

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

A=authentication

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

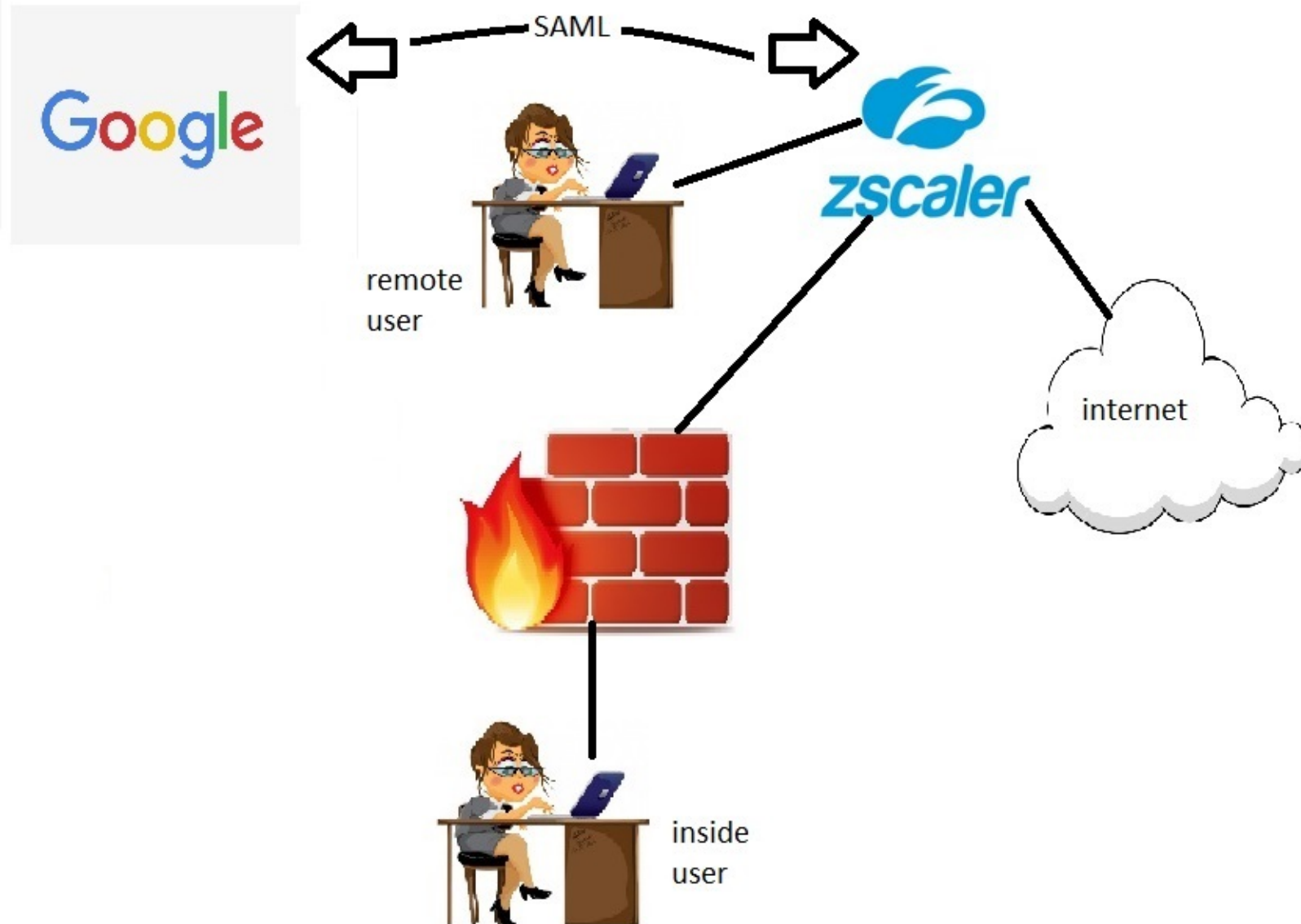
A=authorization

- 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



Authentication - Moving to SAML in Zscaler



zscaler

Dashboard Analytics Policy Administration

Settings Authentication Resources TRAFFIC FORWARDING

Locations ?

VPN Credentials Hosted PAC Files eZ Agent Configurations SecureAgent Notifications ACCESS CONTROL URL Categories Bandwidth Classes Time Intervals

+ Add Location → Import Locations Download CSV Sample Import CSV file

#	Name	IP Addresses	VPN Credentials	XFF	Authentication	SSL
1	CNE	152.46.31.89	---	---	---	---
2	↪ High_School	152.46.31.229	---	---	---	---
3	↪ Middle School	152.46.31.250	---	---	Enabled	---
4	↪ Elementary_School	152.46.31.251	---	---	Enabled	---
5	↪ Other	---	---	---	Enabled	---
6	↪ Central Office	152.46.31.236	---	---	---	---
7	↪ Guest	152.46.31.238	---	---	---	---

Authentication - Moving to SAML in Zscaler



zscaler Dashboard Analytics Policy Administration

Settings Authentication Resources

TRAFFIC FORWARDING

Locations 2

VPN Credentials
Hosted PAC Files
eZ Agent Configurations
SecureAgent Notifications

ACCESS CONTROL

URL Categories
Bandwidth Classes
Time Intervals

+ Add Location + Import Locations Download CSV Sample Import CSV file

#	Name	IP Addresses	VPN Credentials	XFF	Authentication	SSL
1	CNE	152.46.31.89	---	---	---	---
2	High_School	152.46.31.229	---	---	---	---
3	Middle School	152.46.31.250	---	---	Active Directory	Enabled
4	Elementary_School	152.46.31.251	---	---	SAML	Enabled
5	Other	---	---	---	Hosted	Enabled
6	Central Office	152.46.31.236	---	---	---	---
7	Guest	152.46.31.238	---	---	---	---

Authentication - custom category exceptions in Zscaler - GRE/onsite



The image shows the Zscaler web interface with the "Edit URL Category" dialog box open. The dialog has a blue header with the title "Edit URL Category" and a close button. The main content area is divided into several sections:

- Name:** A text input field containing "Google", which is highlighted with a red rectangle.
- URL Super Category:** A dropdown menu currently set to "User-Defined".
- Custom URLs:** A list of URLs with a red rectangle around the first three items: ".gmail.com", ".google.com", and "accounts.google.com". Each item has a small "x" icon to its right. Below the list, it says "3 items" and "Remove All".
- URLs retaining parent category:** An empty text input field with an "Add Items" button.
- Custom Keywords:** An empty text input field with an "Add Items" button.
- Description:** A large empty text area.

At the bottom of the dialog, there are three buttons: "Save", "Delete", and "Cancel".

Authentication - authentication exceptions in Zscaler - GRE/onsite

A screenshot of the Zscaler Administration console. The left sidebar shows the navigation menu with 'Settings' expanded, and 'Authentication' and 'Resources' visible below. The main content area shows the 'Advanced Settings' page. Under the 'Authentication Bypass' section, three items are circled in orange: 'Bypassed URL Categories' with a dropdown menu showing 'Google', 'Bypassed URLs' with an empty text input field and an 'Add Items' button, and 'Bypassed Applications' with a dropdown menu showing 'Google Analytics; Google Apps for Bus...'. The top navigation bar includes 'Dashboard', 'Analytics', 'Policy', and 'Administration'.

zscaler

Dashboard Analytics Policy Administration

Settings

ACCOUNT MANAGEMENT

My Profile
Company Profile
Alerts
Print All Policies

CLOUD CONFIGURATION

Advanced Settings

Authentication

Resources

Admin Ranking

Enable Admin Ranking

Advanced Web App Control Options

Allow Cascading to URL Filtering

Admin UI Session Timeout

Session Timeout Duration

30 Mins

Authentication Bypass

Bypassed URL Categories

Google

Bypassed URLs

Add Items

Bypassed Applications

Google Analytics; Google Apps for Bus...

Authentication - SSL decryption exceptions in Zscaler - GRE/onsite



The image shows the Zscaler management console interface. On the left is a dark sidebar with navigation options: Web, SECURITY (Malware Protection, Advanced Threat Protection, Behavioral Analysis, Browser Control), ACCESS CONTROL (URL & Cloud App Control, File Type Control, Bandwidth Control, SSL Inspection - highlighted in blue), FTP Control, DATA LOSS PREVENTION (Data Loss Prevention), and Mobile. The main content area has a top navigation bar with Dashboard, Analytics, Policy, and Administration. Below this, there are two sections. The first section, "Policy for Non-Decrypted Traffic", includes a "Blocked URL Categories" dropdown menu showing "Adult Sex Education; Adult Themes; An...", a "Blocked URLs" text input field with an "Add Items" button, and a "Show Notifications for Blocked Traffic" toggle switch which is currently turned off. The second section, "Policy for SSL Decryption", includes a "Block Undecryptable Traffic" toggle switch which is currently turned off, a "Bypassed URL Categories" dropdown menu showing "Google" (circled in orange), a "Bypassed URLs" text input field with an "Add Items" button, and a "Bypassed Applications" dropdown menu showing "Google Analytics; Google Apps for Bus..." (circled in orange).

Authentication - exceptions in Zscaler - pac file



Pac file:

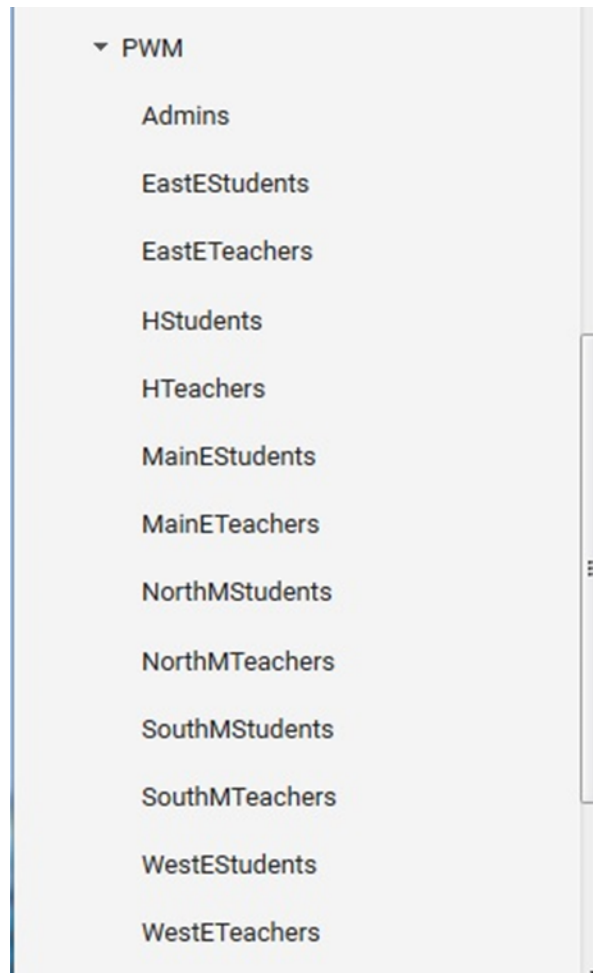
```
if(dnsDomainIs(host, "accounts.google.com")) return  
"DIRECT";
```

```
if(dnsDomainIs(host, "gmail.com")) return "DIRECT";
```

Lab test setup



k12gapps.mcnc.org, OU=PWM, more OUs below:

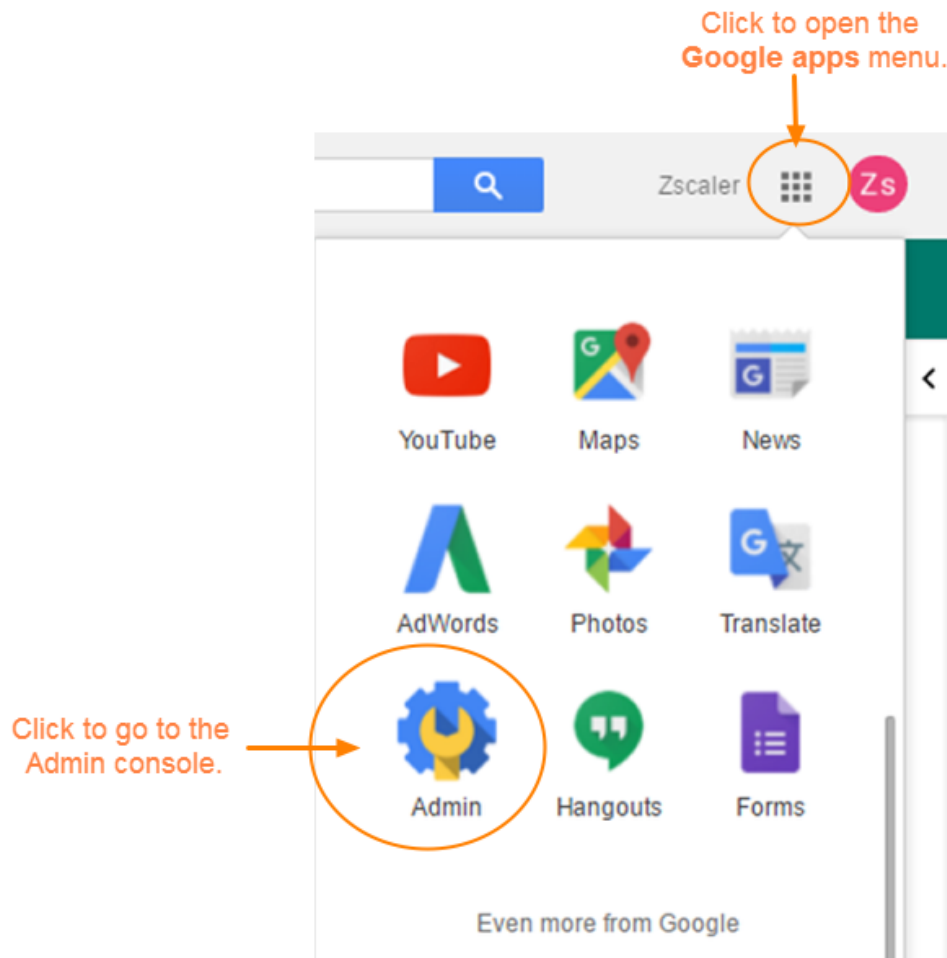


Lab test setup

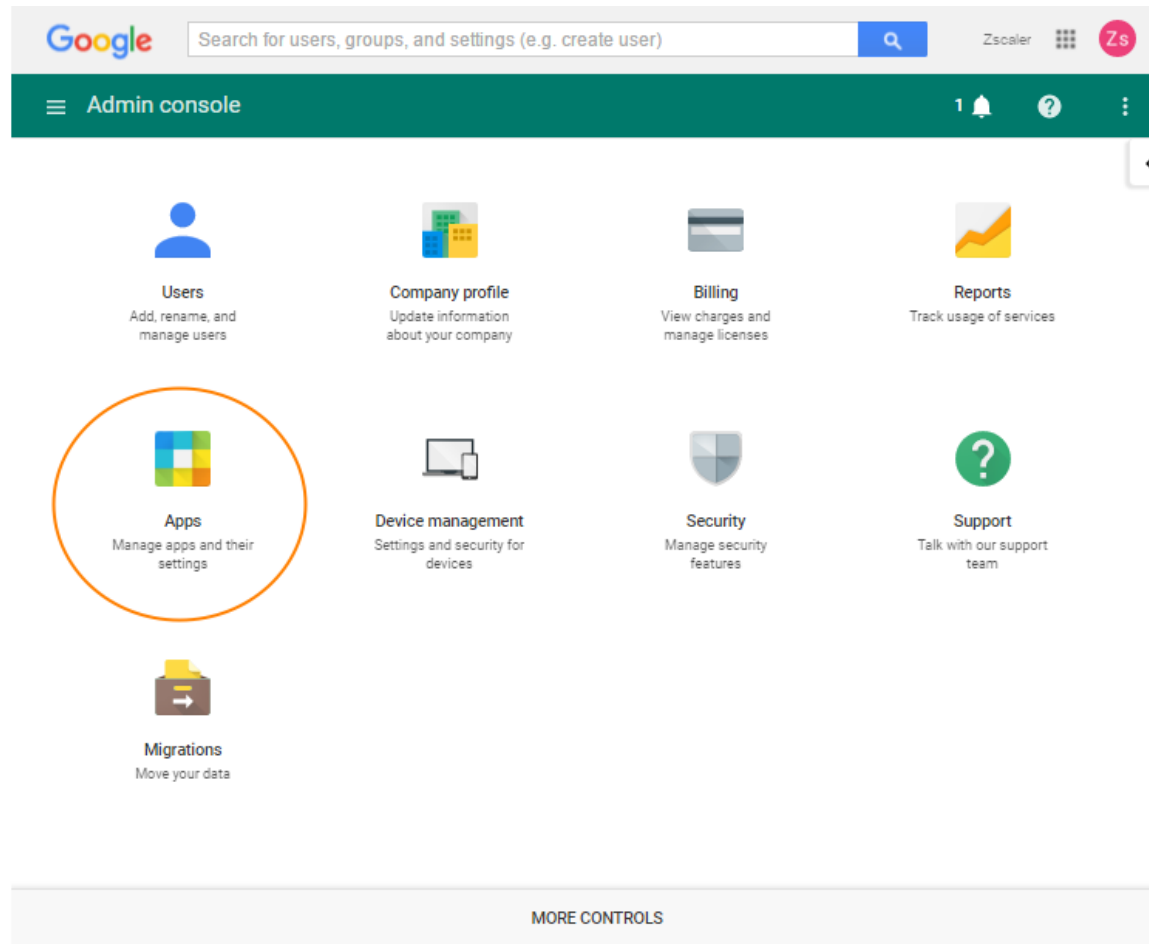


Email	Google non-custom Attributes	
	OU/orgUnitPath	Group/Group-email
9thWonder@k12gapps.mcnc.org	/PWM/Admins	admins@k12gapps.mcnc.org
2\$Fabo@k12gapps.mcnc.org	/PWM/EastEStudents	students@k12gapps.mcnc.org
AlbertEinstein@k12gapps.mcnc.org	/PWM/MainEStudents	students@k12gapps.mcnc.org
12Gauge@k12gapps.mcnc.org	/PWM/NorthMStudents	students@k12gapps.mcnc.org
AlexanderGrahamBell@k12gapps.mcnc.org	/PWM/SouthMStudents	students@k12gapps.mcnc.org
AndersonPaak@k12gapps.mcnc.org	/PWM/Hstudents	students@k12gapps.mcnc.org
50Cent@k12gapps.mcnc.org	/PWM/WestEStudents	students@k12gapps.mcnc.org
2Pistols@k12gapps.mcnc.org	/PWM/EastETeachers	teachers@k12gapps.mcnc.org
ActionBronson@k12gapps.mcnc.org	/PWM/Hteachers	teachers@k12gapps.mcnc.org
40Glocc@k12gapps.mcnc.org	/PWM/MainETeachers	teachers@k12gapps.mcnc.org
AndreNickatina@k12gapps.mcnc.org	/PWM/NorthMTeachers	teachers@k12gapps.mcnc.org
AlfredHitchcock@k12gapps.mcnc.org	/PWM/SouthMTeachers	teachers@k12gapps.mcnc.org
AliVegas@k12gapps.mcnc.org	/PWM/WestETeachers	teachers@k12gapps.mcnc.org

Authentication - Configuring Google SAML



Authentication - Configuring Google SAML



Authentication - Configuring Google SAML

A screenshot of the Google Admin console's "Apps" settings page. The page has a green header bar with the Google logo, a search bar, and user avatars. Below the header, the "Apps" section is active. On the left, under "APPS SETTINGS", there is a link for "Marketplace settings". The main area displays four app categories in a 2x2 grid: "Google Apps" (8 apps), "Additional Google services" (14 apps), "Marketplace apps" (0 apps), and "SAML apps" (0 apps). The "SAML apps" card is circled in orange. It includes a link to "Manage SSO for SAML Application". A "SEND FEEDBACK" button is at the bottom right.

Google Search for users, groups, and settings (e.g. create user) Zscaler Zs

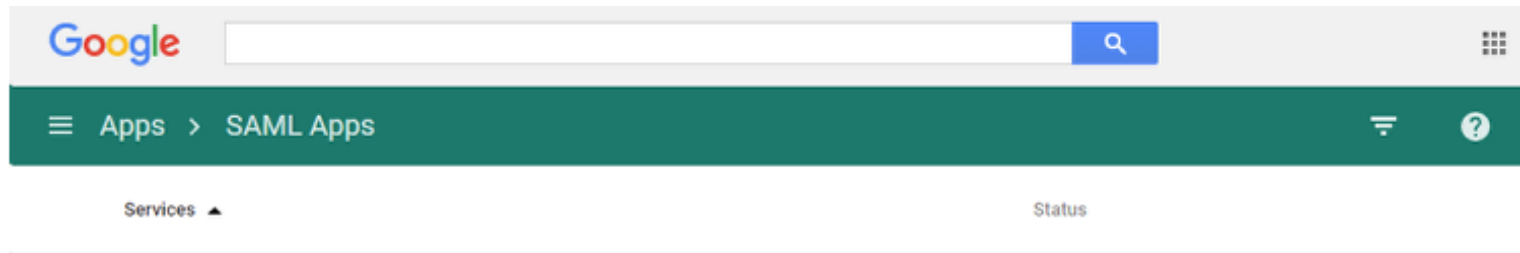
Apps ?

APPS SETTINGS
Marketplace settings

App Category	Count	Description
Google Apps	8	Gmail, Calendar, Drive & more
Additional Google services	14	Blogging, photos, video, social tools and more
Marketplace apps	0	More about Marketplace apps
SAML apps	0	Manage SSO for SAML Application

SEND FEEDBACK

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

Zscaler

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 SSO config for the service provider.

Option 1

SSO URL <https://accounts.google.com/o/saml2/idp?idpid=C00yab4ye>

Entity ID <https://accounts.google.com/o/saml2?idpid=C00yab4ye>

Certificate [↓ DOWNLOAD](#)

----- OR -----

Option 2

IDP metadata [↓ DOWNLOAD](#)

PREVIOUS CANCEL NEXT

Copy this URL. →

Click to download the certificate. →

Authentication - Configuring Google SAML



Step 3 of 5

×

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 *

Zscaler

app-id: zscaler

Description

Upload logo

CHOOSE FILE

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.

PREVIOUS

CANCEL

NEXT

Authentication - Configuring Google SAML



- Enter the Zscaler SSO URL https://login.zscalerone.net:443/sfc_sso
- Entity ID: **zscalerone.net**

Step 4 of 5 ×

Service Provider Details

Please provide service provider details to configure SSO for your Custom App. The ACS url and Entity ID are mandatory.

ACS URL *	<input type="text" value="https://login.zscalerone.net:443/sfc_sso"/>
Entity ID *	<input type="text" value="zscalerone.net"/>
Start URL	<input type="text"/>
Signed Response	<input type="checkbox"/>
Name ID	<input type="text"/> <input type="text"/>

Authentication - Configuring Google SAML



The screenshot shows a two-step configuration process. The foreground window, titled "Step 5 of 5 Attribute Mapping", contains a table for mapping service provider attributes to user profile fields. The first row is highlighted with an orange oval and contains the attribute "displayName", the category "Basic Information", and the field "Primary Email". Below the table is a button labeled "ADD NEW MAPPING", also circled in orange. At the bottom of this window are "PREVIOUS", "CANCEL", and "FINISH" buttons. The background window, partially visible, is titled "Step 4 of 5" and shows the "ACS url and Entity" section, with an orange rectangle highlighting a text input field. It has "PREVIOUS", "CANCEL", and "NEXT" buttons at the bottom.

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

PREVIOUS CANCEL FINISH

Step 4 of 5

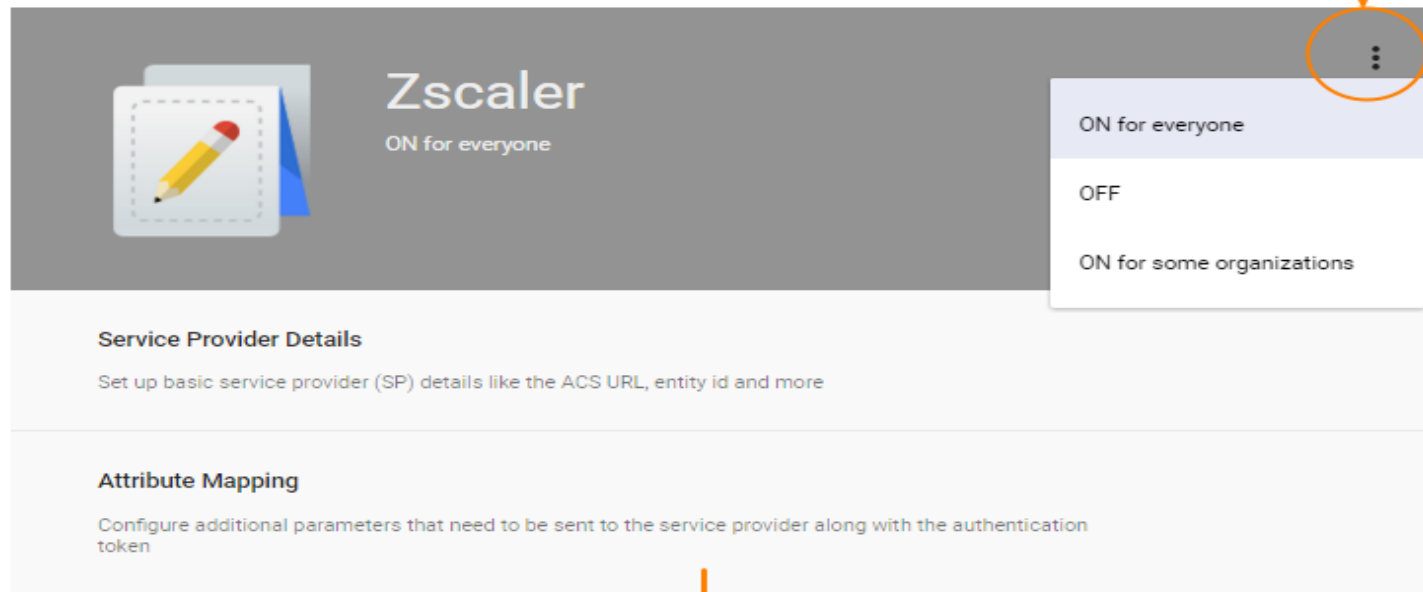
ACS url and Entity

PREVIOUS CANCEL NEXT

Authentication - Configuring Google SAML



Click this icon.



The screenshot shows the Zscaler configuration interface. At the top, there is a header bar with the Zscaler logo and the text "ON for everyone". To the right of the header, there is a dropdown menu with three options: "ON for everyone", "OFF", and "ON for some organizations". An orange circle highlights the three-dot menu icon, and an orange arrow points to it with the text "Click this icon." Below the header, there are two sections: "Service Provider Details" and "Attribute Mapping".

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....

Settings

Authentication

Authentication Configuration

Authentication Settings

User Management

Administration Controls

Administrator Management

Role Management

Audit Logs

Backup & Restore

+ Add Restore Point

Search...

#	Restore Point Name	Description	Created By	Created On	
1	Hosted	---	mcnc@k12gapps.mcnc.org	Tuesday, August 16, 2016 12:57:10 PM	
2	ADnow	---	mcnc@k12gapps.mcnc.org	Tuesday, August 16, 2016 12:47:25 PM	
3	SAML	8/16/2016 SAML	mcnc@k12gapps.mcnc.org	Tuesday, August 16, 2016 12:42:26 PM	
4	Dianne's SAML	---	mcnc@k12gapps.mcnc.org	Tuesday, July 05, 2016 11:15:21 AM	
5	John's SAML	---	mcnc@k12gapps.mcnc.org	Tuesday, July 05, 2016 9:08:32 AM	

Authentication - configuring SAML in Zscaler



A screenshot of the Zscaler Administration console. The browser address bar shows the URL "https://admin.zscalerone.net/#administration/auth-settings". The Zscaler logo is in the top left. The top navigation bar includes "Dashboard", "Analytics", "Policy", and "Administration" (which is circled in orange). The left sidebar contains "Settings", "Authentication", and "AUTHENTICATION CONFIGURATION". Under "Authentication", "Authentication Settings" is circled in orange. The main content area has two tabs: "AUTHENTICATION PROFILE" and "AUTHENTICATION BRIDGES". Under "Authentication Profile", there are three sections: "Directory Type" with buttons for "Hosted DB" (selected), "Active Directory", and "OpenLDAP"; "Authentication Frequency" with a dropdown menu set to "Only Once"; and "Authentication Type" with buttons for "Form-Based", "SAML" (selected), and "Configure SAML" (circled in orange). At the bottom, the "Temporary Authentication" section has buttons for "Disabled" (selected) and "One-Time Link".

Authentication - configuring SAML in Zscaler

The image shows the Zscaler web interface for configuring SAML. The left sidebar contains navigation links: Settings, Authentication, Authentication Settings (highlighted), User Management, Administration Controls, Administrator Management, Role Management, Audit Logs, Backup & Restore, and Resources. The main content area is titled "Edit SAML" and is divided into three sections: Identity Provider (IDP) Options, Service Provider (SP) Options, and Auto-Provisioning Options. In the IDP section, the SAML Portal URL, Login Name Attribute, and Public SSL Certificate are highlighted with orange boxes. In the SP section, the Sign SAML Request checkbox is unchecked. In the Auto-Provisioning section, the Enable SAML Auto-Provisioning checkbox is checked, and the User Display Name Attribute, Group Name Attribute, and Department Name Attribute are highlighted with orange boxes.

Edit SAML

Identity Provider (IDP) Options

SAML Portal URL
https://accounts.google.com/o/saml2/idp?idpi...

Login Name Attribute
Email

Public SSL Certificate
GoogleIDPCertificate-k12gapps.mcnc.org (1).pem
[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

Authentication - configuring SAML in Zscaler



The image shows a screenshot of the Zscaler web interface, specifically the "Edit SAML" configuration window. The window is titled "Edit SAML" and has a close button (X) in the top right corner. The interface is divided into three main sections: Identity Provider (IDP) Options, Service Provider (SP) Options, and Auto-Provisioning Options.

Identity Provider (IDP) Options

- SAML Portal URL**: A text input field containing the URL "https://accounts.google.com/o/saml2/dp?idpi...".
- Login Name Attribute**: A text input field containing the value "Email".
- Public SSL Certificate**: A section showing a certificate for "GoogleIDPCertificate-k12gapps.mcnc.org (1).pem" with a blue "Upload" link.

Service Provider (SP) Options

- Sign SAML Request**: A red toggle switch with a white "X" icon, currently turned off.
- Request Signing SSL Certificate**: A dropdown menu showing "Certificate 21 Expires 2018 September".
- SP's Public SSL Certificate**: A blue "Download" link.
- SP's Metadata**: A blue "Download" link.

Auto-Provisioning Options

- Enable SAML Auto-Provisioning**: A green toggle switch with a white checkmark, currently turned on.
- User Display Name Attribute**: A text input field containing the value "Primary Email".
- Group Name Attribute**: A text input field containing the value "Groups".
- Department Name Attribute**: A text input field containing the value "Department".

At the bottom of the window, there are two buttons: "Save" and "Cancel". The "Save" button is highlighted with an orange circle.

Authentication - turning on for sublocation in Zscaler



The screenshot shows the Zscaler Administration interface. The left sidebar contains the following menu items: Settings, Authentication, Resources, TRAFFIC FORWARDING, Locations (highlighted with a question mark icon), VPN Credentials, Hosted PAC Files, eZ Agent Configurations, SecureAgent Notifications, ACCESS CONTROL, URL Categories, Bandwidth Classes, Time Intervals, and End User Notifications. The main content area displays the 'Locations' table with the following data:

#	Name	IP Add...	VPN C...	XFF	Authentication	SSL
1	CNE	152.46...	---	---	---	---
2	→ 2012AD	152.46...	---	---	---	---
3	→ Even	152.46...	---	---	---	---
4	→ Odd	152.46...	---	---	Enabled	---
5	→ other	---	---	---	---	---
6	→ Traffic Gen 2	152.46...	---	---	---	---
7	→ Traffic Gen	152.46...	---	---	---	---
8	new node	152.26...	---	---	---	---

The 'Authentication' column for the 'Odd' sublocation (row 4) is circled in orange, indicating it is the focus of the configuration change.

Authentication - Department with authorization “off”



Web Insights

1. Select Chart Type

2. Choose a Timeframe

Custom: 8/9/2016 12:00:00 AM - 8/9/2016 7:...

3. Select Filters

Add Filter

User	URL Category	Location	Department	URL Class	Server IP
greenfrog@k12gapps.mcn...	Web Search	Road Warrior	GRADEONE	Business Use	None
greenfrog@k12gapps.mcn...	Web Search	Road Warrior	GRADEONE	Business Use	None
bluefrog@k12gapps.mcn...	Classifieds	Road Warrior	STUDENT	Business Use	208...
dianne@k12gapps.mcn...	Classifieds	Road Warrior	Default Department	Business Use	208...
dianne@k12gapps.mcn...	Classifieds	Road Warrior	Default Department	Business Use	208...
bigcootie@k12gapps.mcn...	Nudity	Road Warrior	STUDENT	Legal Liability	None
bigcootie@k12gapps.mcn...	Nudity	Road Warrior	STUDENT	Legal Liability	None
bigcootie@k12gapps.mcn...	Alcohol/Tobacco	Road Warrior	STUDENT	Productivity Loss	None
bigcootie@k12gapps.mcn...	Alcohol/Tobacco	Road Warrior	STUDENT	Productivity Loss	None
40glocc@k12gapps.mcn...	Alcohol/Tobacco	Road Warrior	STUDENT	Productivity Loss	None
40glocc@k12gapps.mcn...	Alcohol/Tobacco	Road Warrior	STUDENT	Productivity Loss	None
40glocc@k12gapps.mcn...	Science/Tech	Road Warrior	STUDENT	Business Use	74.125.201.94
40glocc@k12gapps.mcn...	Science/Tech	Road Warrior	STUDENT	Business Use	74.125.201.94
40glocc@k12gapps.mcn...	Science/Tech	Road Warrior	STUDENT	Business Use	64.233.190.94
40glocc@k12gapps.mcn...	Science/Tech	Road Warrior	STUDENT	Business Use	64.233.190.94
40glocc@k12gapps.mcn...	Science/Tech	Road Warrior	STUDENT	Business Use	64.233.190.94

Filters:

- ☐ Cloud Application Class
- ☐ DLP Dictionaries
- ☐ DLP Engine
- ☒ Department
- ☐ Event Time
- ☐ File Name
- ☐ HTTP Request

Authentication - Department with authorization “off”



← → ↻ <https://admin.zscalerone.net/#insights/web> 🔑 ☆

zscaler Dashboard Analytics Policy Administration Sign

🔄 Start Over

1. Select Chart Type

Logs

Apply Filters

2. Choose a Timeframe

Last 5 Minutes: 8/8/2016 1:45:15 PM - 8/8/20... ▼

3. Select Filters Clear Filters

Web Action ✕

Web Insights

User	URL	Policy Action	URL Category	Department
40glocc@k12gapps.mcnc...	www.maxim.com/	Not allowed to...	Adult Themes	Default Department
40glocc@k12gapps.mcnc...	www.holytaco.com/manliest-drinks-all-time/	Not allowed to...	Lingerie/Bikini	Default Department
40glocc@k12gapps.mcnc...	www.holytaco.com/favicon.ico	Not allowed to...	Lingerie/Bikini	Default Department
40glocc@k12gapps.mcnc...	www.wine-searcher.com/find/thunderbird+t...	Not allowed to...	Alcohol/Tobacco	Default Department
40glocc@k12gapps.mcnc...	www.wine-searcher.com/favicon.ico	Not allowed to...	Alcohol/Tobacco	Default Department

Authorization - Google configuration



Email	Google non-custom Attributes		Custom Attributes	
	OU/orgUnitPath	Group/Group-email	Zscaler_Dept	Zscaler_Group
9thWonder@k12gapps.mcnc.org	/PWM/Admins	admins@k12gapps.mcnc.org	FRONTOFFICE	nonstudent@k12gapps.mcnc.org
2\$Fabo@k12gapps.mcnc.org	/PWM/EastEStudents	students@k12gapps.mcnc.org	STUDENTS	elementary@k12gapps.mcnc.org
AlbertEinstein@k12gapps.mcnc.org	/PWM/MainEStudents	students@k12gapps.mcnc.org	STUDENTS	elementary@k12gapps.mcnc.org
12Gauge@k12gapps.mcnc.org	/PWM/NorthMStudents	students@k12gapps.mcnc.org	STUDENTS	middle@k12gapps.mcnc.org
AlexanderGrahamBell@k12gapps.mcnc.org	/PWM/SouthMStudents	students@k12gapps.mcnc.org	STUDENTS	middle@k12gapps.mcnc.org
AndersonPaak@k12gapps.mcnc.org	/PWM/Hstudents	students@k12gapps.mcnc.org	STUDENTS	high@k12gapps.mcnc.org
50Cent@k12gapps.mcnc.org	/PWM/WestEStudents	students@k12gapps.mcnc.org	STUDENTS	elementary@k12gapps.mcnc.org
2Pistols@k12gapps.mcnc.org	/PWM/EastETeachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org
ActionBronson@k12gapps.mcnc.org	/PWM/Hteachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org
40Glocc@k12gapps.mcnc.org	/PWM/MainETeachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org
AndreNickatina@k12gapps.mcnc.org	/PWM/NorthMTeachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org
AlfredHitchcock@k12gapps.mcnc.org	/PWM/SouthMTeachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org
AliVegas@k12gapps.mcnc.org	/PWM/WestETeachers	teachers@k12gapps.mcnc.org	TEACHERS	nonstudent@k12gapps.mcnc.org

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>

The screenshot shows the Google Apps Admin SDK Directory API reference page for the `users/patch` endpoint. The page has a dark blue header with the Google Apps Admin SDK logo and navigation links. A left sidebar lists various API endpoints, with 'Users' expanded to show 'patch' as the selected method. The main content area is titled 'Try it!' and includes instructions on how to use the API Explorer. It features a 'userKey' field with the value '40G1occk12gapps.mcnc.' circled in orange, a 'fields' selector, and a 'Patch body' section containing a JSON object. The JSON object has 'customSchemas' as an array, with one object containing 'Department' as a string, another 'Department' as an object with a 'value' of 'STUDENT', and a 'customType' of 'Department'. These parts of the JSON are also circled in orange. At the bottom, there is a legend indicating that 'bold red' text signifies required fields, and a blue 'EXECUTE' button.

Try it!

Use the APIs Explorer below to call this method on live data and see the response.

Authorize requests using OAuth 2.0: ☒

userKey `40G1occk12gapps.mcnc.` Email or immutable Id of the user. If Id, it should match with id of user object (string)
This parameter was URL encoded.

fields Selector specifying which fields to include in a partial response.
[Use fields editor](#)

Patch body

```
{
  "customSchemas": [
    {
      "Department": " "
    },
    {
      "Department": {
        "value": "STUDENT",
        "customType": "Department"
      }
    }
  ]
}
```

bold red = required [EXECUTE](#)

Authorization - populating Department schema in Google (web)



```
200
- SHOW HEADERS -
- {
  "kind": "admin#directory#user",
  "id": "114273000339697970674",
  "etag": "\"XGyyUMiAmCo7o31SWwFDDNla4RE/4fz1fFvrWWD4WawsZIbZ0ue_IUw\"",
  "primaryEmail": "40glocc@k12gapps.mcnc.org",
  "name": {
    "givenName": "40",
    "familyName": "Glocc",
    "fullName": "40 Glocc"
  },
  "isAdmin": false,
  "isDelegatedAdmin": false,
  "lastLoginTime": "2016-08-08T17:41:02.000Z",
  "creationTime": "2016-08-03T19:50:14.000Z",
  "agreedToTerms": true,
  "suspended": false,
  "changePasswordAtNextLogin": false,
  "ipWhitelisted": false,
  "emails": [
    {
      "address": "40glocc@k12gapps.mcnc.org",
      "primary": true
    }
  ],
  "customerId": "C01k0d5zn",
  "orgUnitPath": "/PWM/MainETeachers",
  "isMailboxSetup": true,
  "includeInGlobalAddressList": true,
  "customSchemas": {
    "Department": {
      "Department": [
        {
          "customType": "Department",
          "value": "STUDENT"
        }
      ]
    }
  }
}
```

Authorization - adding Department (and/or Group) schema in Google with GAM



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

The screenshot shows a YouTube video player with the URL https://www.youtube.com/watch?v=_dybYXJpBH0 in the address bar. The video content is a presentation slide titled "Google Apps Manager". The slide features the following elements:

- Logos for Google+, MCNC (Connecting North Carolina's Future Today), and NCREN.
- The GEG North Carolina logo.
- Contact information for John Warf: jwarf@mcnc.org.
- A Google Apps EDU Certified Trainer badge.
- Text: "We will start in just a moment, allowing folks to join."
- Text: "Today's Presentation - <http://goo.gl/thLQBd>"
- Text: "Sign In for Today - <http://goo.gl/cEczR6>"

The MCNC logo is also visible in the bottom right corner of the slide.

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 multivalued STUDENT

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

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

gam update user vct@k12gapps.mcnc.org Groups.Groups multivalued
nonstudent@k12gapps.mcnc.org

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

gam update user 50cent@k12gapps.mcnc.org Department.Department multivalued FRONTOFFICE
Department.Department multivalued 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:

Authorization - populating new users, OUs, Departments (and/or Group) schema in Google GAM csv



Gam to create new users.

File is testuser.csv:

fullname	Email	firstname	lastname	orgUnitPath	Password	Ggroup	Zscaler_Dept	Zscaler_Group
MrKila	MrKila@k12gapps.mcnc.org	Mr	Kil	/PWM/MainETeachers	Qwerty1234!	eteachers@k12gapps.mcnc.org	TEACHERS	nons
MrGlocc	MrGlocc@k12gapps.mcnc.org	Mr	Gloc	/PWM/MainETeachers	Qwerty1234!	eteachers@k12gapps.mcnc.org	TEACHERS	nons

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

A	W	AG
primaryEmail	orgUnitPath	Department
100kila@k12gapps.mcnc.org	/PWM/MainETeachers	STUDENT
12gauge@k12gapps.mcnc.org	/PWM/NorthMStudents	STUDENT
2chainz@k12gapps.mcnc.org	/PWM/EastEStudents	STUDENT
2pistols@k12gapps.mcnc.org	/PWM/EastETeachers	STUDENT
abrahamlincoln@k12gapps.mcnc.org	/PWM/MainETeachers	STUDENT
abstractrude@k12gapps.mcnc.org	/PWM/Admins	NONSTUDENT
acehood@k12gapps.mcnc.org	/PWM/SouthMStudents	STUDENT
actionbronson@k12gapps.mcnc.org	/PWM/HTeachers	STUDENT
adamsaleh@k12gapps.mcnc.org	/PWM/WestEStudents	STUDENT
andre3000@k12gapps.mcnc.org	/PWM/Admins	NONSTUDENT
andrenickatina@k12gapps.mcnc.org	/PWM/NorthMTeachers	STUDENT
andygriffith@k12gapps.mcnc.org	/PWM/NorthMStudents	STUDENT
andymineo@k12gapps.mcnc.org	/PWM/MainETeachers	STUDENT
andyrooney@k12gapps.mcnc.org	/PWM/HTeachers	STUDENT

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

Authorization - department/group attribute mapping in Google



≡ Apps > SAML Apps > Settings for Zscaler



Zscaler

ON for everyone

Service Provider Details

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

^ Attribute Mapping

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

Email	Basic Information ▼	Primary Email ▼
Department	Department ▼	Department ▼
Groups	Groups ▼	Groups ▼

Authorization - configuring SAML in Zscaler



The image shows the Zscaler web interface for configuring SAML. The left sidebar contains navigation links: Settings, Authentication, Authentication Settings (selected), User Management, Administration Controls, Administrator Management, Role Management, Audit Logs, Backup & Restore, and Resources. The main content area is titled "Edit SAML" and is divided into three sections: Identity Provider (IDP) Options, Service Provider (SP) Options, and Auto-Provisioning Options. Several fields are highlighted with orange boxes.

Identity Provider (IDP) Options

- SAML Portal URL**:
- Login Name Attribute**:
- Public SSL Certificate**: [Upload](#)

Service Provider (SP) Options

- Sign SAML Request**: ☒ [×](#)
- Request Signing SSL Certificate**:
- SP's Public SSL Certificate**: [Download](#)
- SP's Metadata**: [Download](#)

Auto-Provisioning Options

- Enable SAML Auto-Provisioning**: ☒
- User Display Name Attribute**:
- Group Name Attribute**:
- Department Name Attribute**:

Authorization - department/group behavior



	Department	Groups
Single-membership appearance in logs?	Yes	No
Single-membership filtering decisions?	Yes	Yes
Multiple-membership appearance in logs?	No*	No
Multiple membership filtering decisions?	No*	Yes

* 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: /PWM/WestEStudents
```

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



Advanced Threat Protection

Behavioral Analysis

Browser Control

ACCESS CONTROL

URL & Cloud App Control

File Type Control

Bandwidth Control

SSL Inspection

FTP Control

DATA LOSS PREVENTION

Data Loss Prevention

Mobile

URL FILTERING POLICY

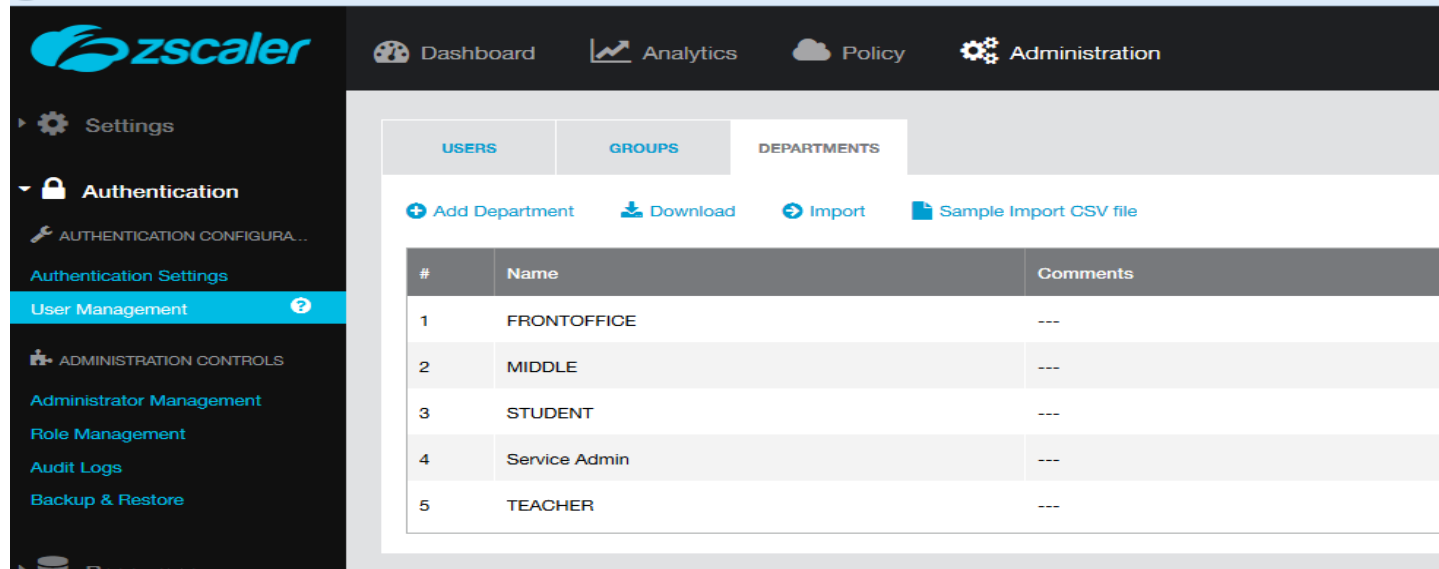
CLOUD APP CONTROL POLICY

ADVANCED POLICY SETTINGS

+ Add URL Filtering Rule

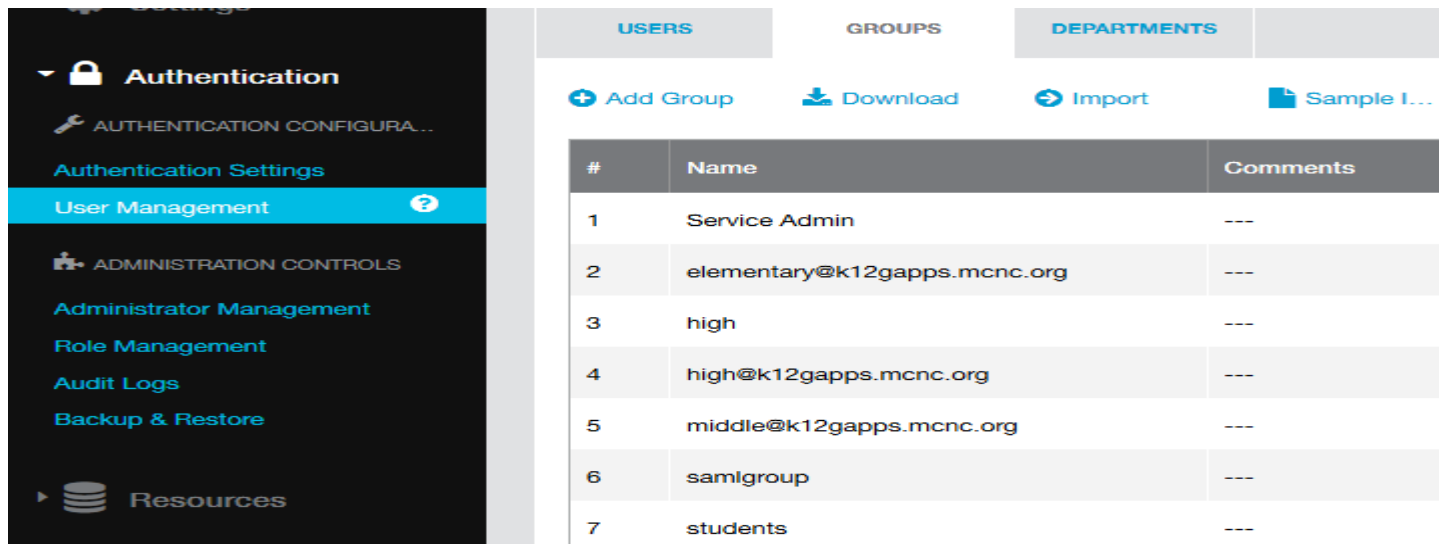
Rule Order	Criteria	Action
1	DEPARTMENTS FRONTOFFICE URL CATEGORIES Lingerie/Bikini; Alcohol/Tobacco	Allow
2	DEPARTMENTS TEACHERS URL CATEGORIES Drugs	Allow
3	GROUPS middle@k12gapps.mcnc.org URL CATEGORIES Gambling	Allow
4	GROUPS high@k12gapps.mcnc.org URL CATEGORIES Profanity	Allow

Authorization - auto-provisioning



The screenshot shows the Zscaler User Management interface. The left sidebar contains the Zscaler logo and navigation links: Settings, Authentication (with a sub-link for AUTHENTICATION CONFIGURA...), ADMINISTRATION CONTROLS (with sub-links for Administrator Management, Role Management, Audit Logs, and Backup & Restore), and Resources. The main content area has tabs for USERS, GROUPS, and DEPARTMENTS. The DEPARTMENTS tab is active, showing a table with 5 rows. Above the table are links for Add Department, Download, Import, and a Sample Import CSV file.

#	Name	Comments
1	FRONTOFFICE	---
2	MIDDLE	---
3	STUDENT	---
4	Service Admin	---
5	TEACHER	---



The screenshot shows the Zscaler User Management interface with the GROUPS tab active. The left sidebar is identical to the previous screenshot. The main content area shows a table with 7 rows. Above the table are links for Add Group, Download, Import, and a Sample I... file.

#	Name	Comments
1	Service Admin	---
2	elementary@k12gapps.mcnc.org	---
3	high	---
4	high@k12gapps.mcnc.org	---
5	middle@k12gapps.mcnc.org	---
6	samlgroup	---
7	students	---

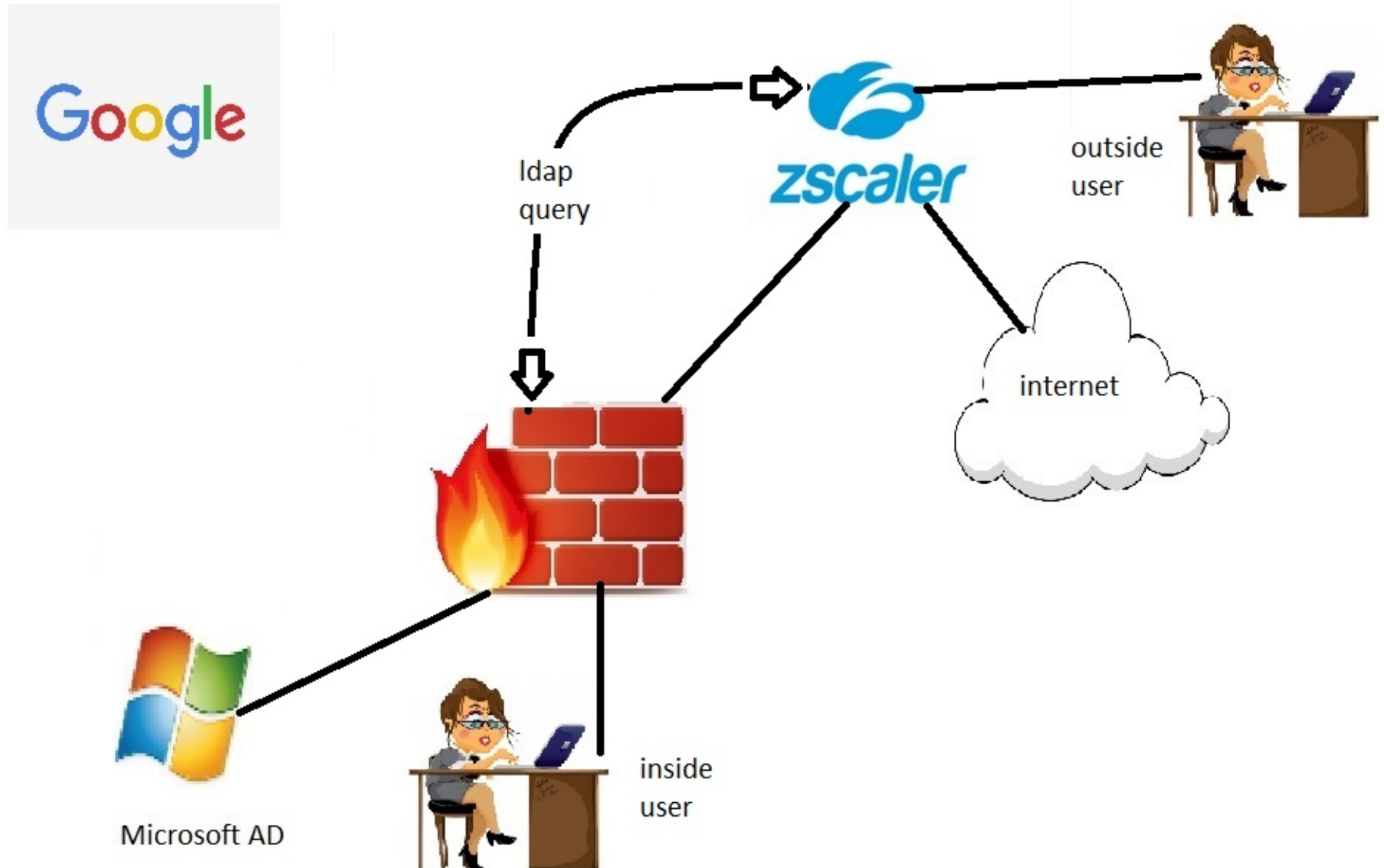
Accounting - logs



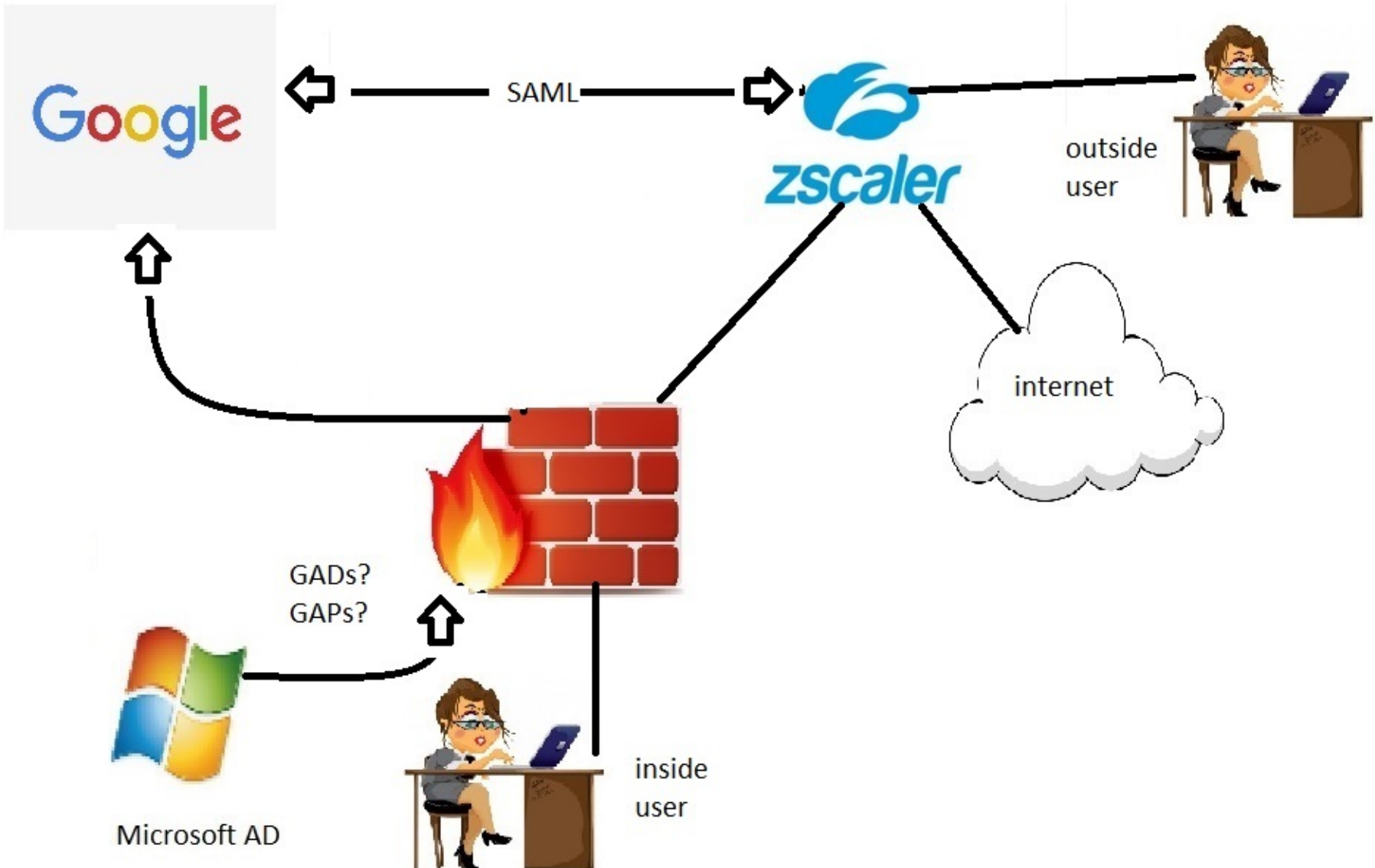
.

No.	Logged Time	User	URL	Policy Action	Department
1	Tuesday, August 09,...	greenfrog@k12gapps.mcn...	www.bing.com/	Not allowed to...	GRADEONE
2	Tuesday, August 09,...	greenfrog@k12gapps.mcn...	www.bing.com/favicon.ico	Not allowed to...	GRADEONE
3	Tuesday, August 09,...	bigcootie@k12gapps.mcn...	porn.com/	Not allowed to...	STUDENT
4	Tuesday, August 09,...	bigcootie@k12gapps.mcn...	porn.com/favicon.ico	Not allowed to...	STUDENT
5	Tuesday, August 09,...	bigcootie@k12gapps.mcn...	www.wine-searcher.com/find/thunderbird+the...	Not allowed to...	STUDENT
6	Tuesday, August 09,...	bigcootie@k12gapps.mcn...	www.wine-searcher.com/favicon.ico	Not allowed to...	STUDENT
7	Tuesday, August 09,...	40glocc@k12gapps.mcnc....	www.winespectator.com/	Not allowed to...	STUDENT
8	Tuesday, August 09,...	40glocc@k12gapps.mcnc....	www.winespectator.com/favicon.ico	Not allowed to...	STUDENT

AD - no SAML



SAML with AD



Caveats



,

Platform	Chrome	Firefox	Google-drive-app	MIE	Safari
Chromebook	x	N/A	N/A	N/A	N/A
ipad	x	N/A	x	N/A	x
Microsoft	x	x	x	x	N/A
Macbook	x	x	x	N/A	x

Caveats



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

The screenshot shows the MCNC website with the URL <https://www.mcnc.org/our-community/k12/docs/web-security/category-definitions> in the browser address bar. The page features the MCNC logo and a navigation menu. The main content area is titled 'DEFAULT CATEGORY DEFINITIONS' and contains several sections with category definitions and lists of domains.

MCNC
Connecting North Carolina's Future Today

Media | Careers | Directions | Contact Us

SEARCH

K12

Public Schools of North Carolina
State Board of Education
Department of Public Instruction

K12

- [K12](#)
- [News](#)
- [Services](#)
- [Documentation & Training](#)
- [Facts & Additional Information](#)
- [NCREN Utilization Map - K-12](#)
- [DPI Connectivity Services](#)
- [Support & Contacts](#)

Resources

- [Edspace](#)
- [Portal](#)
- [Knowledgebase](#)

DEFAULT CATEGORY DEFINITIONS

Dual-categorization should be avoided in Zscaler. An example of dual-categorization is having [.apple.com](#) in custom list "A" and custom list "B". If [apple.com](#) traffic is to be processed differently, for example, excluded from authentication and SSL-filtering, one would create a single list, custom list "C" containing [.apple.com](#). Then list "C" would be excluded from authentication under authentication exclusions and from SSL-filtering under SSL exclusions.

AES - add to no authentication

- [.kidsandcomputers.com/starter.htm](#)
- [.brainbuzz.com/](#)
- [.cramsession.com/](#)

Chromebooks - add to no authentication and no ssl inspection

- [sites.google.com](#)
- [groups.google.com](#)
- [video.google.com](#)

Child Nutrition - add to no authentication

- [.lunchprepay.com](#)
- [.lunchapplication.com](#)
- [.mealsplus.com](#)

E-Procurement - add to no ssl inspection

- [.hubadmin.ncgov.com](#)

G Drive - add to no authentication and no ssl inspection

- [.docs.google.com](#)
- [ssl.gstatic.com](#)
- [.spreadsheets.google.com](#)

iTunes-Bypass - add to no authentication and no ssl inspection

Caveats



Choose an account



Unknown Unknown

bigcootie@k12gapps.mcnc.org



Dianne Dunlap

dianne@k12gapps.mcnc.org



40 Glocc

40glocc@k12gapps.mcnc.org



j ane

janedoe@k12gapps.mcnc.org




Add account

Remove

Caveats



ip.zscaler.com/cgi-bin/index.cgi



Your request is arriving at this server from the IP address **152.26.210.24**

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: **40glocc@k12gapps.mcnc.org**.

Logout

Caveats

A screenshot of a web browser window. The address bar shows the URL: https://gateway.zscalerone.net/auF?url=http%3A%2F%2Fwww%2Ebing%2Ecom%2F&ordtok=PsZ3WVRVKk0DDsqkKtssTDPPrPt&sm_af=EXP. The page content is a sign-in form with a green border. The form has a title "Sign In" with a person icon, a message "To keep you safe from internet threats, please sign in to your company's security service.", a "User Name" label, a text input field with placeholder text "Enter your User Name...", a blue "Sign In" button, and a link "Need help? Contact your IT support." at the bottom.

Sign In

To keep you safe from internet threats, please sign in to your company's security service.

User Name

Sign In

[Need help? Contact your IT support.](#)

Questions?



■ 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