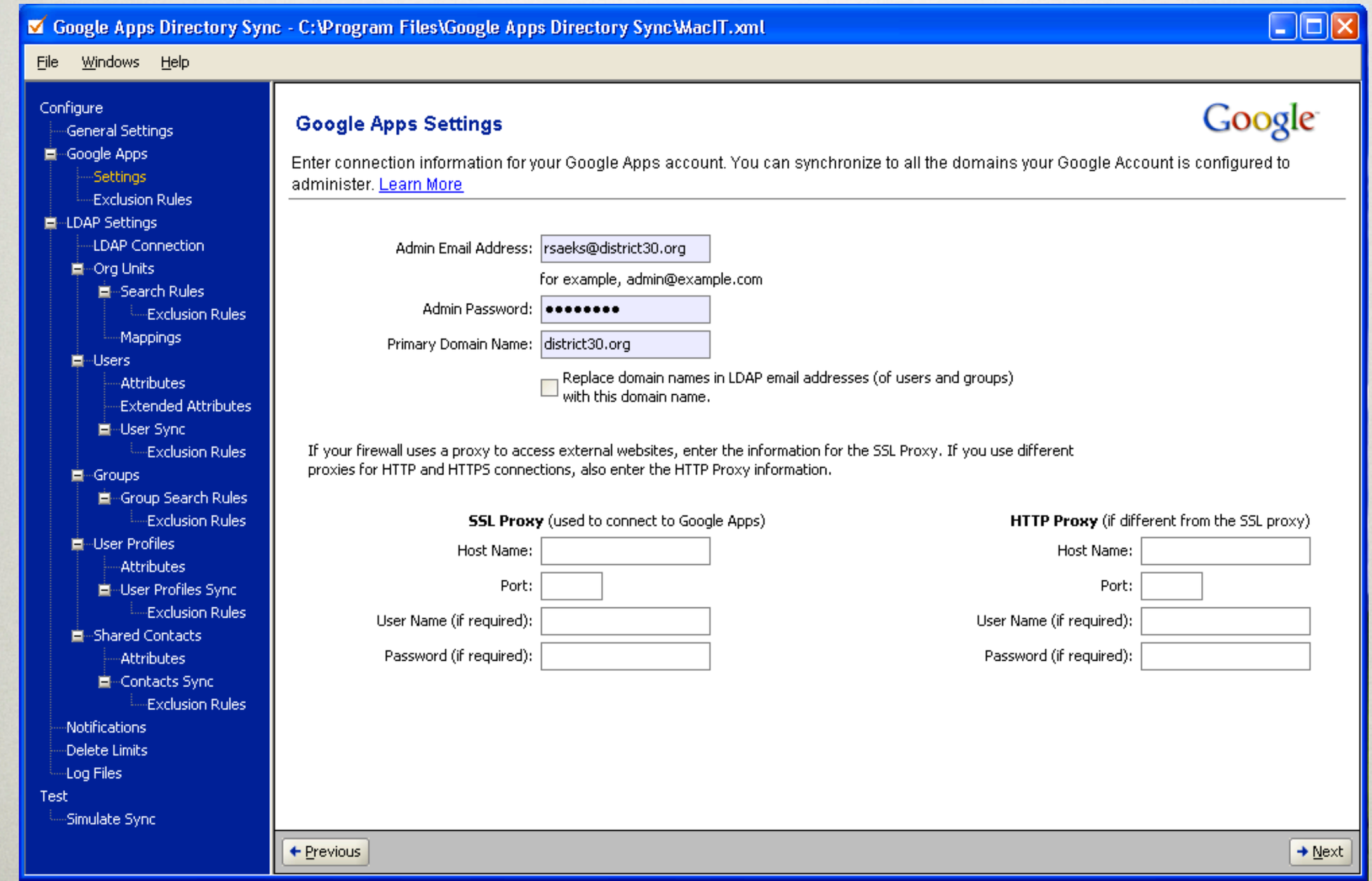
Specify which categories of objects to synchronize. Learn More

Synchronization of Google Organizations (from LDAP Org Units)

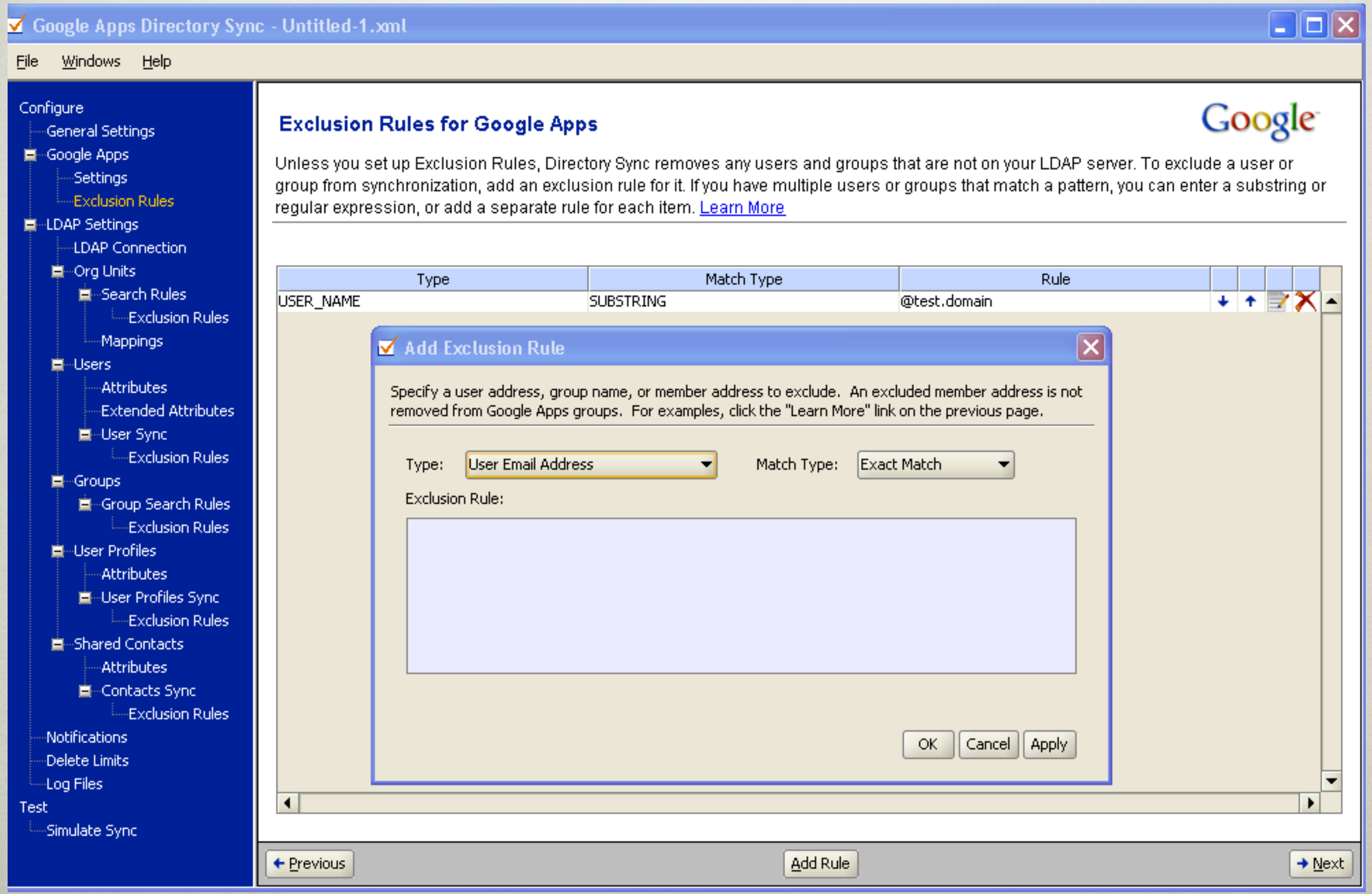
- ( ) Sync LDAP Org Units, and move users into Google Organizations, as specified in the User Sync Rules
- ( ) Do not create or delete Google Organizations, but move users between existing Organizations, as specified in the User Sync Rules
- (•) Ignore any Google Organization information (Any new users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

Synchronize: [ ] Users [ ] Groups [ ] Profiles [ ] Contacts

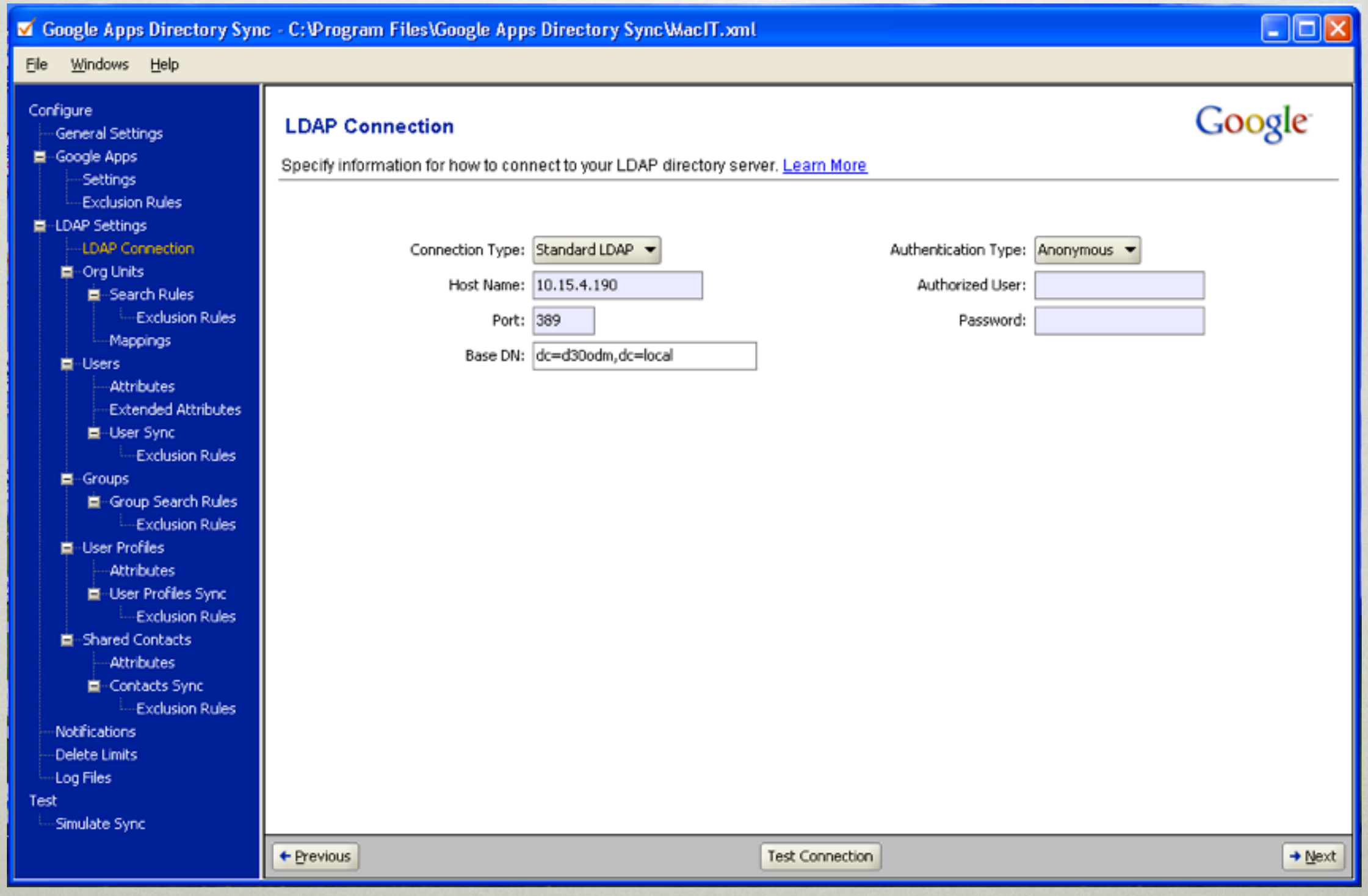
Domain Setting



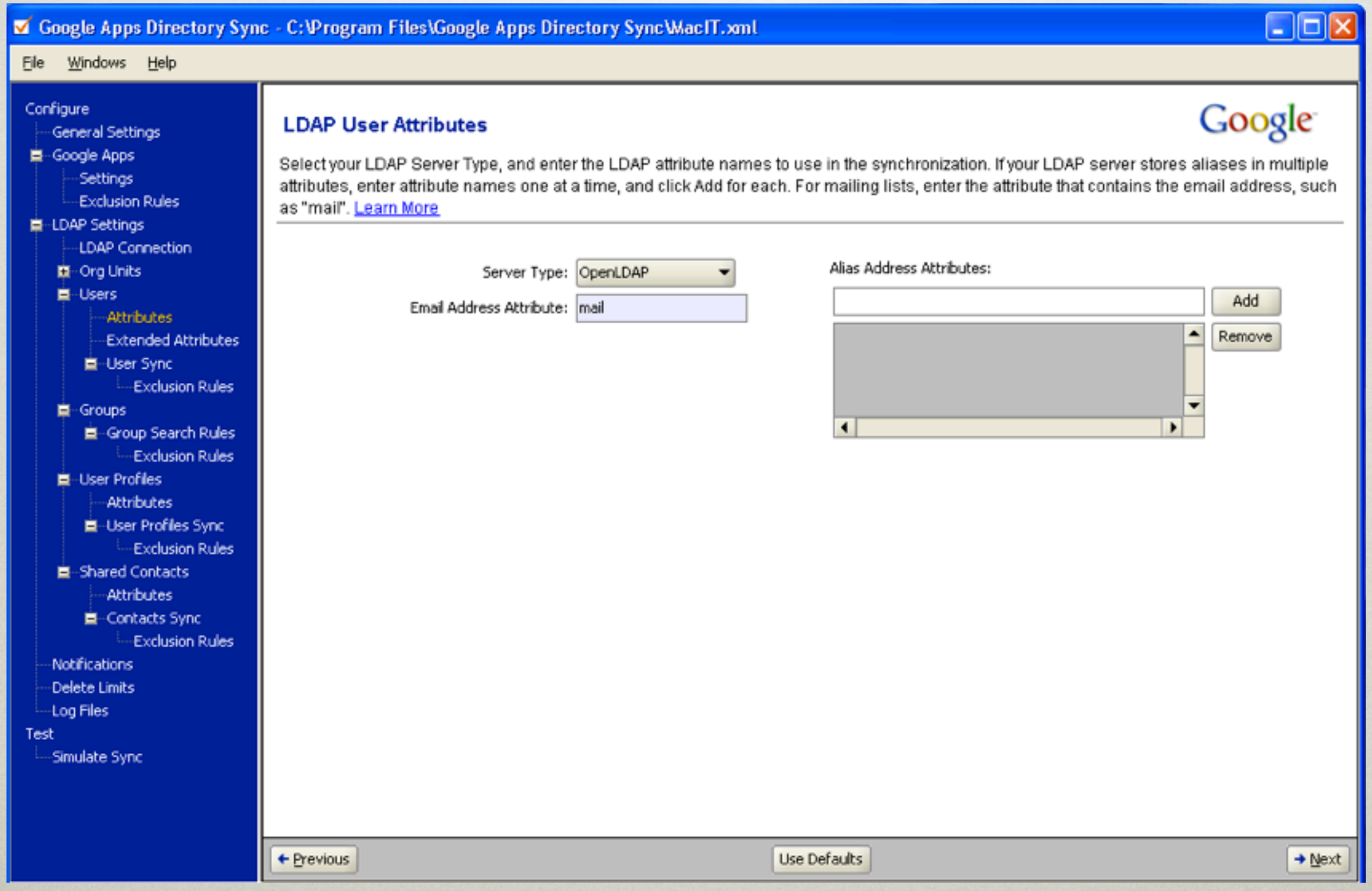
Exclusion Rules



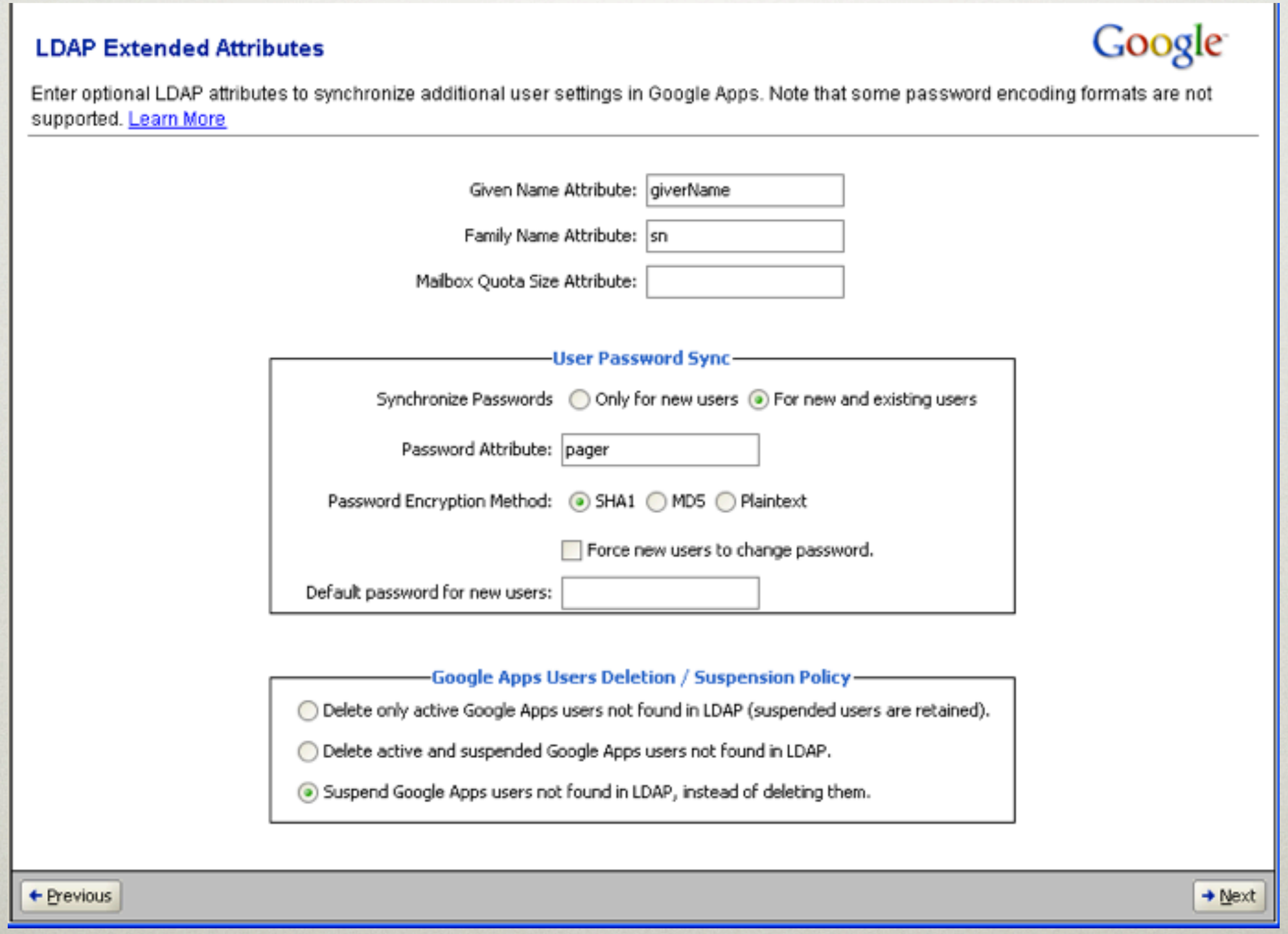
LDAP Connection



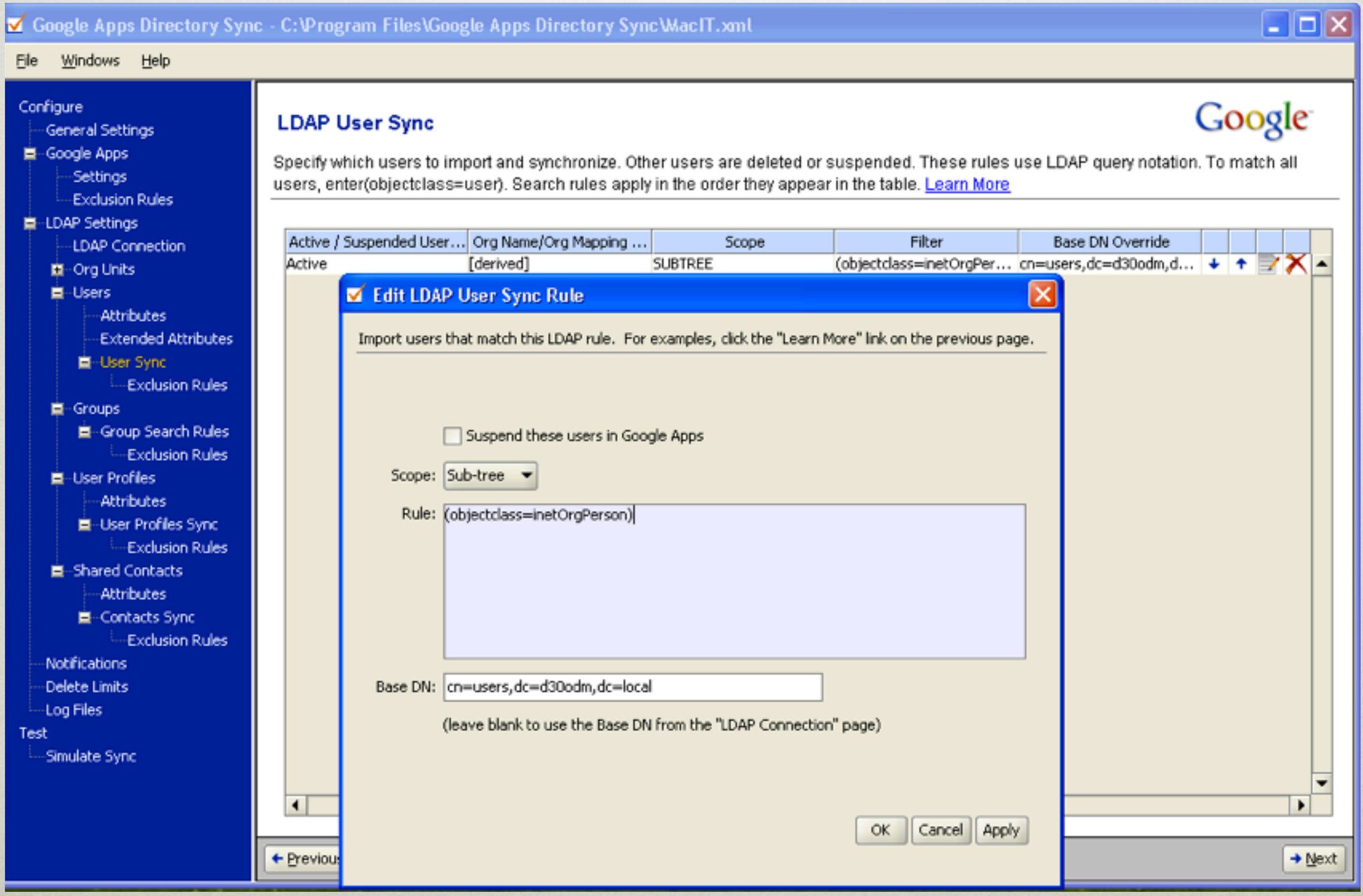
LDAP Attributes, PT I



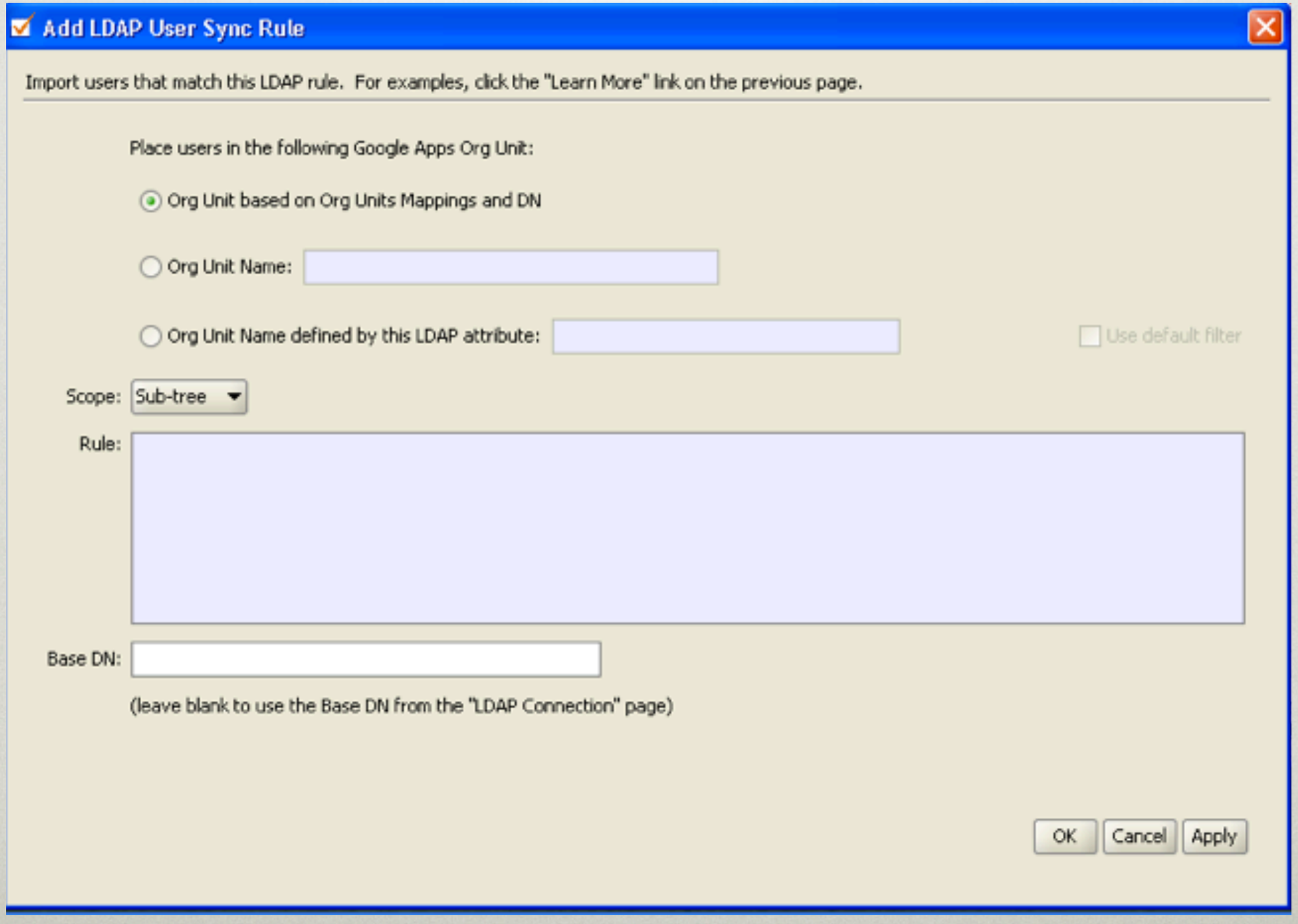
LDAP Attributes, PT II



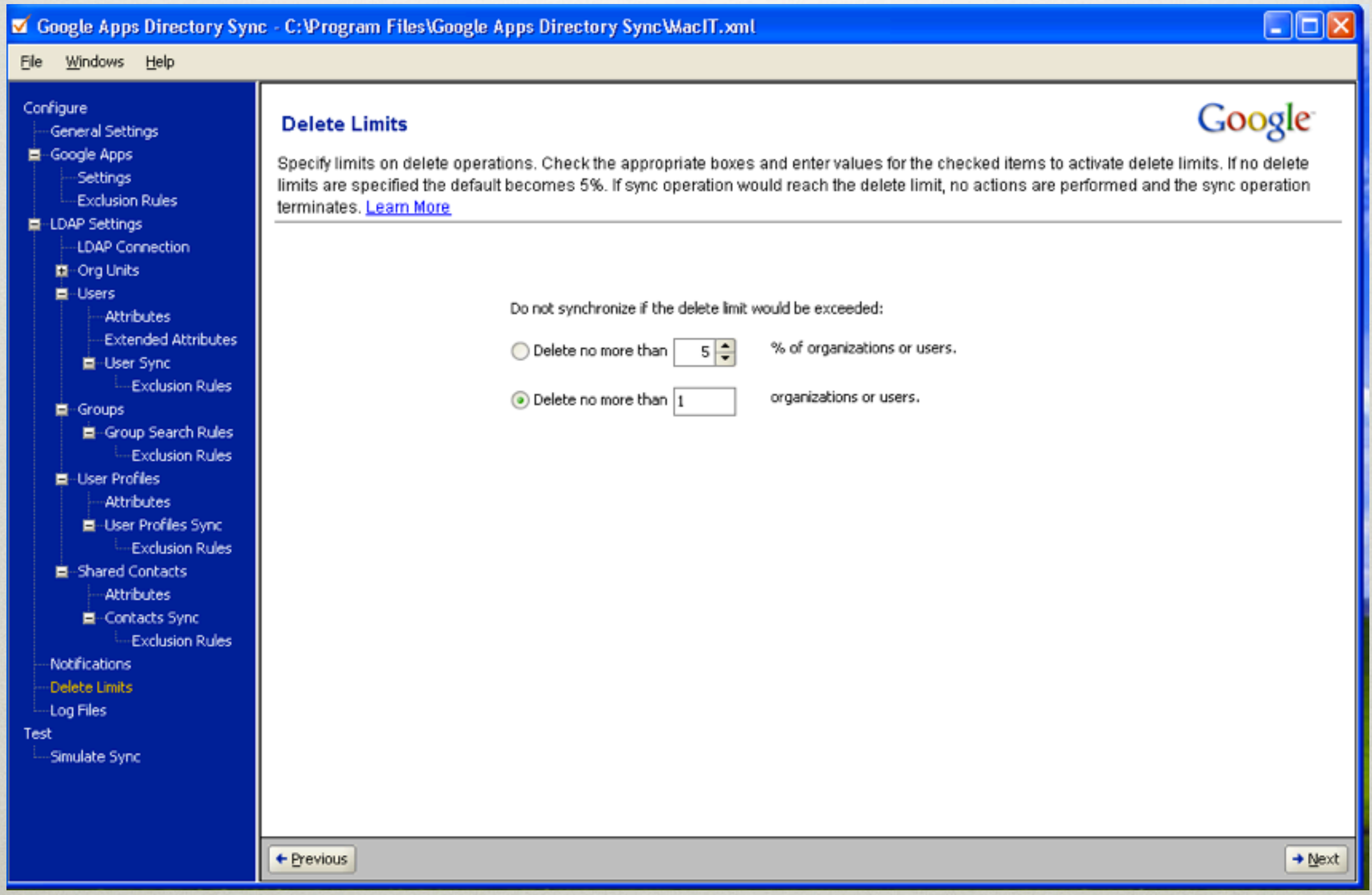
User Sync Options, Pt I



User Sync Options, Pt II



Delete Limits



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
UserAy@example.com	User	Ay	,alas
UserBee@example.com	User	Bee	honey
UserSea@example.com	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 wil 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 wil 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');
}
```

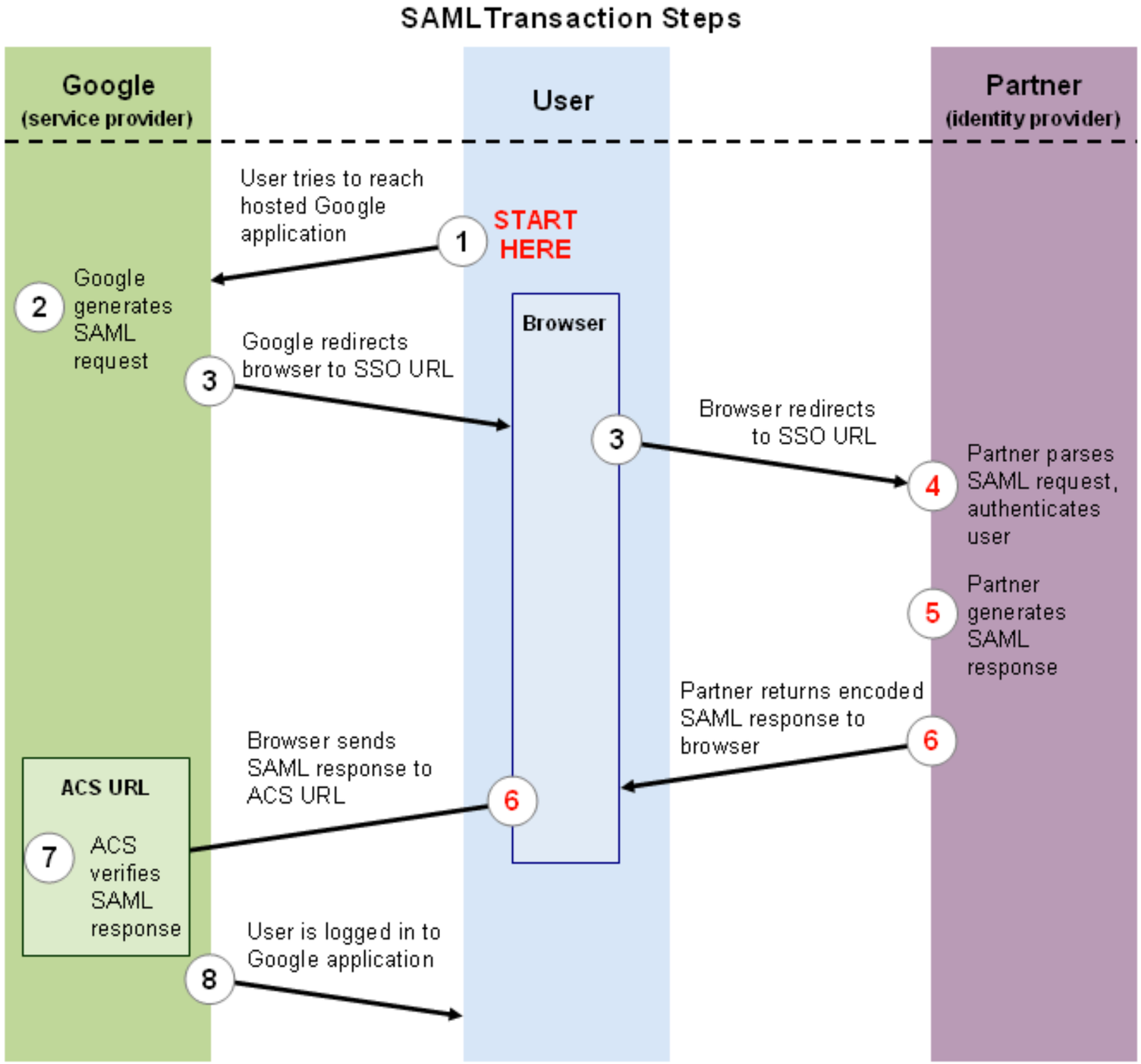
- Once toolkit is configured, navigate to http://ip/GoogleAppsToolKit/admin/
- Walks you through process with options

SimpleSAMLphp

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

SAML Overview

Figure 1: Logging in to Google Apps using SAML



Source: http://code.google.com/googleapps/domain/sso/saml_reference_implementation.html

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/saml20-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',
        'simplesaml.nameidattribute'    =>  'mail', /* uid for rsaeks: mail for rsaeks@district30.org */
        'simplesaml.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 *

https://d30svcs.district30.org/sso/saml2/idp/SSOService.php URL for signing in to your system and Google Apps

Sign-out page URL *

https://d30svcs.district30.org/sso/saml2/idp/initSLO.php?RelayS URL to redirect users to when they sign out

Change password URL *

https://d30odm.district30.org:443/changepassword 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

Save changes | Cancel

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