Summer Webinar Series
Google <-- SAML --> Zscaler Integration

Dianne Dunlap (ddunlap@mcnc.org, 919-248-8439)
Client Network Engineering

Webinar Links: www.mcnc.org/cne-webinars
Google<-SAML->Zscaler Integration Agenda

- What is “SAML”?  
- AAA, Testing, Switching Databases  
- Lab test setup  
- Authentication - Google configuration  
- Authentication – Zscaler configuration  
- Authorization – Google configuration  
- Authorization – Zscaler configuration  
- Accounting  
- AD  
- Caveats  
- Questions?
What is “SAML”?

Security Assertion Markup Language

XML-based, open-standard data format for exchanging authentication and authorization data between identity provider (IdP) and service provider (SP)

IdP=Google

SP=Dropbox, Facebook at Work, Docusign, Amazon Web Service, etc.

And SP…Zscaler!
Advantages of Google<<-SAML-> Integration

- Consolidation of users in one place instead of Google and Zscaler hosted database
- Fewer authentications
- One less username and password to remember, synchronized password changes
- Ability to add authentication to content-filtering at no cost
- Means to apply filtering policies by users’ category (authorization)
- Removes need for Active Directory or other on-premise directory for filtering
- Advantages of SAML over AD - fewer logins
Disadvantages of Google<-SAML-> Integration

- Login and a half (username twice, password once)
- SAML assertion cookies may be persistent depending on browser, device
AAA

A/authentication
- Who is the user?
- Google username/password only

A/authorization
- What is the user allowed to do?
- User’s membership in Google custom Department and/or Groups

A/accounting
- What did the user do?
- Zscaler logs
SAML - no AD
Considerations - Moving to SAML in Zscaler

1. If authorization, do we have rules in Zscaler?
2. Are accounts in Google?
3. Are there infrastructure devices to be excluded?
4. Do old accounts match new?
5. Can we test in a limited fashion?
6. Are there websites to be excluded?
7. Have users been trained?
## Authentication - Moving to SAML in Zscaler

![Zscaler Dashboard](image)

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>IP Addresses</th>
<th>VPN Credentials</th>
<th>XFF</th>
<th>Authentication</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ONE</td>
<td>152.48.31.89</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>High_School</td>
<td>152.48.31.229</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>Middle_School</td>
<td>152.48.31.250</td>
<td>---</td>
<td>---</td>
<td>Enabled</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>Elementary_School</td>
<td>152.48.31.251</td>
<td>---</td>
<td>---</td>
<td>Enabled</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>Other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>Enabled</td>
<td>---</td>
</tr>
<tr>
<td>6</td>
<td>Central Office</td>
<td>152.48.31.236</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>Guest</td>
<td>152.48.31.238</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
Authentication - Moving to SAML in Zscaler
Authentication - custom category exceptions in Zscaler - GRE/onsite
Authentication - authentication exceptions in Zscaler - GRE/onsite

- Enable Admin Ranking
- Allow Cascading to URL Filtering
- Session Timeout Duration: 30 Mins
- Bypassed URL Categories: Google
- Bypassed Applications: Google Analytics, Google Apps for Business
Authentication - SSL decryption exceptions in Zscaler - GRE/onsite
Pac file:

if(dnsDomainIs(host, "accounts.google.com")) return "DIRECT";

if(dnsDomainIs(host, "gmail.com")) return "DIRECT";
Lab test setup

k12gapps.mcnc.org, OU=PWM, more OUs below:
<table>
<thead>
<tr>
<th>Email</th>
<th>OU/orgUnitPath</th>
<th>Group/Group-email</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:9thWonder@k12gapps.mcnc.org">9thWonder@k12gapps.mcnc.org</a></td>
<td>/PWM/Adms</td>
<td><a href="mailto:admins@k12gapps.mcnc.org">admins@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td>2$<a href="mailto:Fabo@k12gapps.mcnc.org">Fabo@k12gapps.mcnc.org</a></td>
<td>/PWM/EastEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AlbertEinstein@k12gapps.mcnc.org">AlbertEinstein@k12gapps.mcnc.org</a></td>
<td>/PWM/MainEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:12Gauge@k12gapps.mcnc.org">12Gauge@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AlexanderGrahamBell@k12gapps.mcnc.org">AlexanderGrahamBell@k12gapps.mcnc.org</a></td>
<td>/PWM/SouthMStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AndersonPaak@k12gapps.mcnc.org">AndersonPaak@k12gapps.mcnc.org</a></td>
<td>/PWM/Hstudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:50Cent@k12gapps.mcnc.org">50Cent@k12gapps.mcnc.org</a></td>
<td>/PWM/WestEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:2Pistols@k12gapps.mcnc.org">2Pistols@k12gapps.mcnc.org</a></td>
<td>/PWM/EastETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:ActionBronson@k12gapps.mcnc.org">ActionBronson@k12gapps.mcnc.org</a></td>
<td>/PWM/Hteachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:40Glocc@k12gapps.mcnc.org">40Glocc@k12gapps.mcnc.org</a></td>
<td>/PWM/MainETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AndreNickatina@k12gapps.mcnc.org">AndreNickatina@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMTeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AlfredHitchcock@k12gapps.mcnc.org">AlfredHitchcock@k12gapps.mcnc.org</a></td>
<td>/PWM/SouthM Teachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AliVegas@k12gapps.mcnc.org">AliVegas@k12gapps.mcnc.org</a></td>
<td>/PWM/WestETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
</tr>
</tbody>
</table>
Authentication - Configuring Google SAML

Click to open the Google apps menu.

Click to go to the Admin console.
Authentication - Configuring Google SAML
Authentication - Configuring Google SAML
Authentication - Configuring Google SAML

No services/Apps configured for SAML.
Add a service/App to your domain
Authentication - Configuring Google SAML

Step 1
Enable SSO for SAML Application
Select an service/App for which you want to setup SSO

- Amazon Web Services
- BlueJeans
- Citrix GotoMeeting
- Docusign
- Dropbox
- Freshdesk
- Jive
- SETUP MY OWN CUSTOM APP
- Zcaler
Authentication - Configuring Google SAML

Step 2 of 5
Google IdP Information

Choose from either option to setup Google as your identity provider. Please add details in the SS0 config for the service provider.

Option 1
SS0 URL: https://accounts.google.com/o/saml2/idp?idpid=C00yab4ye
Entity ID: https://accounts.google.com/o/saml2/idp?idpid=C00yab4ye
Certificate: [DOWNLOAD]

Option 2
IDP metadata: [DOWNLOAD]

Copy this URL:
https://accounts.google.com/o/saml2/idp?idpid=C00yab4ye
Click to download the certificate.
Basic information for your Custom App

Please provide the basic information needed to configure your Custom App. This information will be viewed by end-users of the application.

Application Name *: Zocaler

Description

Upload logo

This logo will be displayed for all users who have access to this application. Please upload a .png or .gif image of size 256 x 256 pixels.
Enter the Zcaler SSO URL https://login.zscalerone.net:443/sfc_sso

Entity ID: zscalerone.net
Authentication - Configuring Google SAML

Step 5 of 5
Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

- displayName
- Basic Information
- Primary Email

ADD NEW MAPPING
Authentication - Configuring Google SAML

Click this icon.

Zscaler
ON for everyone

Service Provider Details
Set up basic service provider (SP) details like the ACS URL, entity id and more

Attribute Mapping
Configure additional parameters that need to be sent to the service provider along with the authentication token

Turn on Zscaler for everyone

- Zscaler will be turned ON for everyone in your domain.

These changes may take up to 24 hours to propagate to all users.

CANCEL TURN ON FOR EVERYONE
Authentication - Back Up Zscaler

Zscaler backup....

<table>
<thead>
<tr>
<th>#</th>
<th>Restore Point Name</th>
<th>Description</th>
<th>Created By</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hostad</td>
<td>---</td>
<td><a href="mailto:mcnc@k12gapps.mcnc.org">mcnc@k12gapps.mcnc.org</a></td>
<td>Tuesday, August 16, 2016 12:57:10 PM</td>
</tr>
<tr>
<td>2</td>
<td>ADnow</td>
<td>---</td>
<td><a href="mailto:mcnc@k12gapps.mcnc.org">mcnc@k12gapps.mcnc.org</a></td>
<td>Tuesday, August 16, 2016 12:47:25 PM</td>
</tr>
<tr>
<td>3</td>
<td>SAML</td>
<td>8/16/2016 SAML</td>
<td><a href="mailto:mcnc@k12gapps.mcnc.org">mcnc@k12gapps.mcnc.org</a></td>
<td>Tuesday, August 16, 2016 12:42:26 PM</td>
</tr>
<tr>
<td>4</td>
<td>Dianne's SAML</td>
<td>---</td>
<td><a href="mailto:mcnc@k12gapps.mcnc.org">mcnc@k12gapps.mcnc.org</a></td>
<td>Tuesday, July 05, 2016 11:15:21 AM</td>
</tr>
<tr>
<td>5</td>
<td>John's SAML</td>
<td>---</td>
<td><a href="mailto:mcnc@k12gapps.mcnc.org">mcnc@k12gapps.mcnc.org</a></td>
<td>Tuesday, July 05, 2016 9:08:32 AM</td>
</tr>
</tbody>
</table>
Authentication – configuring SAML in Zscaler

1. Go to the Zscaler Administration panel.
2. Click on Authentication Settings.
3. In the Authentication Profile, select SAML for Authentication Type.
4. Click on Configure SAML.
Authentication - configuring SAML in Zscaler
Authentication - configuring SAML in Zscaler
Authentication - turning on for sublocation in Zscaler

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>IP Address</th>
<th>VPN Config</th>
<th>XFF</th>
<th>Authentication</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ONE</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>2012AD</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>Even</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>Odd</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td><strong>Enabled</strong></td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>other</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>6</td>
<td>Traffic Gen 2</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>Traffic Gen</td>
<td>152.46...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>8</td>
<td>new node</td>
<td>152.26...</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
Authentication - Department with authorization “off”
Authentication - Department with authorization “off”
## Authorization - Google configuration

<table>
<thead>
<tr>
<th>Email</th>
<th>OU/orgUnitPath</th>
<th>Group/Group-email</th>
<th>Custom Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:9thWonder@k12gapps.mcnc.org">9thWonder@k12gapps.mcnc.org</a></td>
<td>/PWM/Admins</td>
<td><a href="mailto:admins@k12gapps.mcnc.org">admins@k12gapps.mcnc.org</a></td>
<td>Zscaler_Dpt</td>
</tr>
<tr>
<td>2$<a href="mailto:Fabo@k12gapps.mcnc.org">Fabo@k12gapps.mcnc.org</a></td>
<td>/PWM/EastEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td>Zscaler_Group</td>
</tr>
<tr>
<td><a href="mailto:AlbertEinstein@k12gapps.mcnc.org">AlbertEinstein@k12gapps.mcnc.org</a></td>
<td>/PWM/MainEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td>FRONTOFFICE</td>
</tr>
<tr>
<td><a href="mailto:12Gauge@k12gapps.mcnc.org">12Gauge@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td><a href="mailto:nonstudent@k12gapps.mcnc.org">nonstudent@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AlexanderGrahamBell@k12gapps.gov">AlexanderGrahamBell@k12gapps.gov</a></td>
<td>/PWM/SouthMStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td>STUDENTS</td>
</tr>
<tr>
<td><a href="mailto:AndersonPaak@k12gapps.mcnc.gov">AndersonPaak@k12gapps.mcnc.gov</a></td>
<td>/PWM/Hstudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td><a href="mailto:elementary@k12gapps.mcnc.org">elementary@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:50Cent@k12gapps.mcnc.org">50Cent@k12gapps.mcnc.org</a></td>
<td>/PWM/WestEStudents</td>
<td><a href="mailto:students@k12gapps.mcnc.org">students@k12gapps.mcnc.org</a></td>
<td>STUDENTS</td>
</tr>
<tr>
<td><a href="mailto:2Pistols@k12gapps.mcnc.org">2Pistols@k12gapps.mcnc.org</a></td>
<td>/PWM/EastETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td><a href="mailto:middle@k12gapps.mcnc.org">middle@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:ActionBronson@k12gapps.mcnc.org">ActionBronson@k12gapps.mcnc.org</a></td>
<td>/PWM/Headteachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td>STUDENTS</td>
</tr>
<tr>
<td><a href="mailto:40Gloc@k12gapps.mcnc.org">40Gloc@k12gapps.mcnc.org</a></td>
<td>/PWM/MainETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td><a href="mailto:high@k12gapps.mcnc.org">high@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AndreNickatina@k12gapps.mcnc.org">AndreNickatina@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMTEachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td>STUDENTS</td>
</tr>
<tr>
<td><a href="mailto:AlfredHitchcock@k12gapps.mcnc.org">AlfredHitchcock@k12gapps.mcnc.org</a></td>
<td>/PWM/SouthMTEachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td><a href="mailto:nonstudent@k12gapps.mcnc.org">nonstudent@k12gapps.mcnc.org</a></td>
</tr>
<tr>
<td><a href="mailto:AliVegas@k12gapps.mcnc.org">AliVegas@k12gapps.mcnc.org</a></td>
<td>/PWM/WestETeachers</td>
<td><a href="mailto:teachers@k12gapps.mcnc.org">teachers@k12gapps.mcnc.org</a></td>
<td>TEACHERS</td>
</tr>
</tbody>
</table>
Authorization - adding Department (and/or Group) schema in Google (web)

https://support.google.com/a/answer/6327792?hl=en
Schema insert page:
https://developers.google.com/admin-sdk/directory/v1/reference/schemas/insert#try-it

{  
  "fields": [
    {
      "fieldName": "Department",
      "fieldType": "STRING",
      "readAccessType": "ADMINS_AND_SELF",
      "multiValued": true
    }
  
  },

  "schemaName": "Department"
}
Authorization - populating Department schema in Google (web)

https://developers.google.com/admin-sdk/directory/v1/reference/users/patch#try-it
Authorization - populating Department schema in Google (web)
Authorization - adding Department (and/or Group) schema in Google with GAM

- GAM=Google Apps Manager
- https://www.youtube.com/watch?v=_dybYXJpBH0

We will start in just a moment, allowing folks to join.
Today's Presentation - http://goo.gl/thLQBD
Sign In for Today - http://goo.gl/cEcZR6
Authorization - adding Department (and/or Group) schema in Google with GAM

C:\gam> gam info domain

C:\gam> gam create schema Department
  field Department type string multivalued endfield

C:\gam> gam create schema Groups
  field Groups type string multivalued endfield

C:\gam> gam print schemas
Authorization - populating Department (and/or Group) schema existing users in Google GAM

`gam update user janedoe@k12gapps.mcnc.org Department.Department multivalue STUDENT`

gam update user vct@k12gapps.mcnc.org Department.Department multivalue TEACHER

gam update user mrzeke@k12gapps.mcnc.org Department.Department multivalue FRONTOFFICE

`gam update user vct@k12gapps.mcnc.org Groups.Groups multivalue nonstudent@k12gapps.mcnc.org`

gam update user janedoe@k12gapps.mcnc.org Groups.Groups multivalue elementary@k12gapps.mcnc.org Groups.Groups multivalue middle@k12gapps.mcnc.org

gam update user 50cent@k12gapps.mcnc.org Department.Department multivalue FRONTOFFICE Department.Department multivalue TEACHER
Authorization - populating Department (and/or Group) schema in Google GAM

gam info user janedoe@k12gapps.mcnc.org

User: janedoe@k12gapps.mcnc.org
First Name: j
Last Name: ane
Is a Super Admin: False
Is Delegated Admin: False
Has Agreed to Terms: True
IP Whitelisted: False
Account Suspended: False
Must Change Password: False
Google Unique ID: 106911627312612860553
Customer ID: C01k0d5zn
Mailbox is setup: True
Included in GAL: True
Creation Time: 2016-05-09T20:40:12.000Z
Last login time: 2016-08-01T15:29:37.000Z
Google Org Unit Path: /all_grades/elementary@k12gapps.mcnc.org

Custom Schemas:
Schema: Department
  Department:
    STUDENT

Schema: Groups
  Groups:
    elementary@k12gapps.mcnc.org
    middle@k12gapps.mcnc.org

Licenses:
Gam to create new users.

File is testuser.csv:

<table>
<thead>
<tr>
<th>fullname</th>
<th>Email</th>
<th>firstname</th>
<th>lastname</th>
<th>orgUnitPath</th>
<th>Password</th>
<th>Ggroup</th>
<th>Zscaler_Dept</th>
<th>Zscaler_Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>MrKila</td>
<td><a href="mailto:MrKila@k12gapps.mcnc.org">MrKila@k12gapps.mcnc.org</a></td>
<td>Mr</td>
<td>Kil</td>
<td>/PWM/MainETeachers</td>
<td>Qwerty1234!</td>
<td><a href="mailto:eteachers@k12gapps.mcnc.org">eteachers@k12gapps.mcnc.org</a></td>
<td>TEACHERS</td>
<td></td>
</tr>
<tr>
<td>MrGlocc</td>
<td><a href="mailto:MrGlocc@k12gapps.mcnc.org">MrGlocc@k12gapps.mcnc.org</a></td>
<td>Mr</td>
<td>Glocc</td>
<td>/PWM/MainETeachers</td>
<td>Qwerty1234!</td>
<td><a href="mailto:eteachers@k12gapps.mcnc.org">eteachers@k12gapps.mcnc.org</a></td>
<td>TEACHERS</td>
<td></td>
</tr>
</tbody>
</table>

```
gam csv testuser.csv gam create user ~Email password ~Password firstname ~firstname lastname
```

```
gam csv testuser.csv gam update user ~Email OU ~orgUnitPath
```

```
gam csv testuser.csv gam update user ~Email Department.Department multivalue ~Zscaler_Dept
```

```
gam csv testuser.csv gam update user ~Email Groups.Groups multivalue ~Zscaler_Group
```
Authorization - updating existing users with Departments (and/or Groups) schema in Google GAM csv

Retrieving list of existing users:

gam print users allfields

gam print users allfields > outfile.csv
Authorization - updating existing user Departments (and/or Group) schema in Google GAM csv

=IF(ISNUMBER(SEARCH("Admins*",W<row#>)),"NONSTUDENT","STUDENT")

<table>
<thead>
<tr>
<th>primaryEmail</th>
<th>orgUnitPath</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:100kila@k12gapps.mcnc.org">100kila@k12gapps.mcnc.org</a></td>
<td>/PWM/MainETeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:12gauge@k12gapps.mcnc.org">12gauge@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMStudents</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:2chainz@k12gapps.mcnc.org">2chainz@k12gapps.mcnc.org</a></td>
<td>/PWM/EastEStudents</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:2pistols@k12gapps.mcnc.org">2pistols@k12gapps.mcnc.org</a></td>
<td>/PWM/EastETeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:abrahamlincoln@k12gapps.mcnc.org">abrahamlincoln@k12gapps.mcnc.org</a></td>
<td>/PWM/MainETeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:abstractrude@k12gapps.mcnc.org">abstractrude@k12gapps.mcnc.org</a></td>
<td>/PWM/Adms</td>
<td>NONSTUDENT</td>
</tr>
<tr>
<td><a href="mailto:acehood@k12gapps.mcnc.org">acehood@k12gapps.mcnc.org</a></td>
<td>/PWM/SouthMStudents</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:actionbronson@k12gapps.mcnc.org">actionbronson@k12gapps.mcnc.org</a></td>
<td>/PWM/HTeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:adamsaleh@k12gapps.mcnc.org">adamsaleh@k12gapps.mcnc.org</a></td>
<td>/PWM/WestEStudents</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:andre3000@k12gapps.mcnc.org">andre3000@k12gapps.mcnc.org</a></td>
<td>/PWM/Adms</td>
<td>NONSTUDENT</td>
</tr>
<tr>
<td><a href="mailto:andrenickatina@k12gapps.mcnc.org">andrenickatina@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMTeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:andygriffith@k12gapps.mcnc.org">andygriffith@k12gapps.mcnc.org</a></td>
<td>/PWM/NorthMStudents</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:andymineo@k12gapps.mcnc.org">andymineo@k12gapps.mcnc.org</a></td>
<td>/PWM/MainETeachers</td>
<td>STUDENT</td>
</tr>
<tr>
<td><a href="mailto:andyrooney@k12gapps.mcnc.org">andyrooney@k12gapps.mcnc.org</a></td>
<td>/PWM/HTeachers</td>
<td>STUDENT</td>
</tr>
</tbody>
</table>
Authorization - updating existing users, Departments (and/or Group) schema in Google GAM csv

- `gam csv outfile.csv gam update user ~Email Department.Department multivalue ~Department`
Authorization – updating existing users, Departments (and/or Group) schema in Google GAM csv bat file

@echo off
rem Script to pull users from Google using gam and repopulate the Department.Department or Groups.Groups custom field for Zscaler
if "%1"=="" echo Google group is undefined & goto end
set infile=%1
if "%2"=="" echo Zscaler group or department missing & goto end
set outfile=%2
cls

echo Do you want for variable to go in schema Groups.Groups or Department.Department for Zscaler?
set /p grodep=G/D
if %grodep%==G set field=Groups
if %grodep%==D set field=Department
cls

echo.
Authorization - updating existing users, Departments (and/or Group) schema in Google GAM csv bat file

echo Enter F to continue and associate Google users in group %infile% with Zscaler %field% %2 and place in %infile %csv, %infile%%%field%.csv

echo.

echo Enter Y to continue and associate Google users in group %infile% with Zscaler %field% %2 and place in %infile %csv, %infile%%%field%.csv then modify Google entries using gam

echo.

echo Enter Q to quit

echo.

set /p choice=F/Y/Q

echo.

if %choice%==Q goto end

call gam info group %1 > %1.csv

echo user,%field%.%field%> %1.%field%.csv

FOR /f "tokens=2" %%i in ('type %1.csv ^| findstr member:') DO @echo %%i,%%2 >> ,%1.%field%.csv

if %choice%==Y gam csv %1.%field%.csv gam update user ~user %field%.%field% multivalue ~%field%.%field%

:end
### Attribute Mapping

Provide mappings between service provider attributes to available user profile fields.

<table>
<thead>
<tr>
<th>Email</th>
<th>Basic Information</th>
<th>Primary Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td>Groups</td>
<td>Groups</td>
<td>Groups</td>
</tr>
</tbody>
</table>
Authorization – configuring SAML in Zscaler

Edit SAML

Identity Provider (IDP) Options

- **SAML Portal URL:** https://account baptist.google.com/saml0/idp?idpl...
- **Login Name Attribute:** Email

Public SSL Certificate
- **GoogleIDP Certificate:** b122gps6.mncn.org (Default)
- **Upload:**

Service Provider (SP) Options

- **Sign SAML Request:**
- **Request Signing SSL Certificate:** Certificate 2 expires 2018 September
- **SP's Public SSL Certificate:** Download
- **SP's Metadata:** Download

Auto-Provisioning Options

- **Enable SAML Auto-Provisioning:**
- **User Display Name Attribute:** Primary Email
- **Group Name Attribute:** Groups
- **Department Name Attribute:** Department
<table>
<thead>
<tr>
<th></th>
<th>Department</th>
<th>Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single-membership appearance in logs?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Single-membership filtering decisions?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple-membership appearance in logs?</td>
<td>No*</td>
<td>No</td>
</tr>
<tr>
<td>Multiple membership filtering decisions?</td>
<td>No*</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Only the first Department will be used/seen/parsed/logged by Zscaler
Authorization - department/group behavior

User: 50cent@k12gapps.mcnc.org
First Name: 50
Last Name: Cent
Is a Super Admin: False
Is Delegated Admin: False
Has Agreed to Terms: True
IP Whitelisted: False
Account Suspended: False
Must Change Password: False
Google Unique ID: 118008096095087238185
Customer ID: C01k0d5zn
Mailbox is setup: True
Included in GAL: True
Creation Time: 2016-08-03T19:50:21.000Z
Last login time: Never
Google Org Unit Path: /PWN/West2Students

Custom Schemas:

**Schema: Department**
- Department:
  - FRONTOFFICE
  - TEACHERS

**Schema: Groups**

- Groups:
  - middle@k12gapps.mcnc.org
  - high@k12gapps.mcnc.org

Groups: (1)
- Students <students@k12gapps.mcnc.org>

Licenses:
### Authorization - department/group behavior

#### URL Filtering Policy

<table>
<thead>
<tr>
<th>Rule Order</th>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEPARTMENTS</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>FRONTOFFICE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL CATEGORIES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lingerie/Bikini; Alcohol/Tobacco</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>DEPARTMENTS</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>TEACHERS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL CATEGORIES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Drugs</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>GROUPS</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:middle@k12apps.mcnc.org">middle@k12apps.mcnc.org</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL CATEGORIES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gambling</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>GROUPS</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:high@k12apps.mcnc.org">high@k12apps.mcnc.org</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL CATEGORIES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Procracy</td>
<td></td>
</tr>
</tbody>
</table>
Authorization - auto-provisioning

User Management

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>FRONTOFFICE</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td>MIDDLE</td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>STUDENT</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td>Service Admin</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td>TEACHER</td>
<td>---</td>
</tr>
</tbody>
</table>

Group Management

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Service Admin</td>
<td>---</td>
</tr>
<tr>
<td>2</td>
<td><a href="mailto:elementary@k12gapps.mcnc.org">elementary@k12gapps.mcnc.org</a></td>
<td>---</td>
</tr>
<tr>
<td>3</td>
<td>high</td>
<td>---</td>
</tr>
<tr>
<td>4</td>
<td><a href="mailto:high@k12gapps.mcnc.org">high@k12gapps.mcnc.org</a></td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td><a href="mailto:middle@k12gapps.mcnc.org">middle@k12gapps.mcnc.org</a></td>
<td>---</td>
</tr>
<tr>
<td>6</td>
<td>samigroup</td>
<td>---</td>
</tr>
<tr>
<td>7</td>
<td>students</td>
<td>---</td>
</tr>
</tbody>
</table>
# Accounting - logs

<table>
<thead>
<tr>
<th>No.</th>
<th>Logged Time</th>
<th>User</th>
<th>URL</th>
<th>Policy Action</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:greenfrog@k12gapps.mcn">greenfrog@k12gapps.mcn</a>...</td>
<td><a href="http://www.bing.com/">www.bing.com/</a></td>
<td>Not allowed to...</td>
<td>GRADEONE</td>
</tr>
<tr>
<td>2</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:greenfrog@k12gapps.mcn">greenfrog@k12gapps.mcn</a>...</td>
<td><a href="http://www.bing.com/favicon.ico">www.bing.com/favicon.ico</a></td>
<td>Not allowed to...</td>
<td>GRADEONE</td>
</tr>
<tr>
<td>3</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:bigcootie@k12gapps.mcn">bigcootie@k12gapps.mcn</a>...</td>
<td>porn.com/</td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
<tr>
<td>4</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:bigcootie@k12gapps.mcn">bigcootie@k12gapps.mcn</a>...</td>
<td>porn.com/favicon.ico</td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
<tr>
<td>5</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:bigcootie@k12gapps.mcn">bigcootie@k12gapps.mcn</a>...</td>
<td><a href="http://www.wine-searcher.com/find/thunderbird+the">www.wine-searcher.com/find/thunderbird+the</a>...</td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
<tr>
<td>6</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:bigcootie@k12gapps.mcn">bigcootie@k12gapps.mcn</a>...</td>
<td><a href="http://www.wine-searcher.com/favicon.ico">www.wine-searcher.com/favicon.ico</a></td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
<tr>
<td>7</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:40glocc@k12gapps.mcn">40glocc@k12gapps.mcn</a>...</td>
<td><a href="http://www.winespectator.com/">www.winespectator.com/</a></td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
<tr>
<td>8</td>
<td>Tuesday, August 09,...</td>
<td><a href="mailto:40glocc@k12gapps.mcn">40glocc@k12gapps.mcn</a>...</td>
<td><a href="http://www.winespectator.com/favicon.ico">www.winespectator.com/favicon.ico</a></td>
<td>Not allowed to...</td>
<td>STUDENT</td>
</tr>
</tbody>
</table>
AD - no SAML
SAML with AD
### Caveats

<table>
<thead>
<tr>
<th>Platform</th>
<th>Chrome</th>
<th>Firefox</th>
<th>Google-drive-app</th>
<th>MIE</th>
<th>Safari</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chromebook</td>
<td>x</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>ipad</td>
<td>x</td>
<td>N/A</td>
<td>x</td>
<td>N/A</td>
<td>x</td>
</tr>
<tr>
<td>Microsoft</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>N/A</td>
</tr>
<tr>
<td>Macbook</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>N/A</td>
<td>x</td>
</tr>
</tbody>
</table>
Caveats

https://www.mcnc.org/our-community/k12/docs/web-security/category-definitions
Caveats

Choose an account

- **Unknown Unknown**
  - Email: bigcootle@k12gapps.mcnc.org

- **Dianne Dunlap**
  - Email: dianne@k12gapps.mcnc.org

- **40 Glocc**
  - Email: 40glocc@k12gapps.mcnc.org

- **j ane**
  - Email: janedoe@k12gapps.mcnc.org

[Buttons]
- Add account
- Remove
Caveats

Your request is arriving at this server from the IP address 192.26.210.24.
You are accessing this host via a Zscaler proxy in the zscalerone.net cloud.

Check Your Connection Quality / Run Zscaler Analyzer

The Zscaler hostname for this proxy appears to be one-pmcnc6b1.
The request is being received by the Zscaler Proxy from the IP address 128.109.64.94
Your Gateway IP Address is 128.109.64.94

K12 GApps

Would you like to Logout?
Your user name is: 49gloc@k12gapps.mcnc.org.
Logout
Caveats
Questions?
Summer Webinar Series
Google <-> SAML -> Zscaler Integration

Dianne Dunlap (ddunlap@mcnc.org, 919-248-8439)
Client Network Engineering

Webinar Links: www.mcnc.org/cne-webinars