Onboard and Cloud Identity Providers

aruba

a Hewlett Packard Enterprise company

ClearPass

Configuration Guide

Change Log

Version	Date	Modified By	Comments
2018-01	10/8/18	Tim Cappalli	Updated to include Google Secure LDAP Connector
2017-01	7/10/17	Tim Cappalli	Public Release

Copyright

Contents

Overview

This document is designed to provide step-by-step configuration guidance for using Azure Active Directory, Google Cloud Identity and Okta as identity stores for ClearPass Onboard device enrollment of BYOD and/or corporate devices.

This configuration guide is very focused and will cover:

- creating the required application in the cloud identity provider
- configuring the ClearPass SAML Service Provider and OAuth 2.0 Relying Party
- Onboard provisioning settings changes required for SAML and OAuth 2.0
- customizing the ClearPass SSO dictionary
- building a SAML pre-authentication service for Onboard
- real-time authorization for Google Cloud Identity

Most cloud identity providers do not store credentials in the legacy format, NT hash, which is commonly used with Active Directory Domain Services and required to support 802.1X authentication via PEAPv0/EAP-MSCHAPv2. This EAP method is very popular due to the native support in most major operating systems and user familiarity with username and password.

The protocol dependencies, configuration complexities and well-known security concerns with PEAPv0/EAP-MSCHAPv2 (and EAP-TTLS) have shifted the focus over to EAP-TLS, the gold standard for 802.1X authentication, which uses client certificates.

Client certificates for network authentication have many benefits including:

- strong, mutual authentication between the authentication server and the client
- a unique device identity associated with a user or group
- the ability to revoke individual device access independent of the user account
- user passwords are not stored on the device
- there is no risk of credential interception via man-in-the-middle attacks
- there is no dependency on traditional Active Directory NT hashes
- certificates issued for network access can be used for other services like single sign-on and traditional web authentication

ClearPass can leverage either Security Assertion Markup Language (SAML) or OAuth 2.0 to authorize against cloud identity providers. The table below breaks down which method is supported in ClearPass for each provider.

Protocol	Microsoft **Azure AD**	Google **G Suite**	**Okta**
OAuth 2.0	✔	✔	✘
SAML	✔	✔	✔

Microsoft Azure Active Directory

ClearPass can leverage Azure Active Directory as an identity provider for Onboard via SAML or OAuth 2.0.

When a user initiates the Onboard process, usually by clicking the Onboard link on a guest portal, they will be redirected straight to the Microsoft Login page. After a successful authentication (and potential MFA challenge), they will be redirected to ClearPass Onboard to begin device enrollment.

Below is a comparison between the two technologies and which features and workflows are available with each authentication method.

Feature	SAML	OAuth 2.0
Requires User Consent Dialog	✗	✓
Group Membership	✗	✓
Requires Azure Active Directory Premium	✓	✗
Workflow Specific Features	**SAML**	**OAuth 2.0**
Evaluate return attributes during Onboard pre-authentication	✓	✗
Evaluate return attributes during subsequent EAP-TLS authentication/authorization	✗	✓

Below is the list of available return attributes for SAML and OAuth 2.0.

User Entity Return Attributes	
SAML	**OAuth2**
assignedroles	objectType
city	objectId
companyname	accountEnabled
country	assignedLicenses
department	city
displayname	companyName

dnsdomainname	country
facsimiletelephonenumber	department
givenname	dirSyncEnabled
jobtitle	displayName
mail	extension_*
mailnickname	facsimileTelephoneNumber
netbiosname	givenName
objectid	groups (Names)
onpremisesecurityidentifier	groups (Emails)
onpremisessamaccountname	immutableId
otherMail	jobTitle
physicaldeliveryofficename	lastDirSyncTime
postalcode	mail
preferredlanguage	mailNickname
state	mobile
streetaddress	onPremisesDistinguishedName
surname	onPremisesSecurityIdentifier
telephonenumber	otherMails
userprincipalname	passwordPolicies
	passwordProfile
	physicalDeliveryOfficeName
	postalCode
	preferredLanguage
	provisionedPlans
	provisioningErrors
	proxyAddresses
	sipProxyAddress
	state
	streetAddress
	surname
	telephoneNumber
	usageLocation
	userPrincipalName
	userType

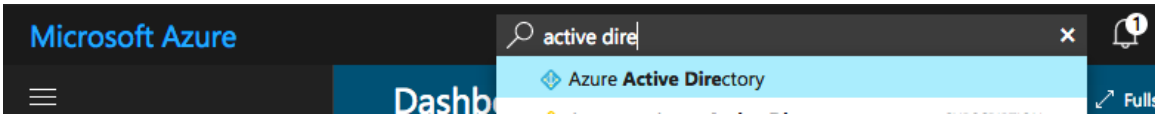
SAML

Azure Active Directory Configuration

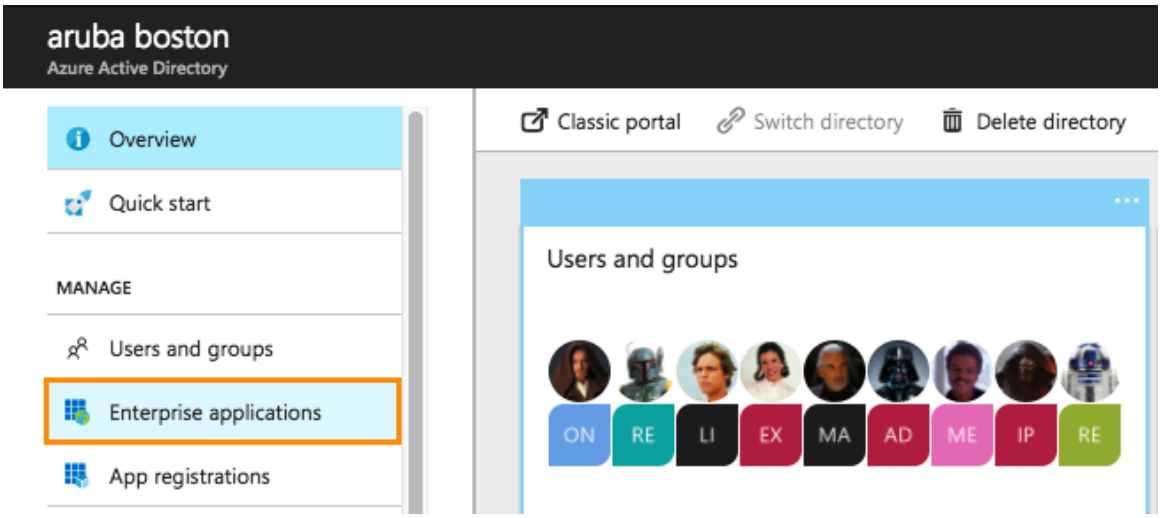
Application Setup

Log into the Microsoft Azure Portal at portal.azure.com. Depending on the Azure IAM policy, you may need to log in as a Global Administrator.

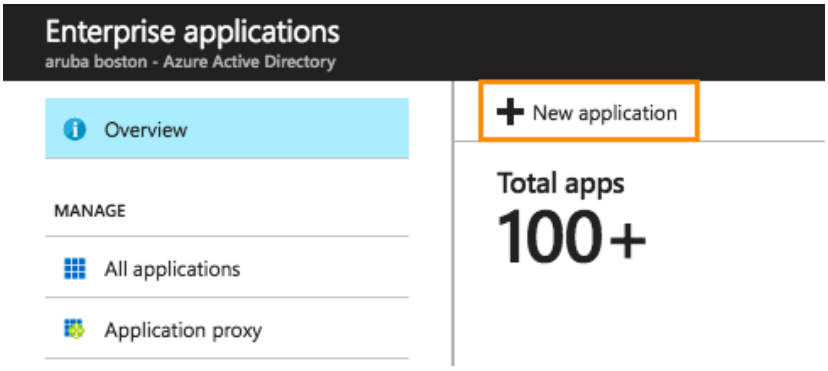
Using the search bar at the top, search for and select **Azure Active Directory**.



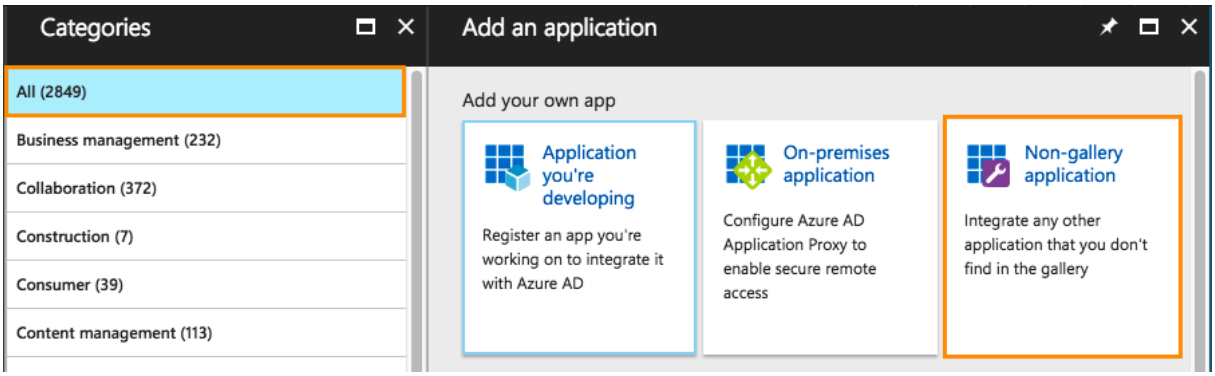
In the Azure Active Directory navigation blade, select **Enterprise applications**.



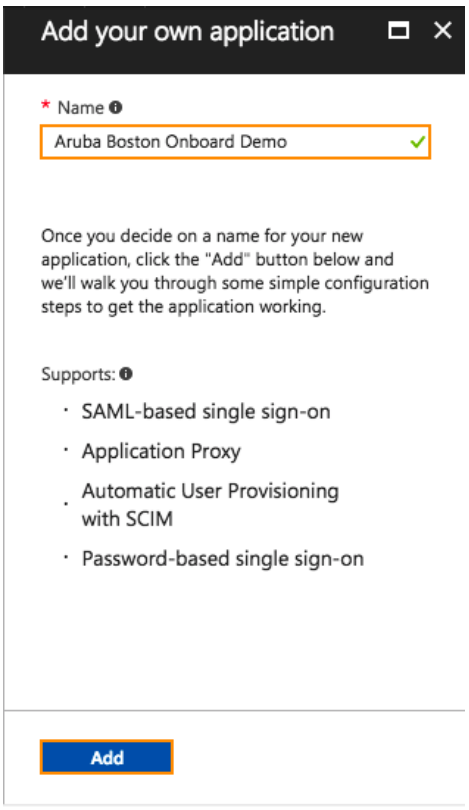
From the Enterprise applications overview blade, select **New application**.



From the Categories list, select **All** and then choose **Non-gallery application** from the application pane.

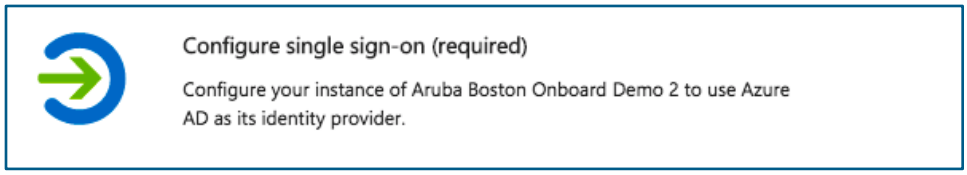


Give the application a **Name** and click **Add**.



SAML Configuration

You will be redirect to the Quick start blade for the app. Select **Configure single sign-on** from the list.



From the **Mode** dropdown list, select **SAML-based Sign-on**.

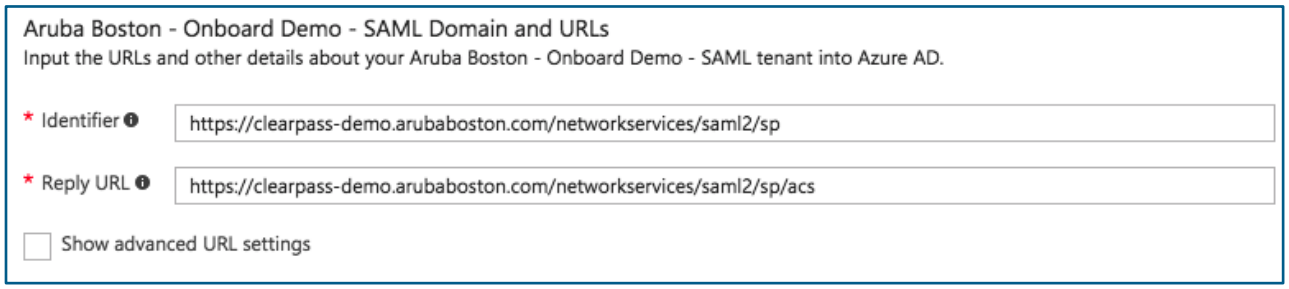
Next is the ClearPass SAML service provider configuration under **Domain and URLs**.

The **Identifier** is the SAML Entity ID URL and is the same in all ClearPass installations. Replace <fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

```
https://<clearpass-fqdn>/networkservices/saml2/sp
```

The **Reply URL** is the SAML Assertion Consumer Service and is the same in all ClearPass installations. Replace <fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

```
https://<clearpass-fqdn>/networkservices/saml2/sp/acs
```



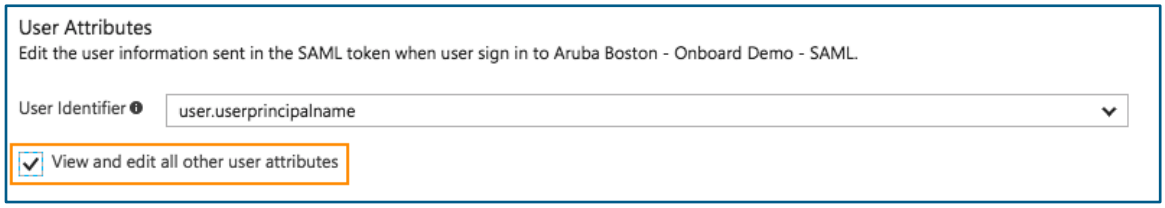
Down in **User Attributes**, userprincipalname will be used by default as the SAML Name Identifier. If there is a need to use a different attribute (such as a custom attribute synced from on premise AD), an alternative can be selected from the drop-down list.

The following token attributes are preconfigured to be sent back to ClearPass in the SAML assertion:

- userprincipalname
- givenname
- surname
- emailaddress
- name

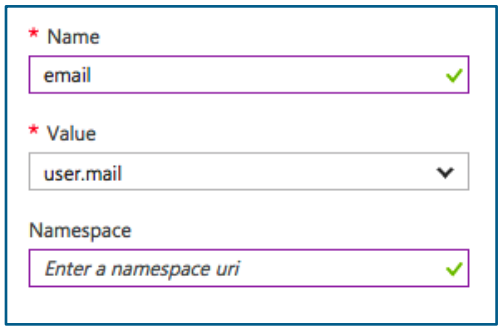
A few modifications need to be made and additional attributes can also be added. These changes to the SAML Token Attributes are only required if return attributes will be used as part of the Onboard enrollment policy decision.

Check **View and edit all other user attributes**.

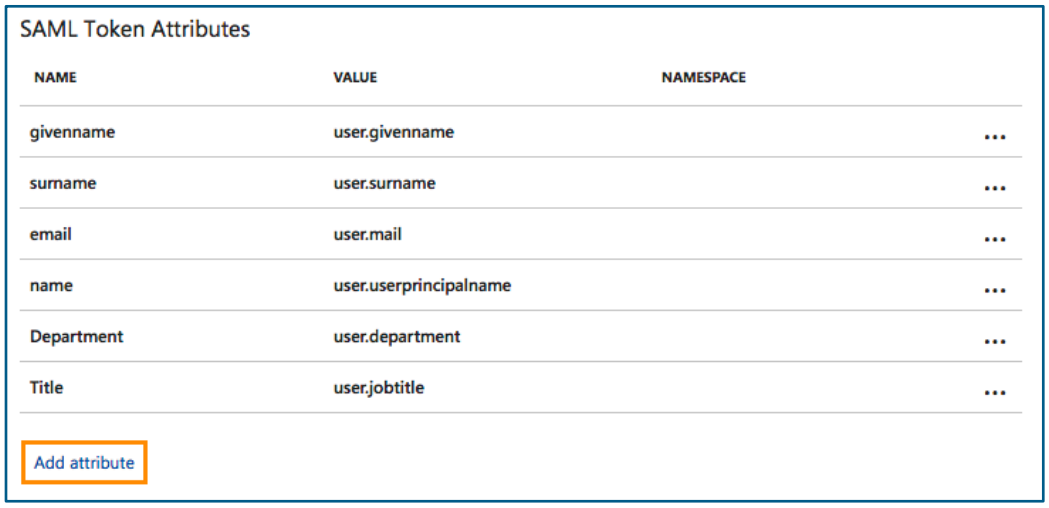


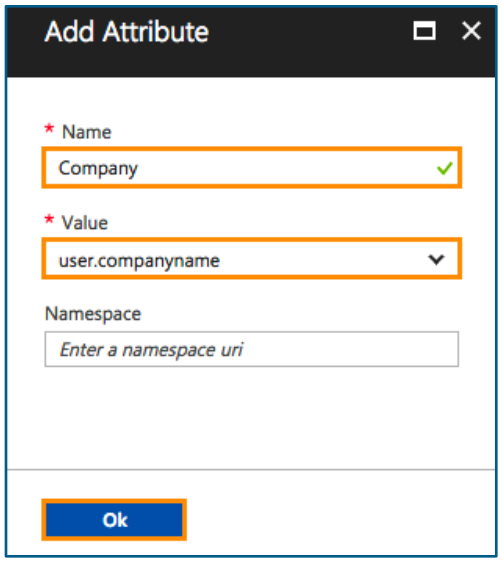
For each of the 4 pre-populated attributes, remove the Namespace data by clicking the attribute, clearing the Namespace field, and then clicking OK.

For the **emailaddress** attribute, change the Name to just **email** along with clearing the **Namespace** field.

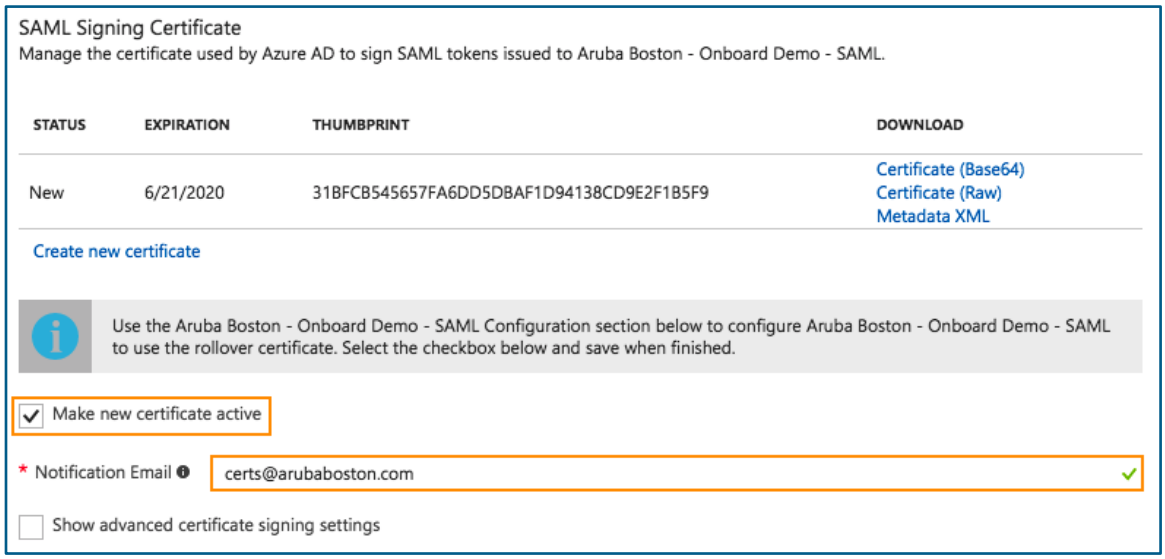


To add additional attributes, click **Add attribute**. In this example, ***Department***, ***Title*** and ***Company*** were added.

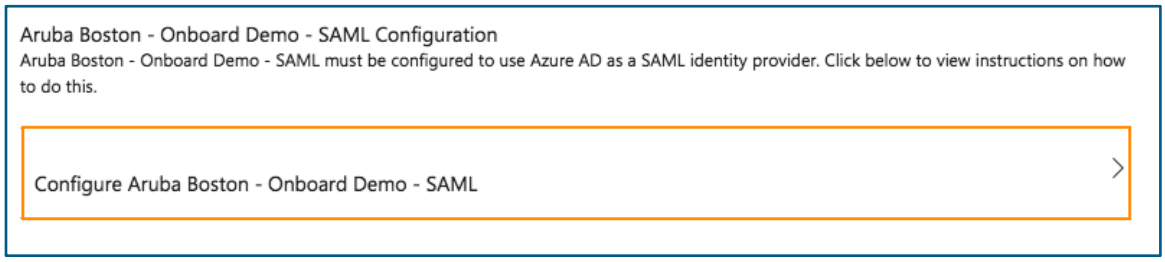




Down under SAML Signing Certificate, a new certificate has been generated. Check **Make new certificate active** and change the **Notification Email** address if necessary. If a certificate has not yet been generated, click **Create new certificate** and follow the prompts.

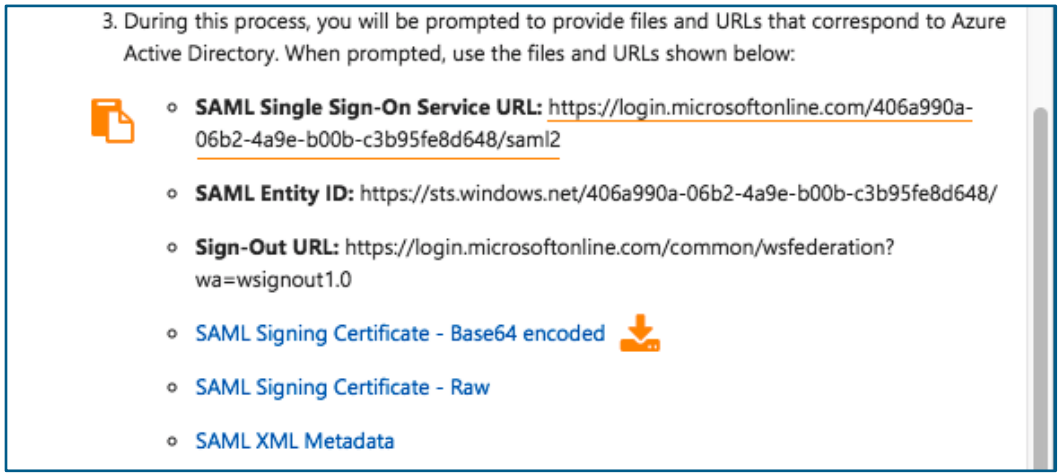


Next select the **Configure <application name>** widget at the bottom. This will take you to the configuration overview.

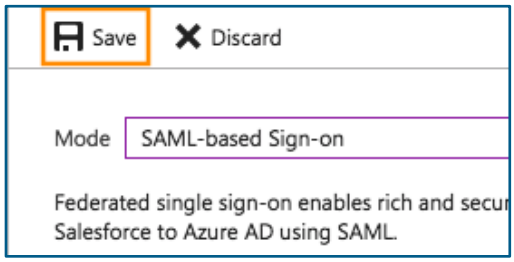


Scroll down and locate the **SAML Single Sign-On Service URL**. Save this value as it will be needed for the ClearPass Policy Manager configuration.

The SAML Signing Certificate will also be needed. Click on **SAML Signing Certificate – Base64 encoded** to download the certificate. This will be used by ClearPass to verify that the assertion was indeed signed by Azure Active Directory.



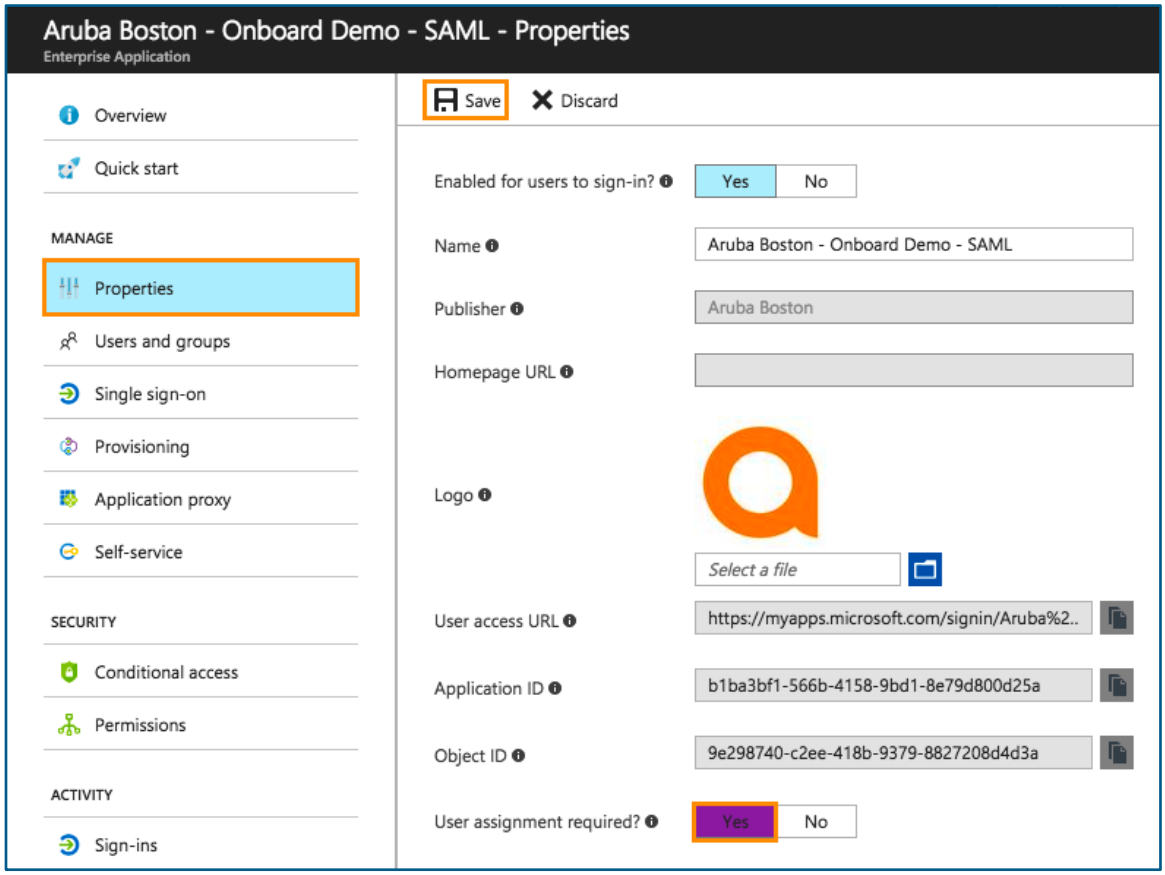
Now close the configuration overview pane with the **X** at the top right. Click the **Save** button at the top.



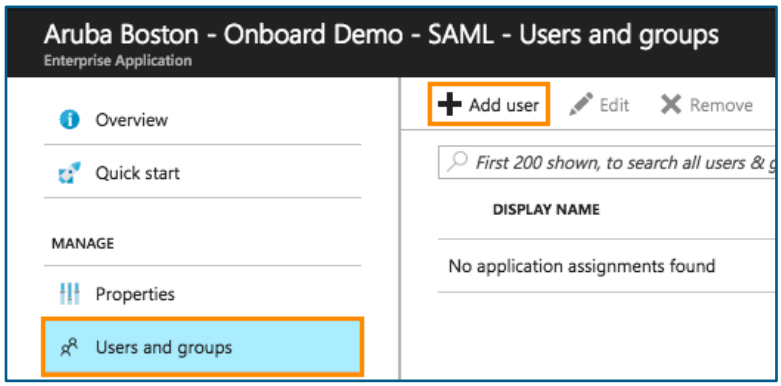
Restricting Access

By default, all users in the Azure Active Directory tenant will be able to authenticate against this SAML identity provider and be redirected back to ClearPass to continue with Onboard.

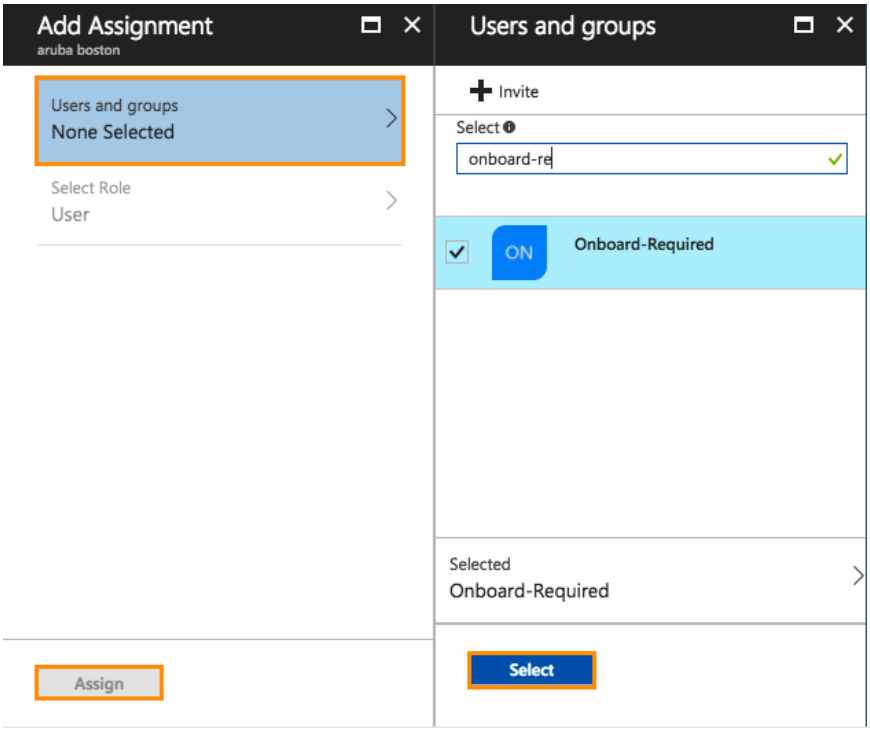
If there is a need to restrict access by group or user at the identity provider level, navigate to **Properties** in the menu blade and for **User assignment required**, select **Yes**. Click **Save** at the top.



Now navigate to **Users and groups** in the menu blade. Click **Add user** at the top.



Click **Users and group** and then search for the user(s) and/or group(s) that should be able to authenticate using this identity provider, then click **Select**. When finished, click **Assign**.



ClearPass Policy Manager Configuration

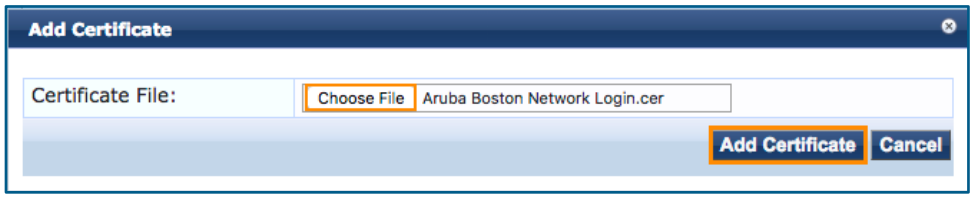
IdP Certificate

The first step in Policy Manager is to upload the identity provider certificate provided in the Azure portal.

Navigate to **Administration** » **Certificates** » **Trust List** and click **Add**.

Browse for the previously downloaded certificate and then click **Add Certificate**.

> **NOTE**: The certificate will be self-signed and have a common name of *Microsoft Azure Federated SSO Certificate*.



The certificate should now appear in the trust list as Enabled.

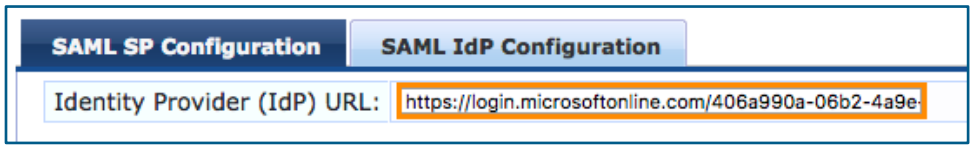
Service Provider Configuration

Next, Policy Manager needs to be configured to use Azure Active Directory as a SAML Identity Provider and enable it for use with Onboard workflows.

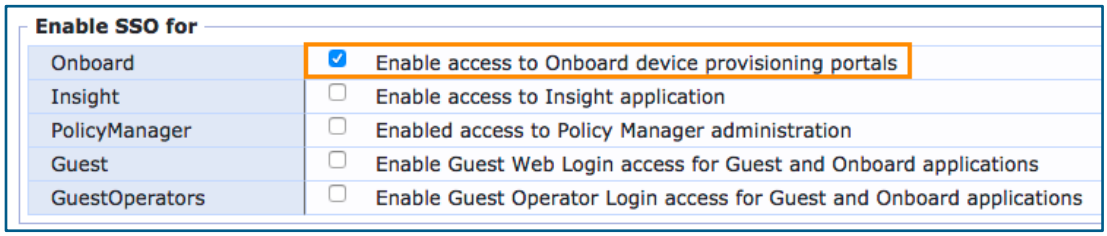
Navigate to **Configuration** » **Identity** » **Single Sign-On (SSO)**.

For Identity Provider (IdP) URL, enter in the **SAML Single Sign-On Service URL** from the Azure Active Directory configuration. The URL should look something like this:

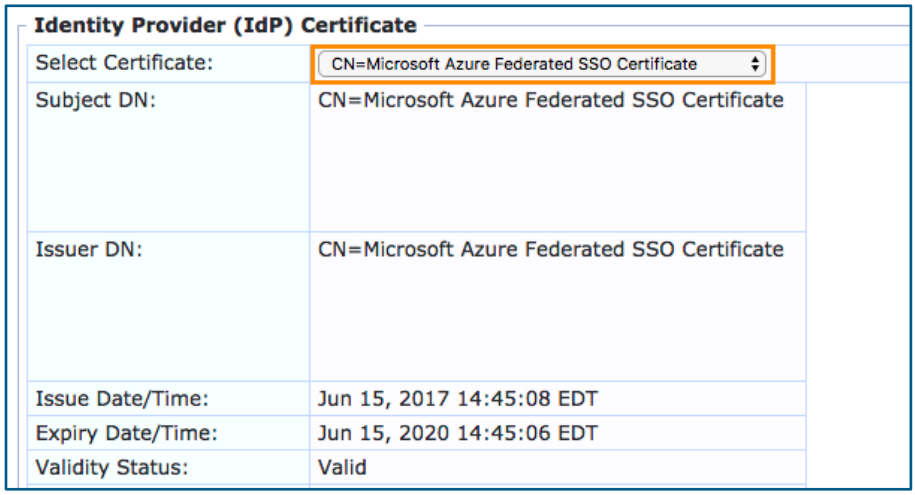
https://login.microsoftonline.com/<GUID>/saml2



Check **Enable access to Onboard device provisioning portals**.



Finally, select the **Microsoft Azure Federated SSO Certificate** from the drop-down list under **Identity Provider (IdP) Certificate**.



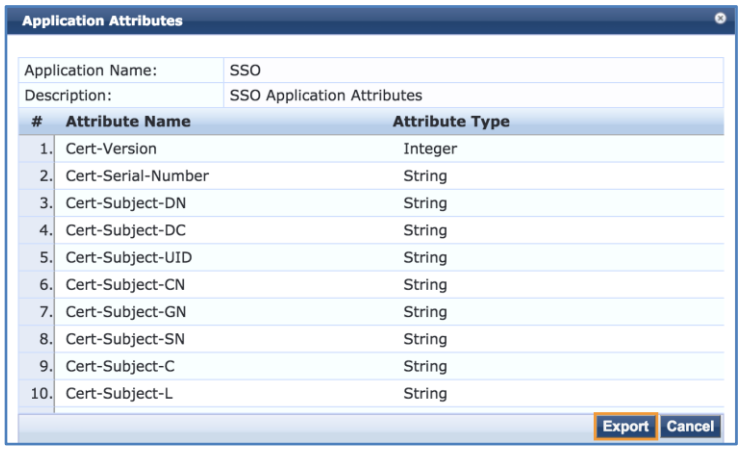
Click **Save** at the bottom.

Application Dictionary

If there is a need to assign different Onboard configuration overrides using SAML Token Attributes, the ClearPass SAML dictionary will need to be updated. Examples would be using a different certificate lifetime for different types of users or even using a different configuration profile. If SAML Token Attributes will not be used during Onboard pre-authentication, skip this step.

NOTE: Department, Title, and Company are available by default in ClearPass and do not require any changes to the SSO dictionary. Just be sure they are enabled in the Azure Active Directory SAML Token Attributes configuration.

Navigate to **Administration » Dictionaries » Applications**, click on SSO and then click **Export**.



Open the exported XML file in a text editor.

Add the SAML Token Attributes, following the same format as the existing entries. Below is an example for the displayname attribute.

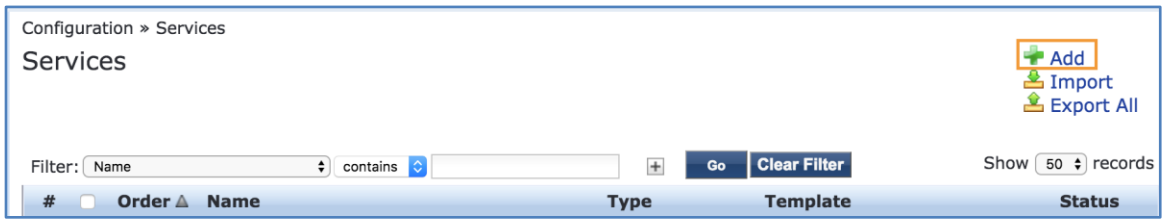
```
<ApplDictionaryAttributes attrType="String"
attrName="http://schemas.microsoft.com/identity/claims/displayname"/>
```

Once all of the desired attributes have been added, save the file and import it back into ClearPass.

Onboard Pre-Authentication Service

A new service will be required to handle the Onboard SAML pre-authentication.

Navigate to **Configuration » Services** and then click **Add**.

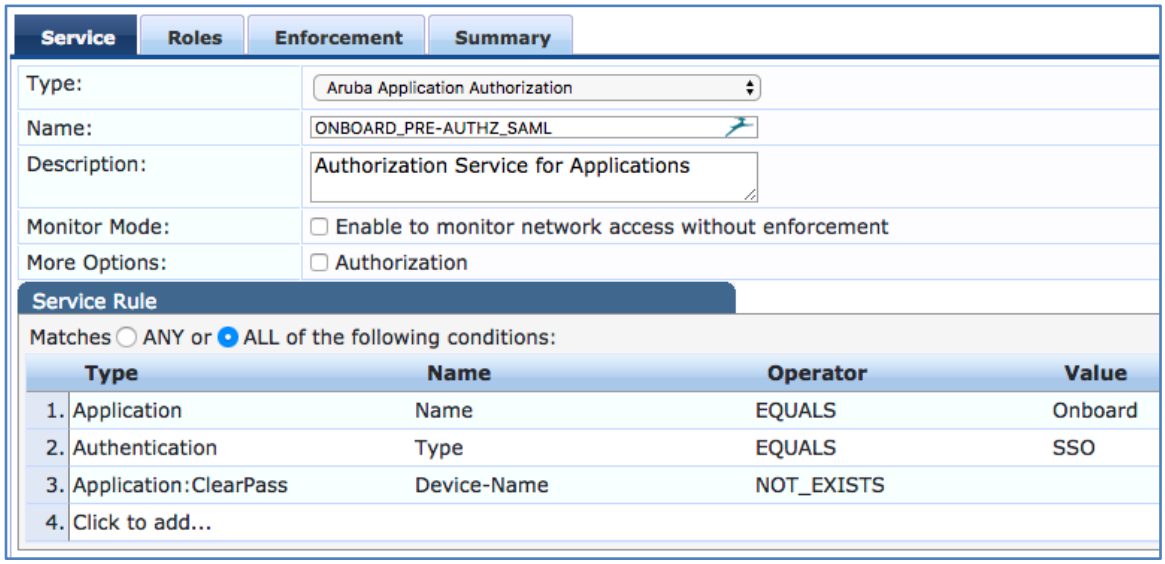


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD_PRE-AUTHZ_SAML* for example.

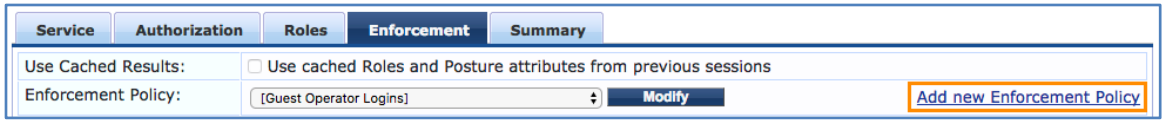
Uncheck the **Authorization** checkbox next to More Options.

Under **Service Rules**, use the following:

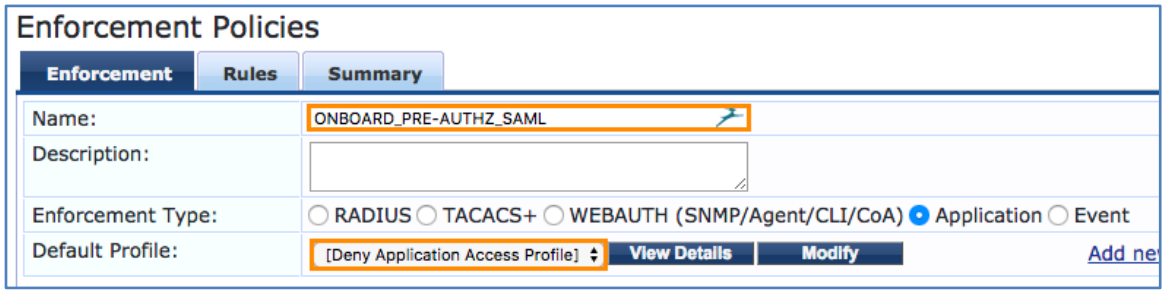
`Application`	`Name`	`EQUALS`	`Onboard`
`Authentication`	`Type`	`EQUALS`	`SSO`
`Application:ClearPass`	`Device-Name`	`NOT_EXISTS`	



Next skip over to the **Enforcement** tab and click **Add new Enforcement Policy**.



Give it the same name as the service and set the **Default Profile** to **[Deny Application Access Profile].**

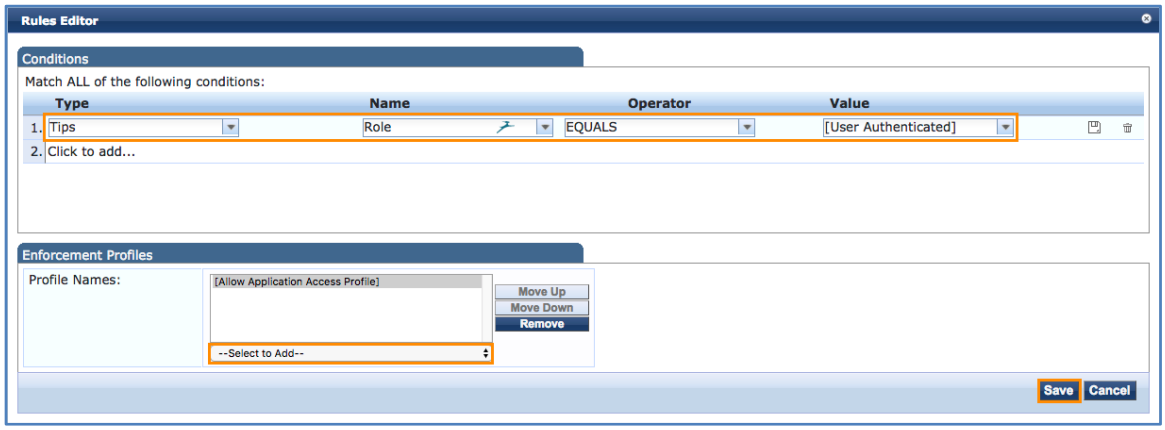


Move over to the **Rules** tab and click **Add Rule.**

Add the following condition:

```
TIPS        Role        EQUALS        [User Authenticated]
```

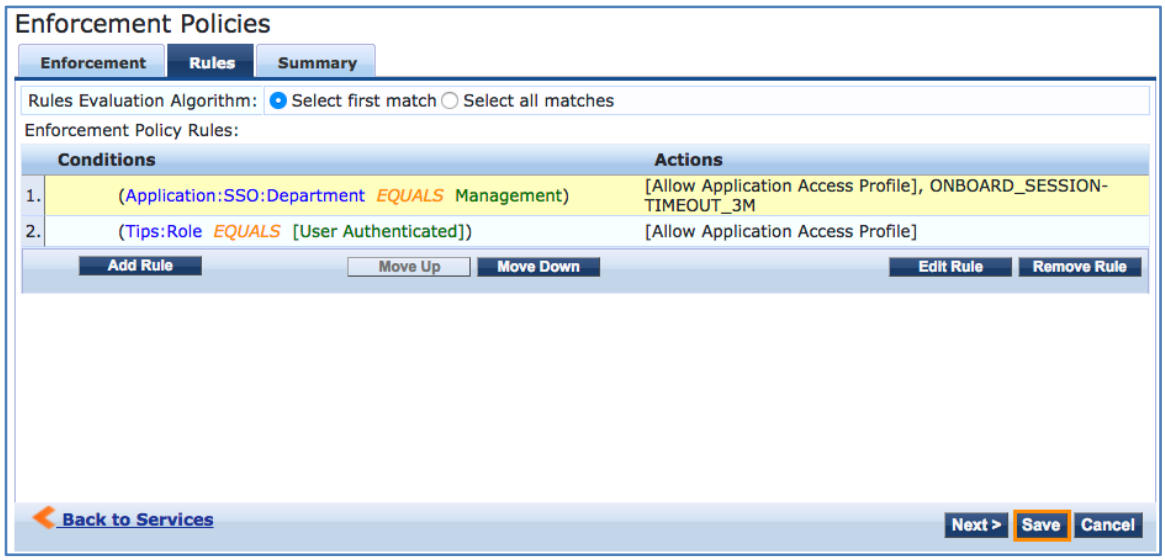
Select [Allow Application Access Profile] under Enforcement Profiles. Click Save.



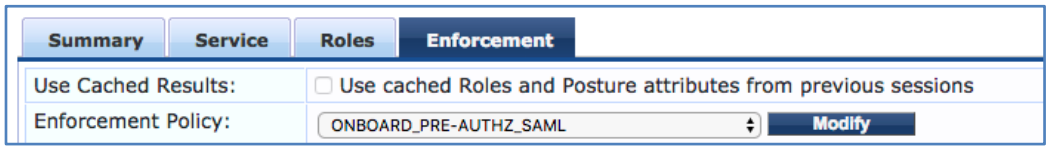
If return attributes from Azure Active Directory will be used in policy, add rules to reference the attributes in the ClearPass:SSO namespace. Below is an example for Department that overrides the certificate lifetime for “Management”.

(Application:SSO:Department *EQUALS* Management)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M

After all the rules have been defined, click **Save** at the bottom.



Now select the newly created Enforcement Policy from the drop-down list and then click **Save** at the bottom.

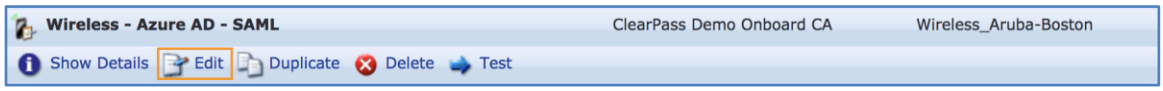


Move this newly created service above any other Onboard application services.

ClearPass Onboard Configuration

Very little configuration is required for SAML in Onboard.

Edit the Provisioning Settings under **Onboard » Deployment and Provisioning » Provisioning Settings**



In the authorization section, check **Single Sign-On – Enable SSO for device provisioning**, then click **Save Changes** at the bottom.

That's the only change required in the Onboard configuration.

NAD Whitelist

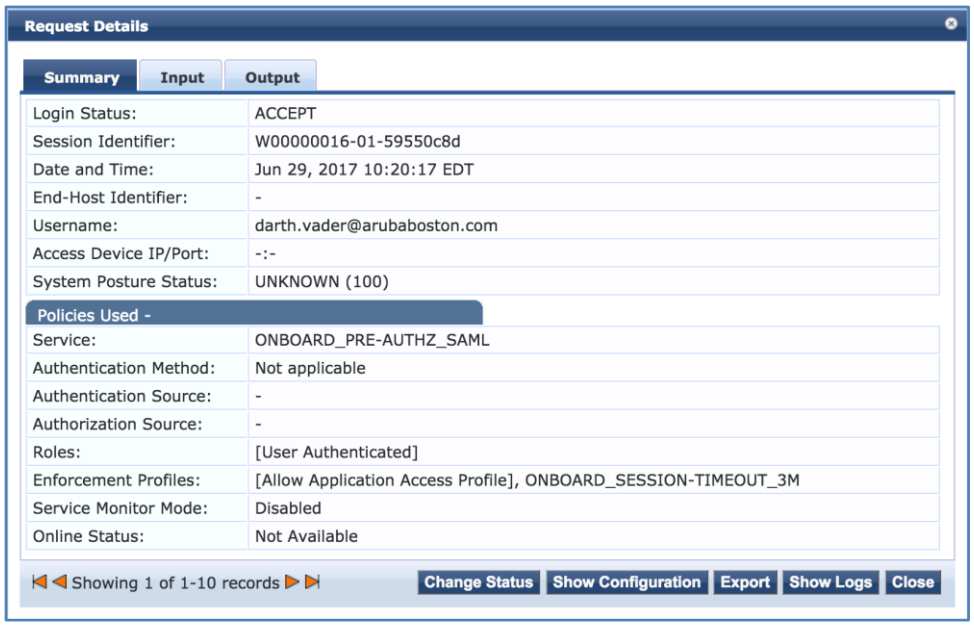
In order for clients to be able to reach the Azure Active Directory login page and other embedded resources, certain domain names need to be whitelisted.

The most up to date version of this whitelist as well as examples for Aruba mobility controllers and Aruba Instant are available on the Aruba GitHub: https://github.com/aruba/clearpass-cloud-service-whitelists.

Direct Link: https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_azure-active-directory.md

Sample Request

This first example shows a user with department Management which returns an override profile for the certificate lifetime.



Request Details

Summary | Input | Output

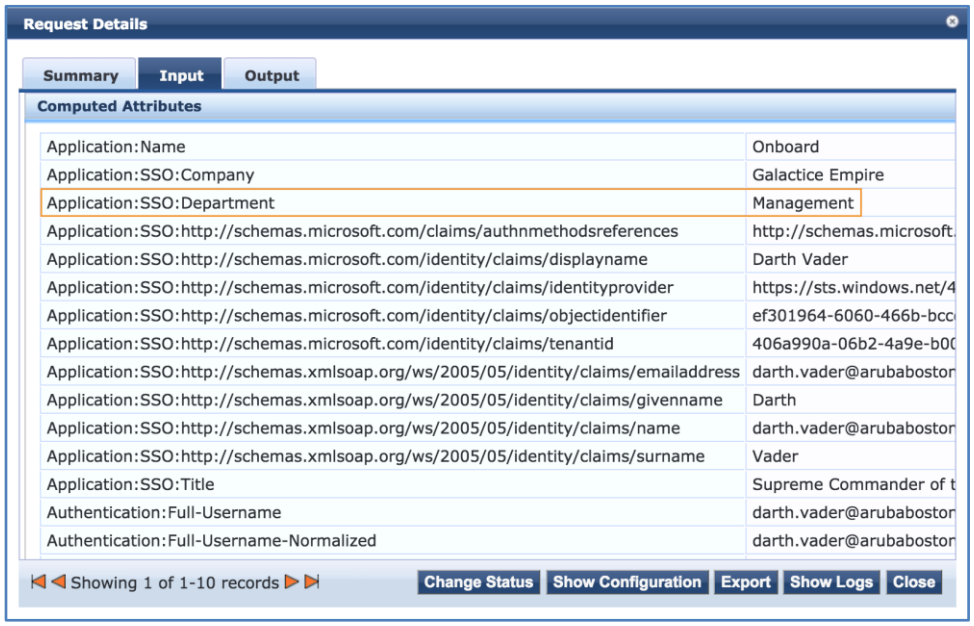
Login Status:	ACCEPT
Session Identifier:	W00000016-01-59550c8d
Date and Time:	Jun 29, 2017 10:20:17 EDT
End-Host Identifier:	-
Username:	darth.vader@arubaboston.com
Access Device IP/Port:	-:-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	ONBOARD_PRE-AUTHZ_SAML
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	[User Authenticated]
Enforcement Profiles:	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-10 records

Change Status | Show Configuration | Export | Show Logs | Close



Request Details

Summary | Input | Output

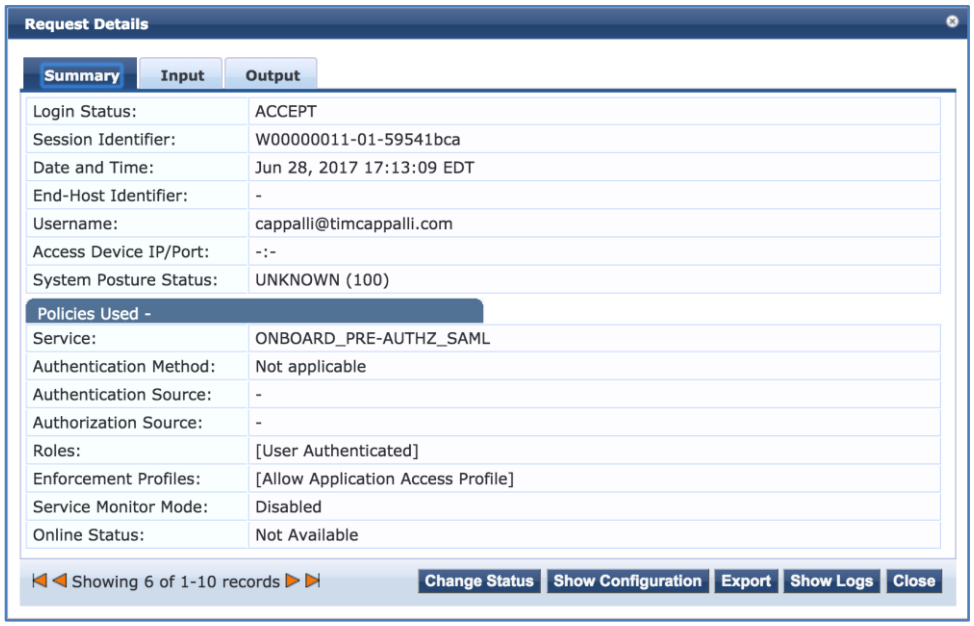
Computed Attributes

Application:Name	Onboard
Application:SSO:Company	Galactice Empire
Application:SSO:Department	Management
Application:SSO:http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.
Application:SSO:http://schemas.microsoft.com/identity/claims/displayname	Darth Vader
Application:SSO:http://schemas.microsoft.com/identity/claims/identityprovider	https://sts.windows.net/4
Application:SSO:http://schemas.microsoft.com/identity/claims/objectidentifier	ef301964-6060-466b-bcc
Application:SSO:http://schemas.microsoft.com/identity/claims/tenantid	406a990a-06b2-4a9e-b0
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	darth.vader@arubaboston
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Darth
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	darth.vader@arubaboston
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Vader
Application:SSO:Title	Supreme Commander of t
Authentication:Full-Username	darth.vader@arubaboston
Authentication:Full-Username-Normalized	darth.vader@arubaboston

Showing 1 of 1-10 records

Change Status | Show Configuration | Export | Show Logs | Close

This request is an example of the more common deployment which just checks to ensure that the user successfully authenticated and then permits the user to begin the Onboard process.



Request Details

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000011-01-59541bca
Date and Time:	Jun 28, 2017 17:13:09 EDT
End-Host Identifier:	-
Username:	cappalli@timcappalli.com
Access Device IP/Port:	-:-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	ONBOARD_PRE-AUTHZ_SAML
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	[User Authenticated]
Enforcement Profiles:	[Allow Application Access Profile]
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 6 of 1-10 records

Change Status | Show Configuration | Export | Show Logs | Close

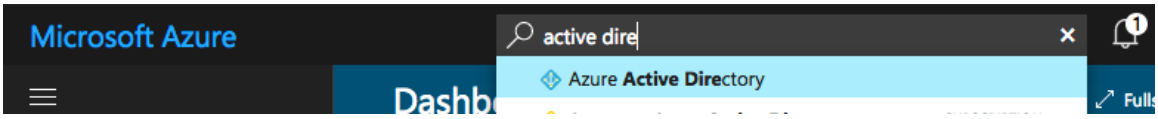
OAuth 2.0

Azure Active Directory Configuration

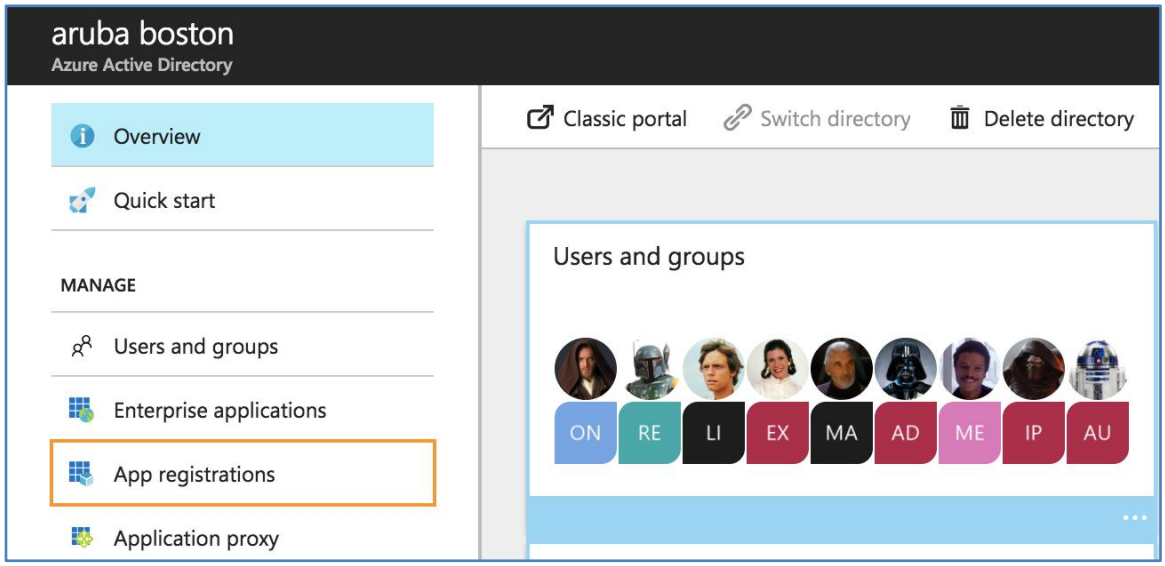
Application Setup

Log into the Microsoft Azure Portal at portal.azure.com. Depending on the Azure IAM policy, you may need to log in as a Global Administrator.

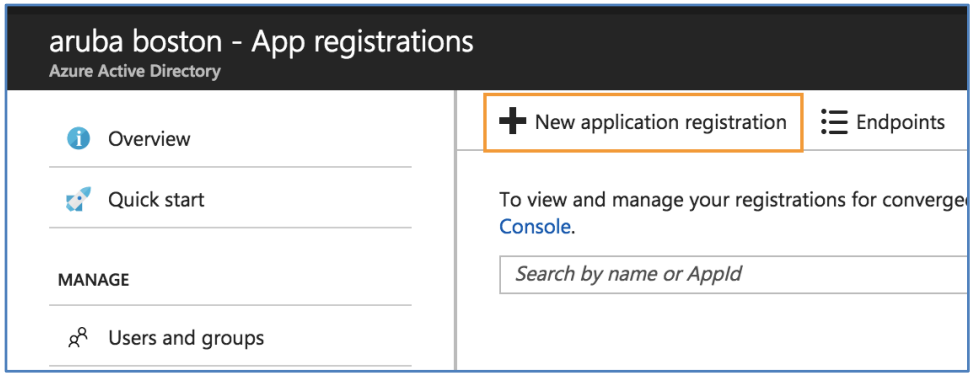
Using the search bar at the top, search for and select **Azure Active Directory**.



In the Azure Active Directory navigation blade, select **App registrations**.



From the App registrations overview blade, select **New application registration**.

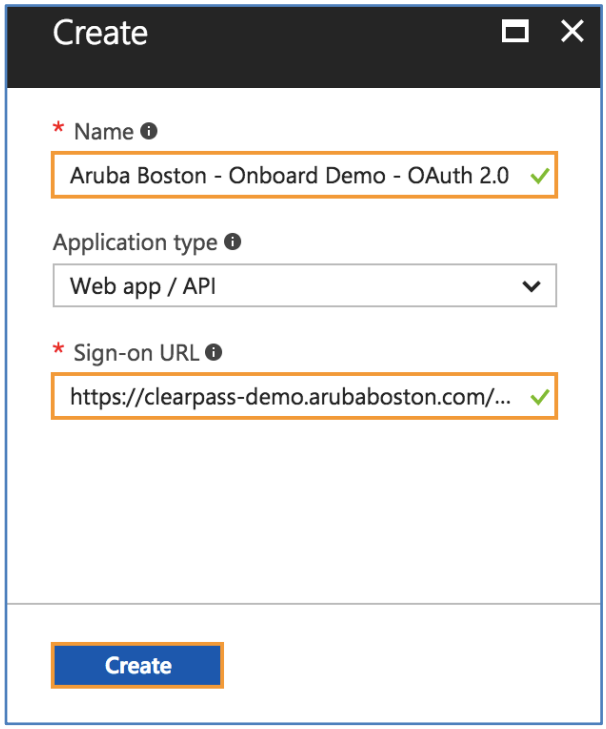


Give the app a friendly name (this will be displayed to users the first time they authenticate).

The **Sign-on URL** is the planned Onboard page name. Do not include any URL parameters after ".php" if present.

```
https://<clearpass-fqdn>/onboard/<page-name>.php
```

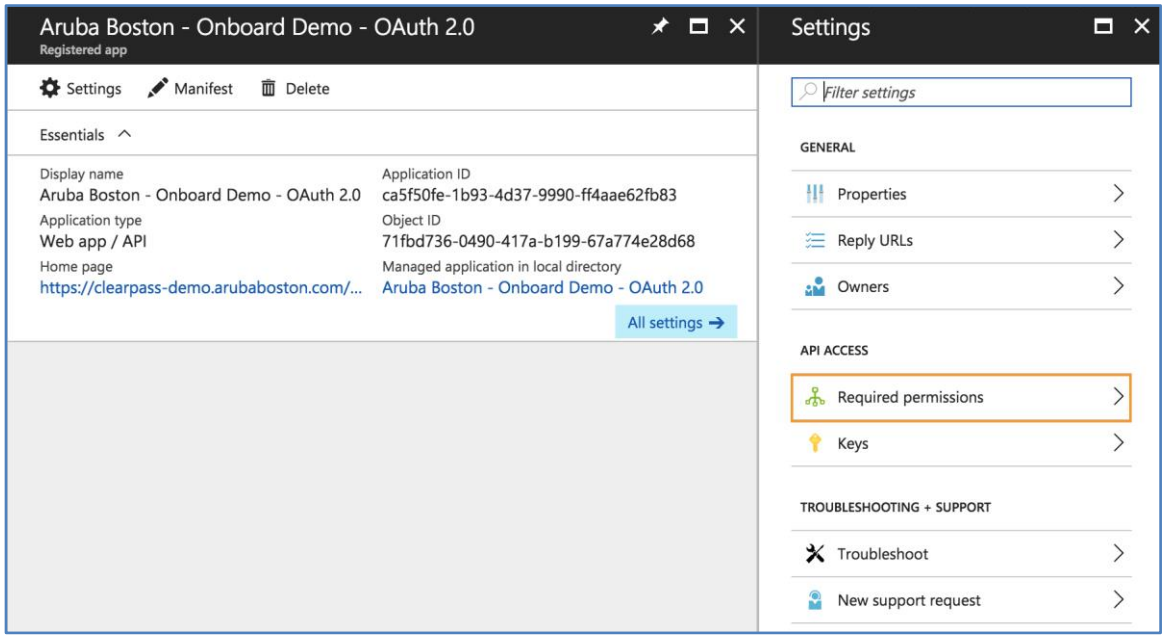
Click **Create** when done.



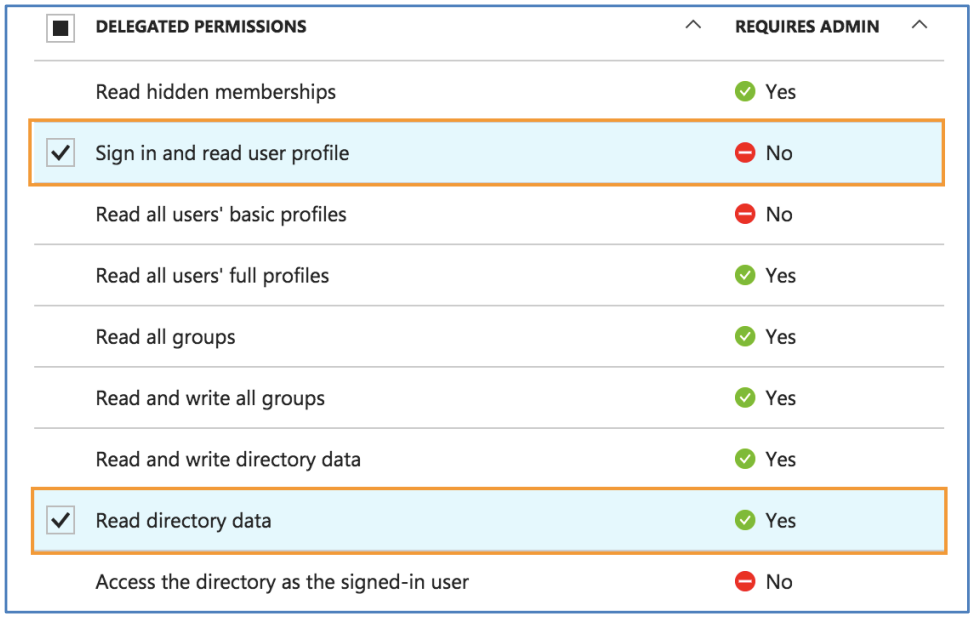
The page will redirect back to the application list. A refresh may be required if the newly created app does not appear.

Click the newly created app to access the configuration.

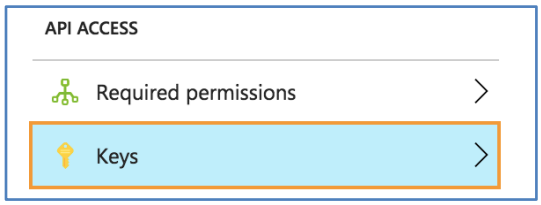
In the Settings blade under API access, click **Required permissions** and then choose **Windows Azure Active Directory**.



Under Delegated Permissions, check **Sign in and read user profile** and **Read directory data.**



Close both permission panes and then select Keys from the main app settings blade.

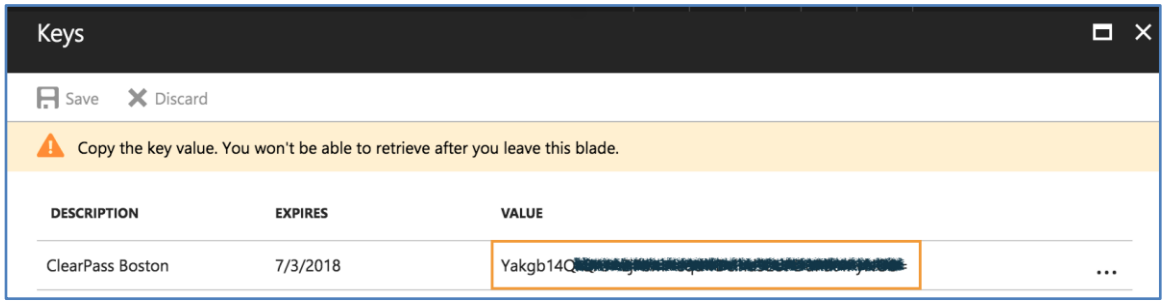


For **Key description**, give the API key a nickname.

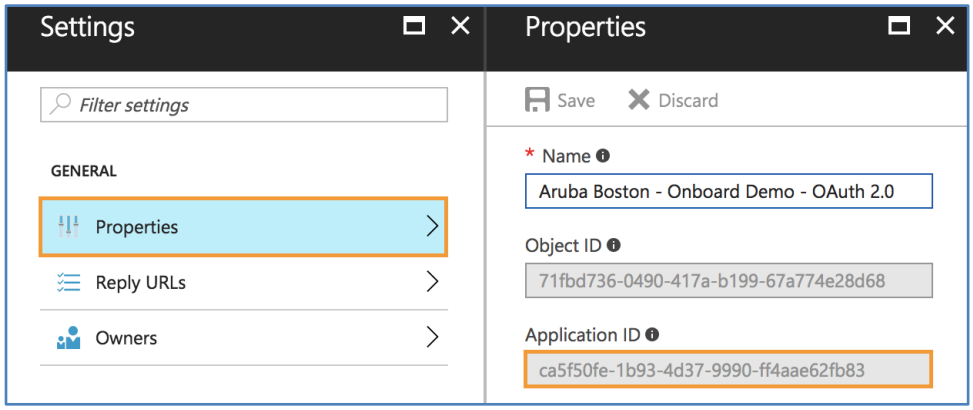
Under **Duration**, select either 1 or 2 years. It is not recommended to generate a key with no expiry.

Click **Save** at the top and the key will be generated.

The API key is not retrievable after this pane is closed. Store this key in a secure location as it will be needed to set up the ClearPass side. It is also recommended to send a calendar reminder to a distribution list for a few days before the scheduled key expiration.



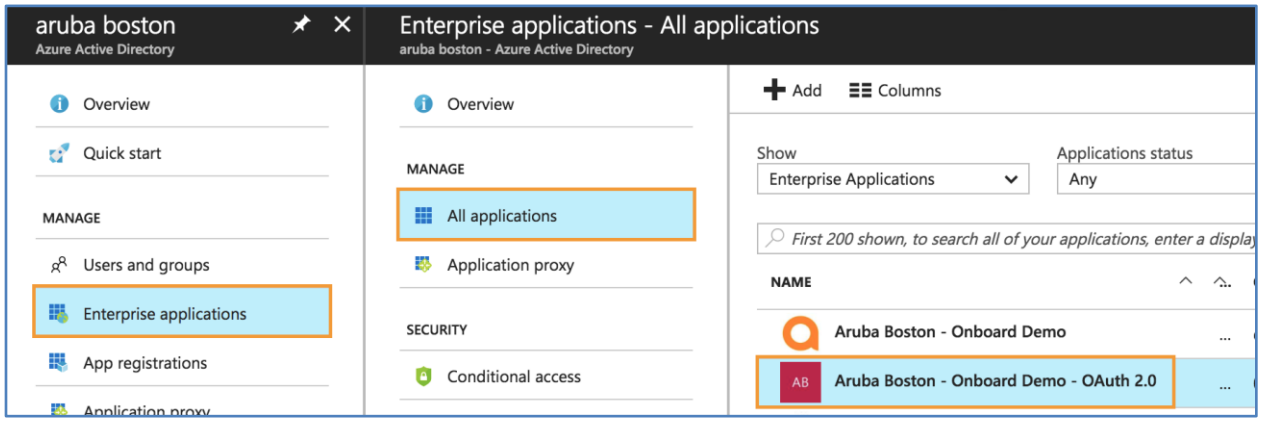
Close the **Keys** pane and then click **Properties**. Copy the **Application ID** and store it. This will be required to configure ClearPass along with the key from the previous step.



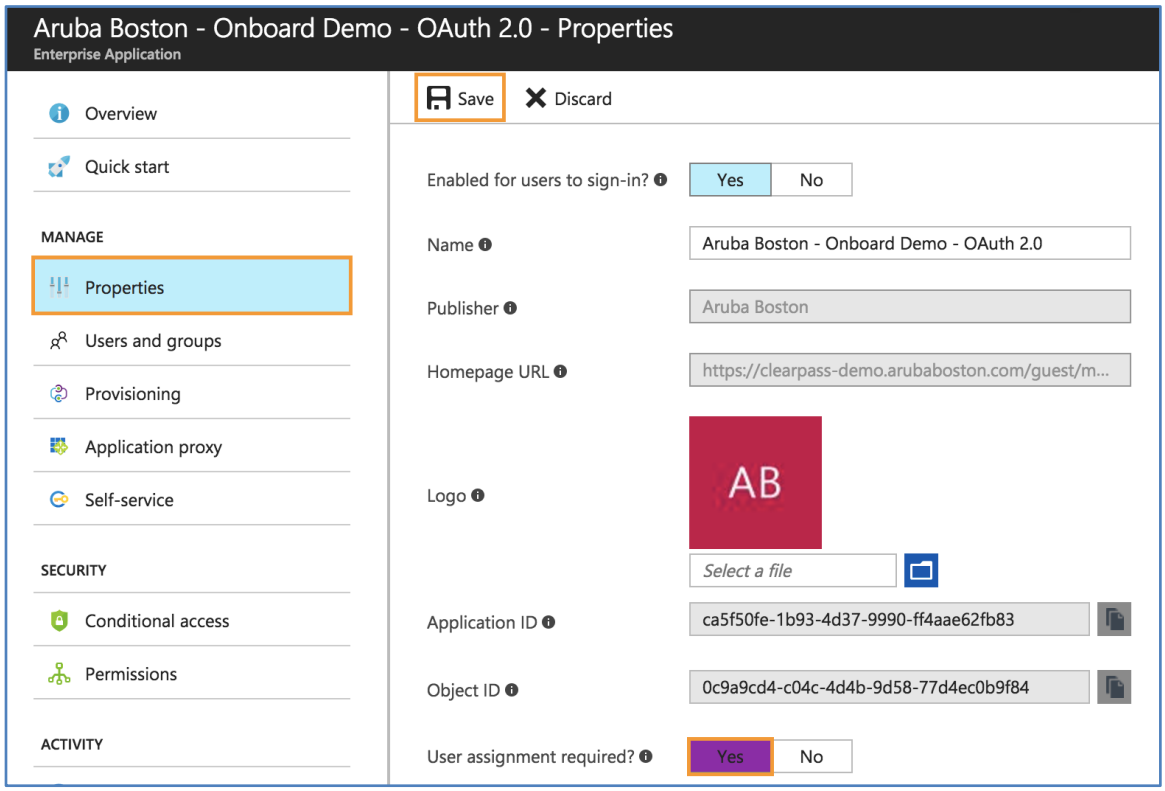
Restricting Access

By default, all users in the Azure Active Directory tenant will be able to authenticate against this OAuth 2.0 provider and be redirected back to ClearPass to continue with Onboard.

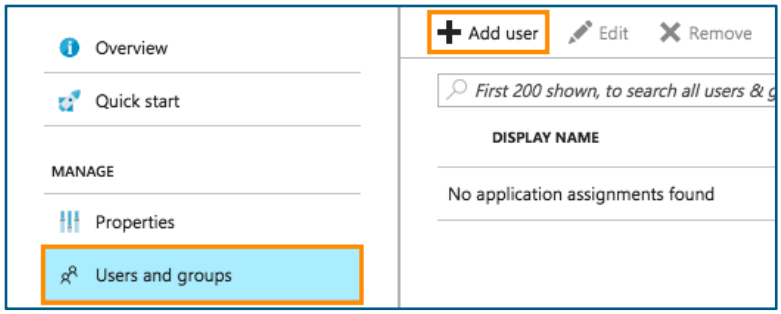
If there is a need to restrict access by group or user at the Azure Active Directory level, navigate back to the top-level Azure Active Directory blade, click **Enterprise applications**, **All applications** and then select the app created in the previous steps.



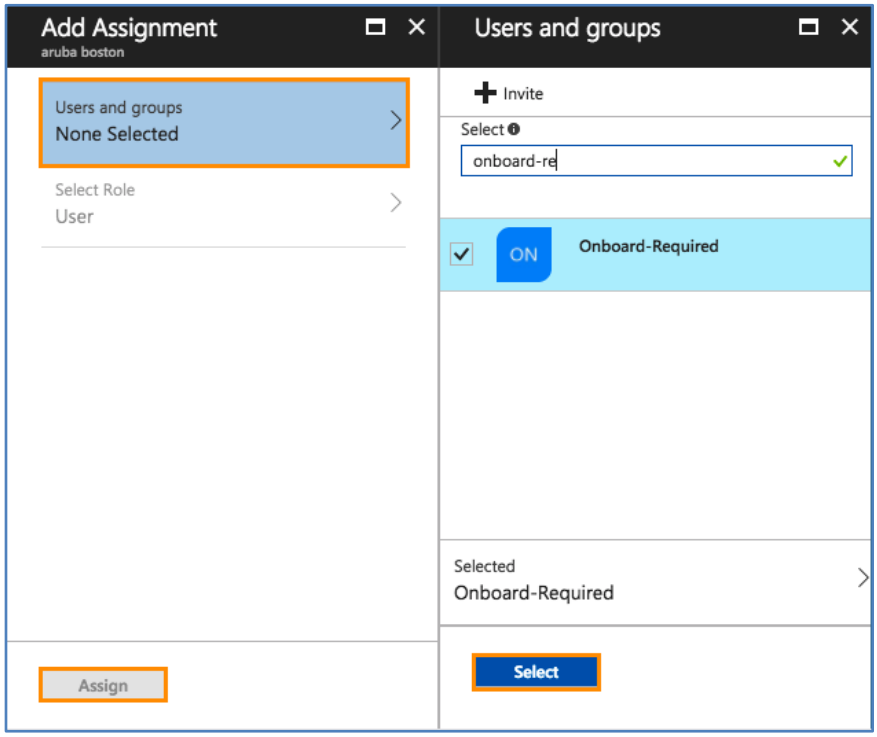
Click **Properties** and then change **User assignment required** to **Yes**, then click **Save** at the top.



Now navigate to **Users and groups** in the menu blade. Click **Add user** at the top.



Click **Users and group** and then search for the user(s) and/or group(s) that should be able to authenticate using this identity provider, then click **Select**. When finished, click **Assign**.

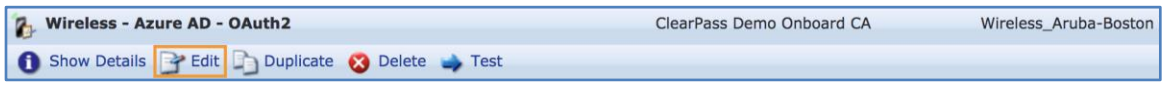


ClearPass Policy Manager Configuration

No specific configuration is required in Policy Manager. The standard Onboard authorization service will be used and pre-authentication will be handled automatically via the ClearPass OAuth 2.0 framework.

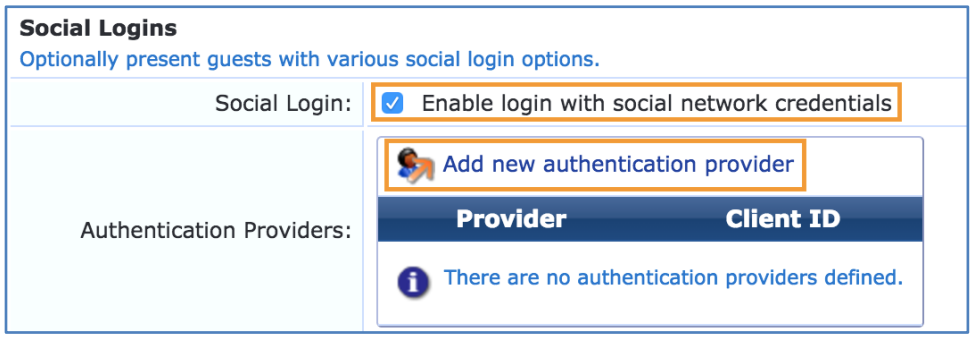
ClearPass Onboard Configuration

Navigate to **Onboard » Deployment and Provisioning » Provisioning Settings**, select the provisioning setting from the list and click **Edit**.



Go to the **Web Login** tab and scroll down to Social Logins.

Check **Enable login with social network credentials** and then click **Add new authentication provider**.



Select **Microsoft Azure** as the **Provider**.

The **Client ID** will be the **Application ID** and the **Client Secret** will be the **API key** that were set up in the Azure portal in the previous steps.

Azure Active Directory will be the only identity provider for Onboard so check **Show advanced properties** and then **Automatically redirect the guest to this provider**.

For **Endpoint Attributes**, select **Create Endpoint converting any arrays to JSON**.

Finally, check **Retrieve the group memberships for the guest's account** and then click **Add**.

Properties	
* Provider:	Microsoft Azure
Enabled:	☑ Use this provider
* Client ID:	<< APPLICATION ID FROM AZURE PORTAL >> The Client ID associated to your provider. They may use a different label.
* Client Secret:	<< API KEY FROM AZURE PORTAL >> The Client Secret associated to your provider. They may use a different label.
Advanced:	☑ Show advanced properties
Destination:	Guests authenticating with this provider will be redirected to this URL after login.
Auto Redirect:	☑ Automatically redirect the guest to this provider Checking this box will remove the ability to support local logins, or any other providers. We recommend also enabling "Custom Form:" in the "Web Login" itself.
Endpoint Attributes:	Create Endpoint attributes converting any arrays to JSON Creating attributes is only needed if you are creating specialized enforcement policies on them.
Flatten Prefix:	Prepend this text to all keys when flattening. If blank, 'social' is used.
Username Prefix:	Prepend this text to all usernames. A prefix or suffix can be useful if you are providing a means to login using a variety of providers.
Username Suffix:	Append this text to all usernames.
Icon Label:	Override the default label on this provider's icon.
Hostname:	If specified, use this hostname when redirecting the user to authenticate. This is optional – leave blank if unsure.
Notes:	Enter comments or notes about this provider. This description is only shown to administrators.
VIP Attribute:	userType Enter the name of the user record attribute to apply to the "social_vip" flag. Refer to the Microsoft Graph API for retrieving users.
Group Membership:	☑ Retrieve the group memberships for the guest's account

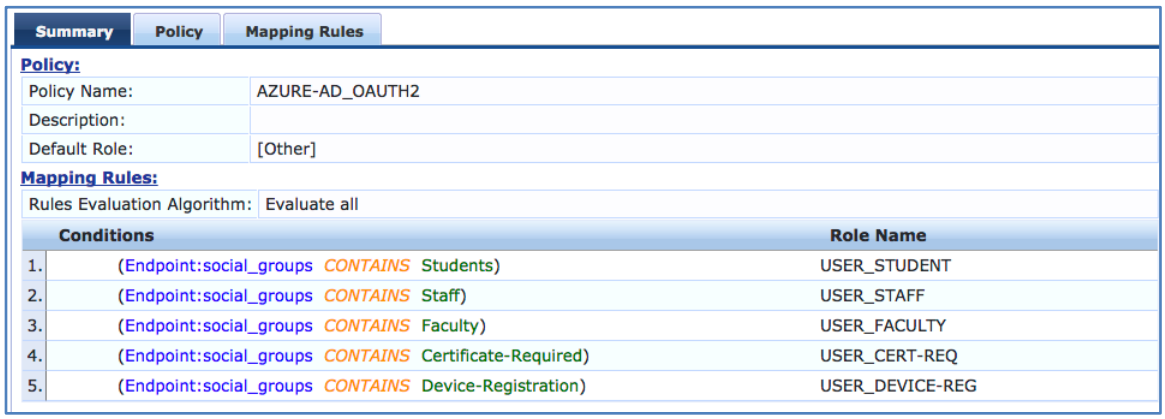
Azure Active Directory will be the only identity provider for Onboard so back on the Web Login page, scroll up to the Login Form section and check **Provide a custom login form.** Then click **Save Changes** at the bottom of the page.

Custom Form:	☑ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.

Dynamic Policy Using Azure Active Directory Attributes

The attributes returned during Onboard pre-authentication via Azure Active Directory can be leveraged post-Onboard as part of a role map or enforcement policy.

The screenshot below is an example of a role map in a standard 802.1X service, leveraging group membership attributes.



Summary | Policy | Mapping Rules

Policy:

Policy Name:	AZURE-AD_OAUTH2
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Endpoint:social_groups *CONTAINS* Students)	USER_STUDENT
2.	(Endpoint:social_groups *CONTAINS* Staff)	USER_STAFF
3.	(Endpoint:social_groups *CONTAINS* Faculty)	USER_FACULTY
4.	(Endpoint:social_groups *CONTAINS* Certificate-Required)	USER_CERT-REQ
5.	(Endpoint:social_groups *CONTAINS* Device-Registration)	USER_DEVICE-REG

NAD Whitelist

In order for clients to be able to reach the Azure Active Directory login page and other embedded resources, certain domain names need to be whitelisted.

The most up to date version of this whitelist as well as examples for Aruba mobility controllers and Aruba Instant are available on the Aruba GitHub: https://github.com/aruba/clearpass-cloud-service-whitelists.

Direct Link: https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_azure-active-directory.md

Google Cloud Identity and G Suite

ClearPass can leverage Google's Cloud Identity service as an identity provider for Onboard via SAML or OAuth 2.0 and can also leverage the Secure LDAP service for real-time authorization during authentication flows.

When a user initiates the Onboard process, usually by clicking the Onboard link on a guest portal, they will be redirected straight to the Google unified login page. After a successful authentication (and potential MFA challenge), they will be redirected to ClearPass Onboard to begin device enrollment.

Below is a comparison between the two technologies and which features and workflows are available with each authentication method.

Feature	SAML	OAuth 2.0
Requires end-user consent dialog	✗	✓
Requires override for Google "Unreviewed Apps"	✗	✓
Group membership	✓ (with Google Secure LDAP connector)	✓ (with Google Secure LDAP connector)
Workflow Specific Features	**SAML**	**OAuth 2.0**
Evaluate return attributes during Onboard pre-authentication	✓	✗
Evaluate return attributes during subsequent EAP-TLS authentication/authorization	✗	✓
Real-time evaluation of Groups, OU, email address and account status	✓ (with Google Secure LDAP connector)	✓ (with Google Secure LDAP connector)

Below is the list of available return attributes for SAML and OAuth 2.0.

User Entity Return Attributes	
SAML	**OAuth 2.0**
address	groups
title	group emails
department	given name
costcenter	family_name
	picture
	gender
	locale
	hd
	kind
	etag
	primaryEmail
	isAdmin
	isDelegatedAdmin
	lastLoginTime
	creationTime
	agreedToTerms
	suspended
	changePasswordAtNextLogin
	ipWhitelisted
	emails
	organizations:primary
	organizations:customType
	organizations:department
	nonEditableAliases
	customerId
	orgUnitPath
	isMailboxSetup
	isEnrolledIn2Sv
	isEnforcedIn2Sv
	includeInGlobalAddressList

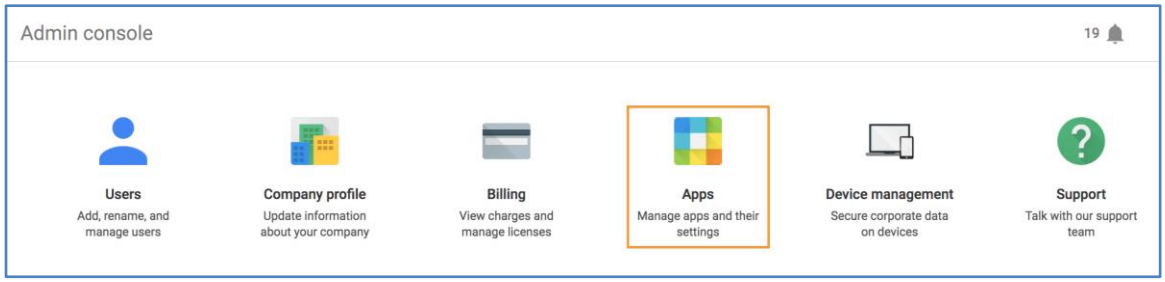
Google Secure LDAP Connector

To support real-time evaluation of attributes like groups, organizational unit, email address and overall account status, the Google Secure LDAP Connector can be used.

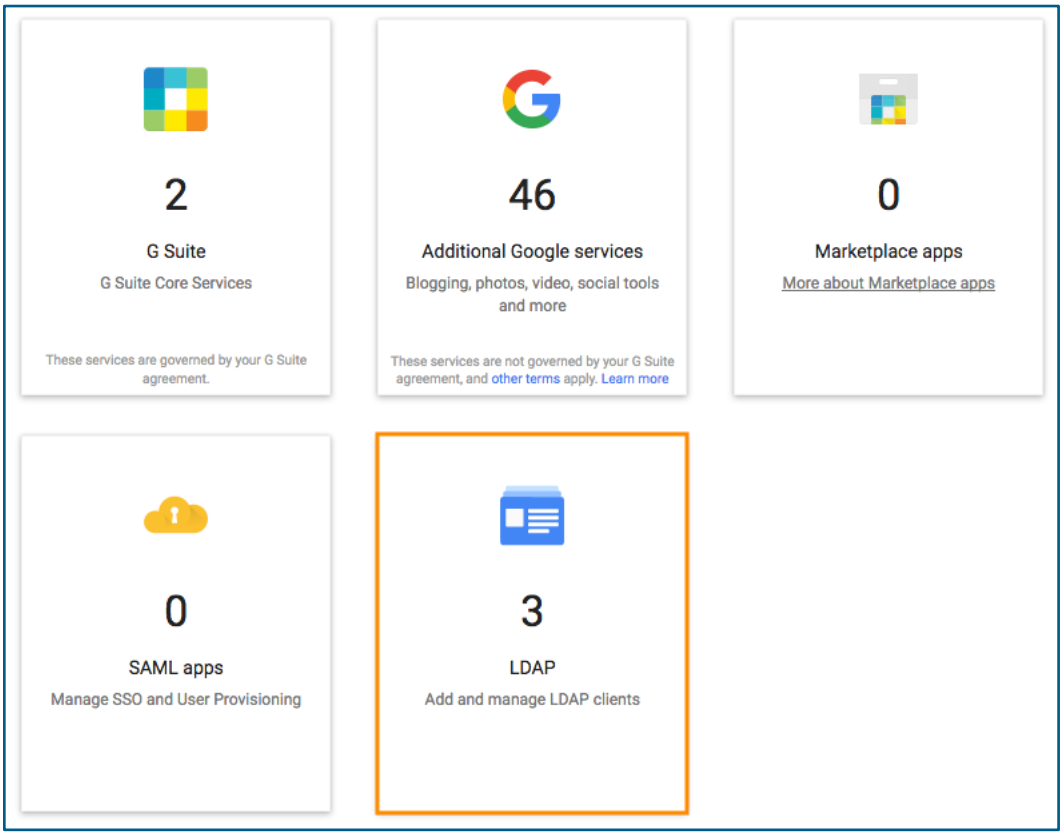
This connector uses the ClearPass Extensions framework. The Google Secure LDAP service is available to Cloud Premium, G Suite Enterprise, and all G Suite for Education organizations.

Google Admin Console Configuration

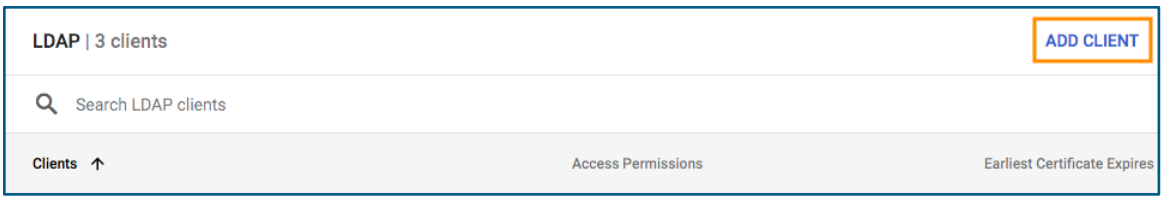
Log into the Google Admin portal at admin.google.com with an account with admin privileges for the organization. At the main admin landing page, click the **Apps** icon.



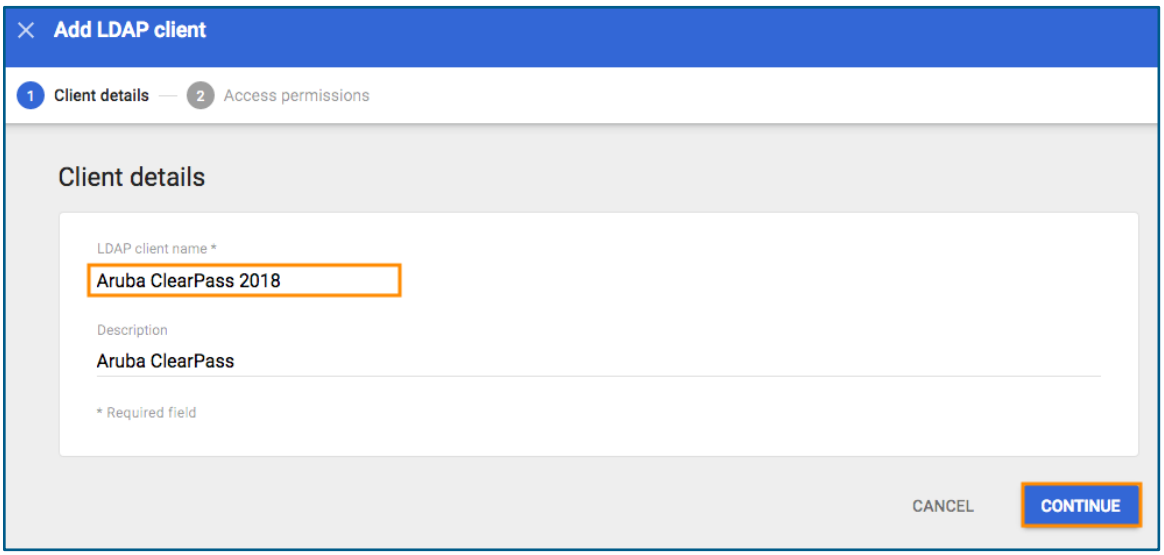
Choose **LDAP** from the list.



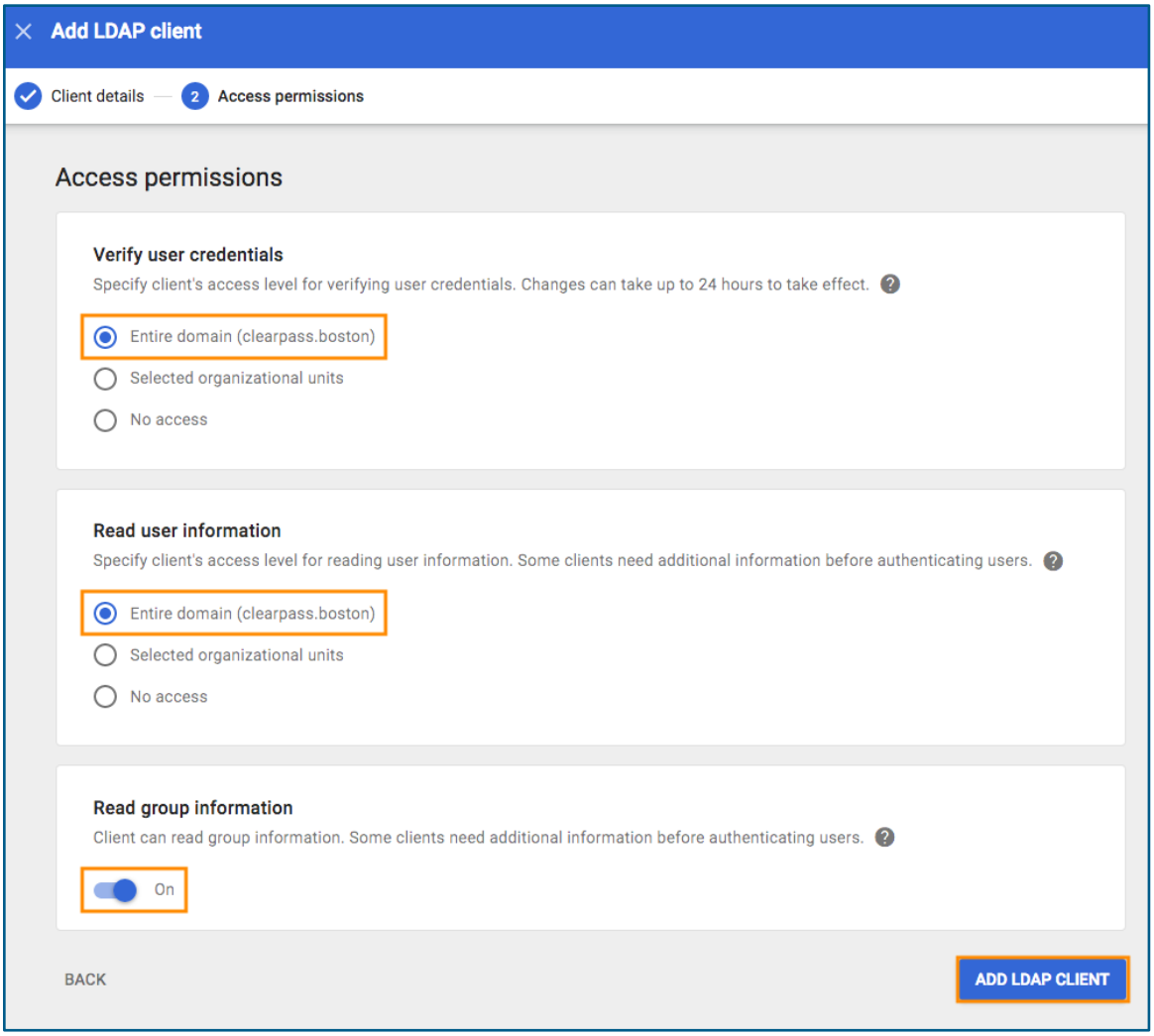
Click **ADD CLIENT**.



Give the client a friendly name and optional description, then click **CONTINUE**.



On the Access permissions page, enable the Entire domain for ***Verify user credentials*** and ***Read user information*** and also enable ***Read group information***. Click **ADD LDAP CLIENT** to continue.

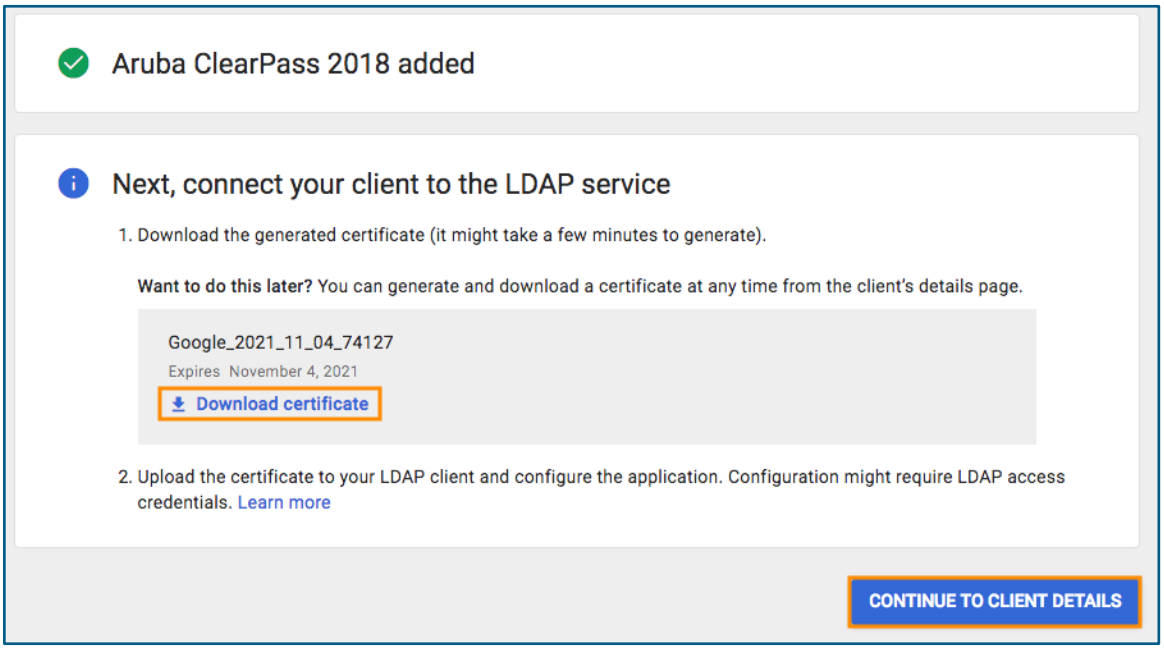


NOTE: If only a subset of users in the organization will be authenticating via ClearPass, these permissions can be isolated down to specific organizational units.

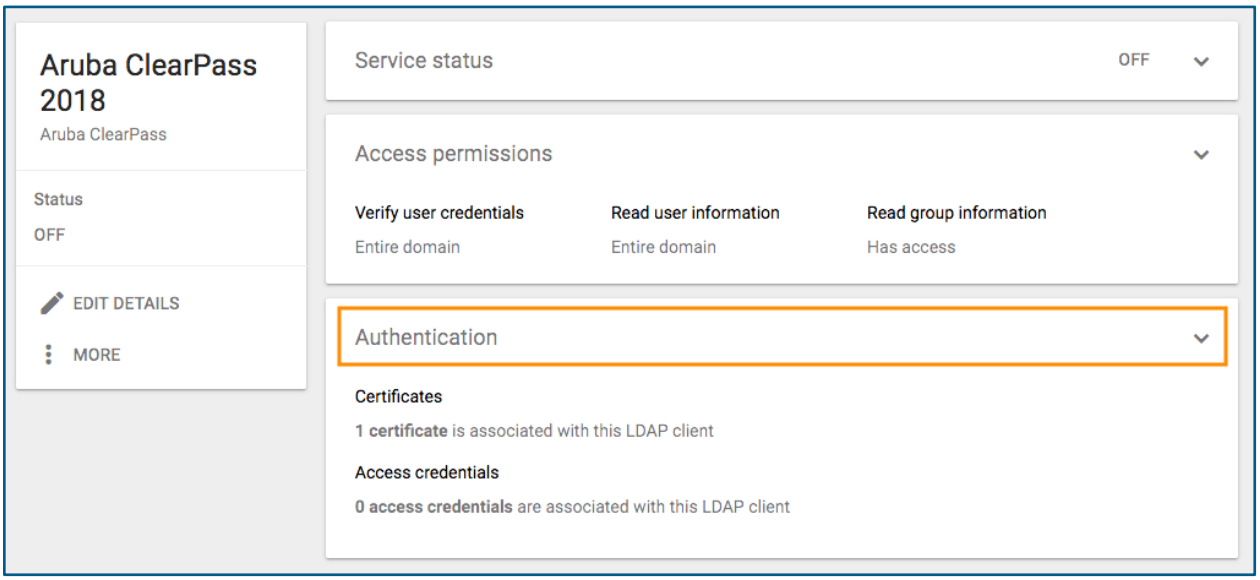
Google will automatically generate a key pair and certificate that will be used for authentication.

Click **Download certificate** and save the file.

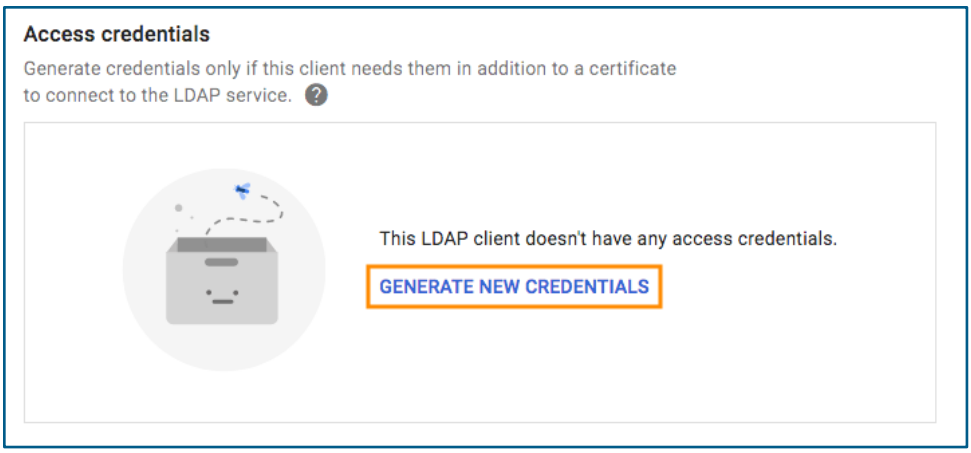
Click **CONTINUE TO CLIENT DETAILS**.



Click ***Authentication*** to open the widget.

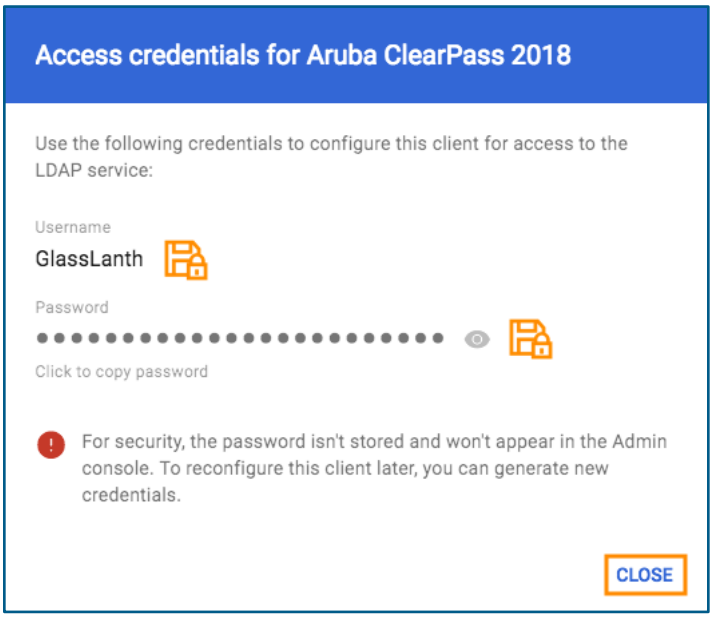


Under Access credentials, choose **GENERATE NEW CREDENTIALS**.



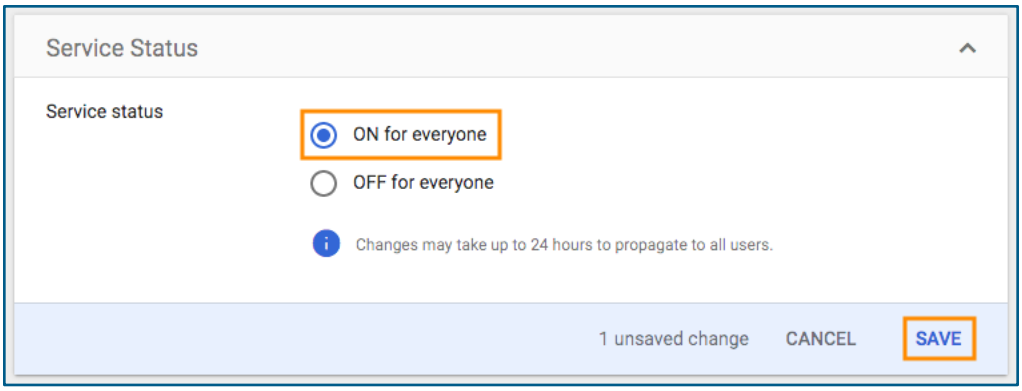
Securely store a copy of the generated credentials. They will be required to configure ClearPass.

Click **Close** when finished.



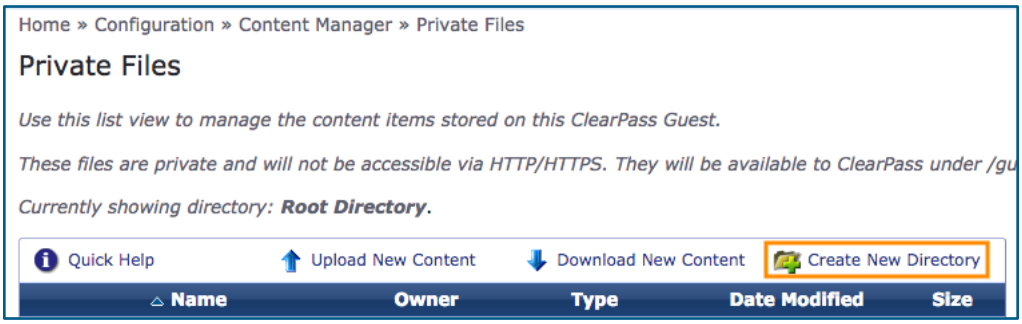
Close the ***Authentication*** widget by clicking it.

Lastly, click the ***Service status*** widget and choose **ON for everyone** and click **SAVE**.

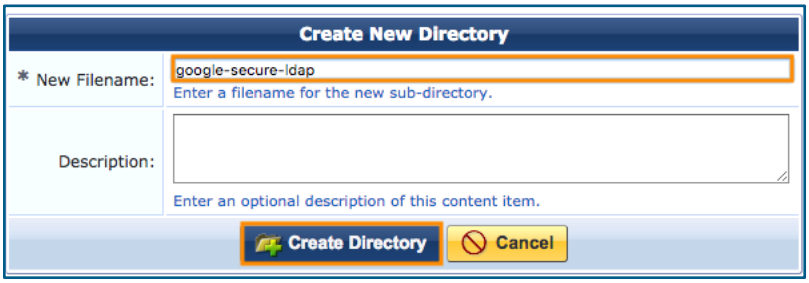


ClearPass Extension Configuration

Over in ClearPass, navigate to ***Guest » Configuration » Content Manager » Private Files*** and click **Create New Directory**.



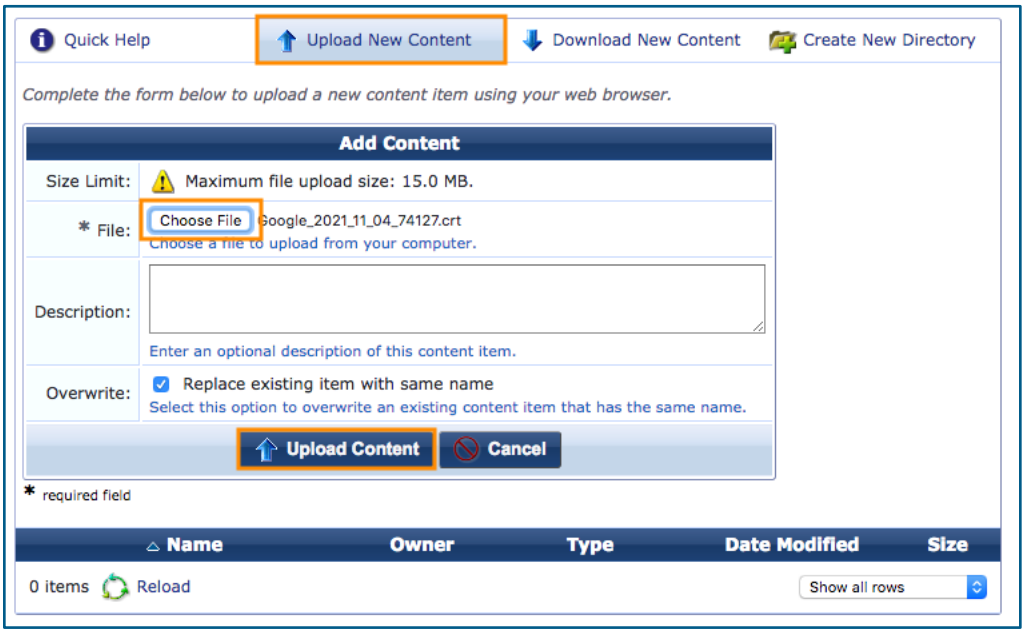
Call the folder **`google-secure-ldap`** and click **Create Directory**.

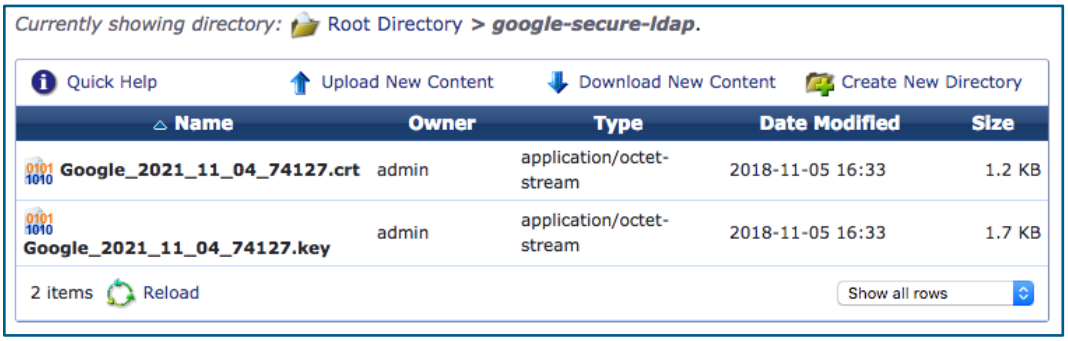


Extract the certificate zip file downloaded from Google Admin Console in the previous steps.

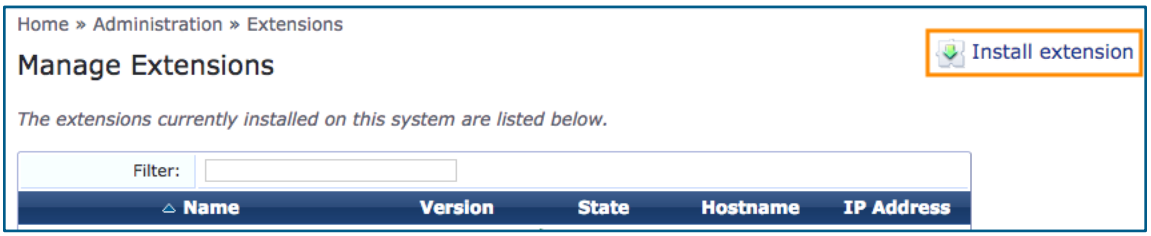
Click **Upload New Content** then click **Choose File** and choose the .crt file and click **Upload Content**.

Repeat the same process for they .key file.



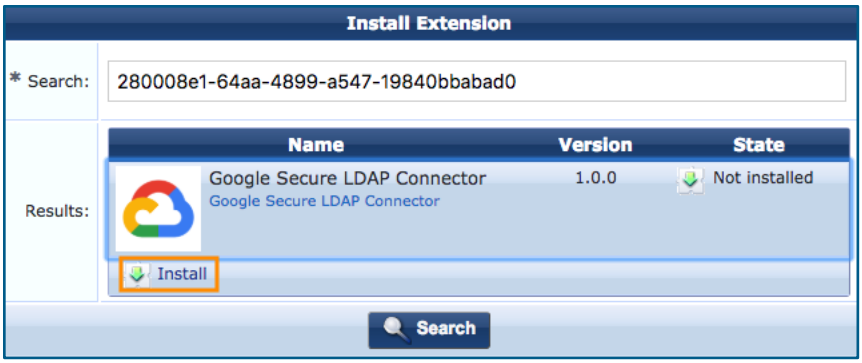


Next, navigate to ***Administration » Extensions*** and then click **Install extension.**



Search for **Google Secure LDAP Connector**.

Click **Install**.



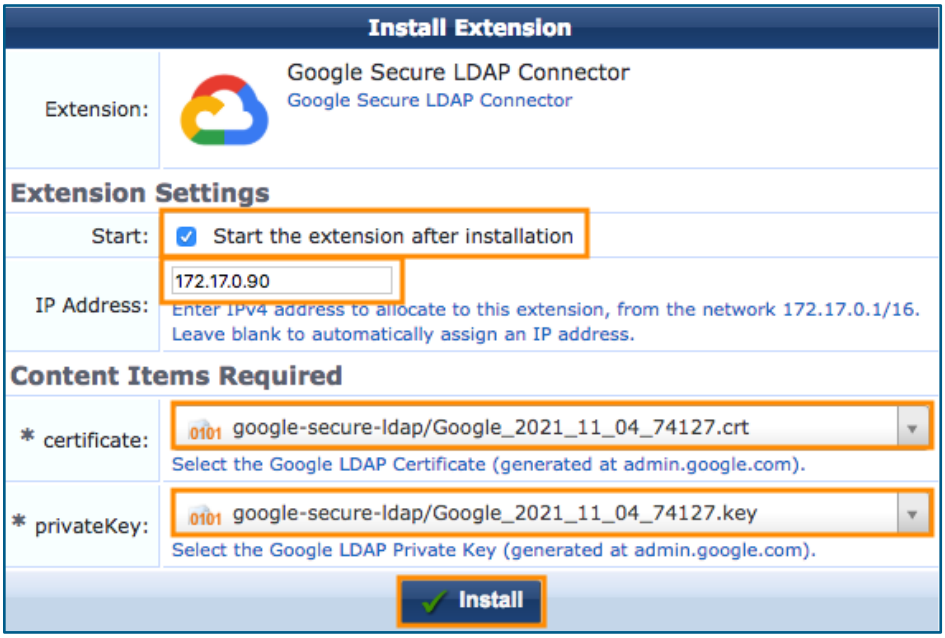
Check ***Start the extension after installation***.

Assign an IP address in the configured Extension IP range (by default, 172.17.0.0/16)

For ***certificate***, select the certificate file (.crt) previously uploaded from the dropdown box.

For ***privateKey***, select the key file (.key) previously uploaded.

Click **Install** to finish.



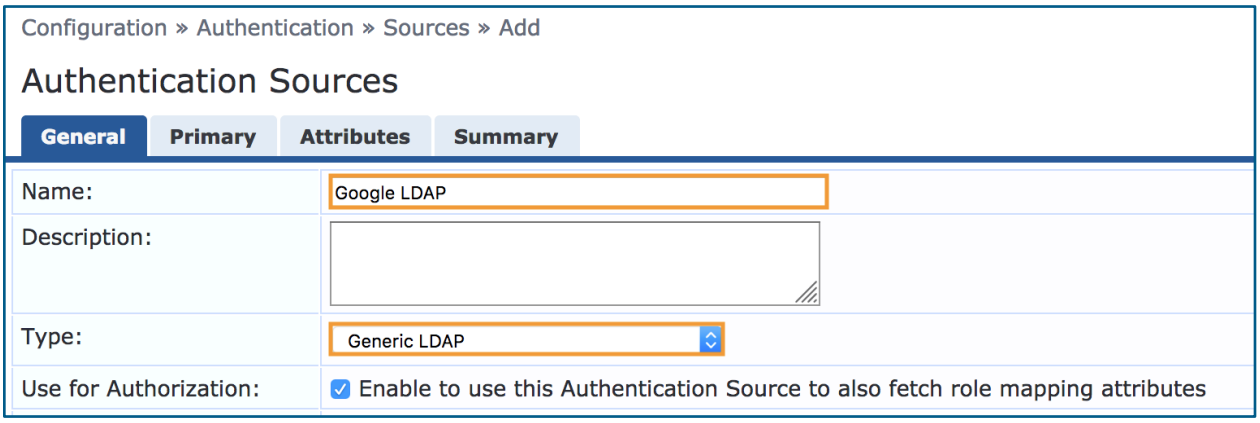
In a multi-node ClearPass cluster, repeat the Extension installation process on each node, ensuring the same IP address is used.

ClearPass Policy Manager Auth Source

Navigate to ***Configuration » Authentication Sources*** and click **Add**.

Give the authentication source a name such as **`Google LDAP`**.

Select **Generic LDAP** under ***Type***.



Switch to the **Primary** tab.

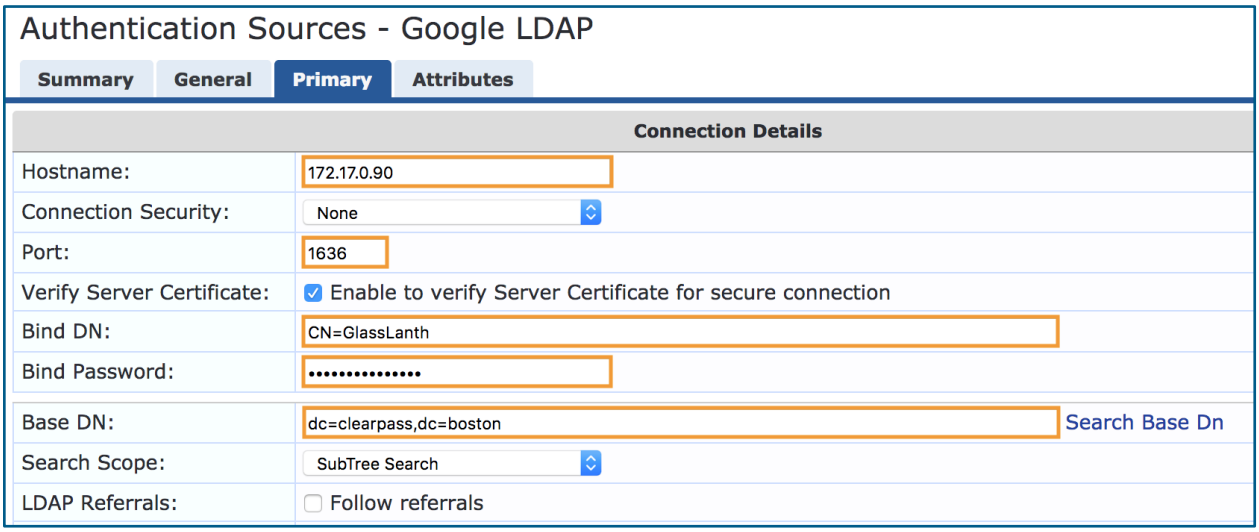
For ***Hostname***, enter the IP address assigned to the Connector Extension.

Change the ***Port*** to 1636.

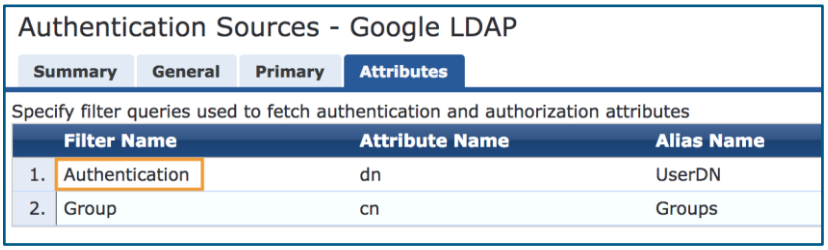
For ***Bind DN***, use the username generated earlier in Google Admin Console with **`CN=`** prepended.

For ***Bind Password***, use the password generated earlier in Google Admin Console.

For ***Base DN***, enter the tenant domain in LDAP DN format.

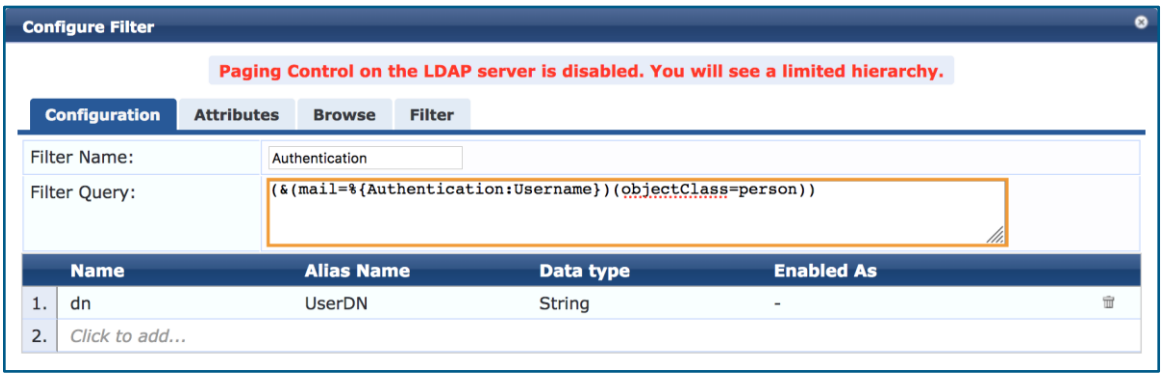


Switch over to the **Attributes** tab and click on **Authentication**.



Replace the ***Filter Query*** with:

```
(&(mail=%{Authentication:Username})(objectClass=person))
```



Click **Save** and then **Save** again.

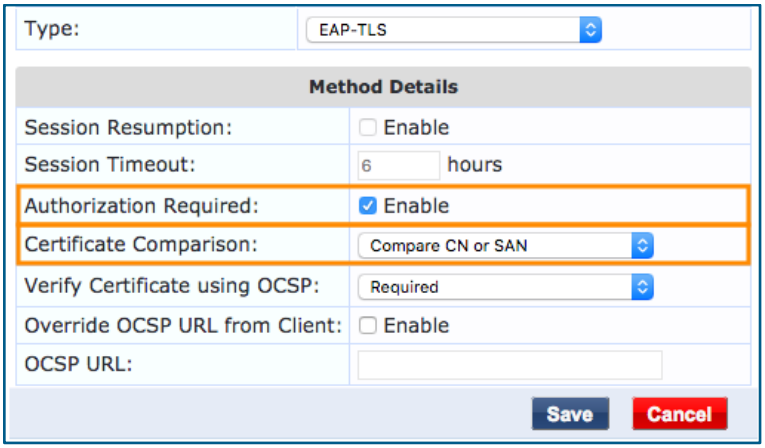
ClearPass Policy Examples

The Google Secure LDAP authentication source has two main uses: a lookup source for EAP-TLS authorization and role mapping or enforcement policies.

EAP-TLS Comparison

Authorization can be enabled on an EAP-TLS method in ClearPass. Enabling Authorization compares the user identity values in the certificate to the configured authentication sources to ensure the user exists in that identity store.

You can also enable Certificate Comparison which will check for a match between the EAP identity and the certificate properties.



Role Mapping and Enforcement Policies

LDAP attributes returned back from Google can also be used in role mapping and enforcement policies just like any other authorization source.

Below is an example of a role map that takes advantage of the LDAP directory data. Rules 1 and 2 use the user's organizational unit. Rules 3 and 4 use the user's group membership.

Policy:

Policy Name:	Google LDAP Roles
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Authorization:Google LDAP:UserDN *ENDS_WITH* ou=Staff,ou=Users,dc=clearpass,dc=boston)	USER_STAFF
2.	(Authorization:Google LDAP:UserDN *ENDS_WITH* ou=Faculty,ou=Users,dc=clearpass,dc=boston)	USER_FACULTY
3.	(Authorization:Google LDAP:Groups *EQUALS* employees)	USER_EMPLOYEE
4.	(Authorization:Google LDAP:Groups *EQUALS* it-admins)	USER_IT

Sample request:

Policies Used -	
Service:	Google Secure LDAP
Authentication Method:	EAP-TLS
Authentication Source:	Ldap:172.17.0.90
Authorization Source:	Google LDAP
Roles:	USER_EMPLOYEE, USER_STAFF, [User Authenticated]
Enforcement Profiles:	LUR_AOS-W_STAFF
Service Monitor Mode:	Disabled

Summary | **Input** | **Output**

Username:	josh@clearpass.boston
End-Host Identifier:	8B-5A-F9-3A-70-C4
Access Device IP/Port:	100.81.2.10:0 (aruba-fmc-1 / Aruba)

RADIUS Request

Authorization Attributes

Authorization:Google LDAP:Groups	employees
Authorization:Google LDAP:UserDN	uid=josh,ou=Staff,ou=Users,dc=clearpass,dc=boston

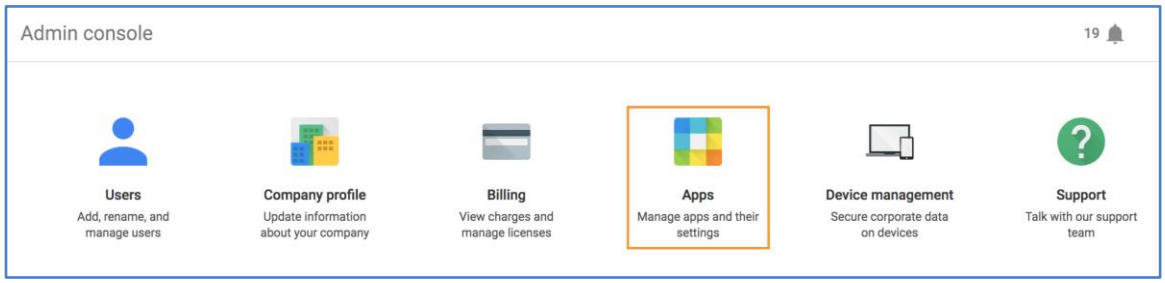
SAML

Google Admin Configuration

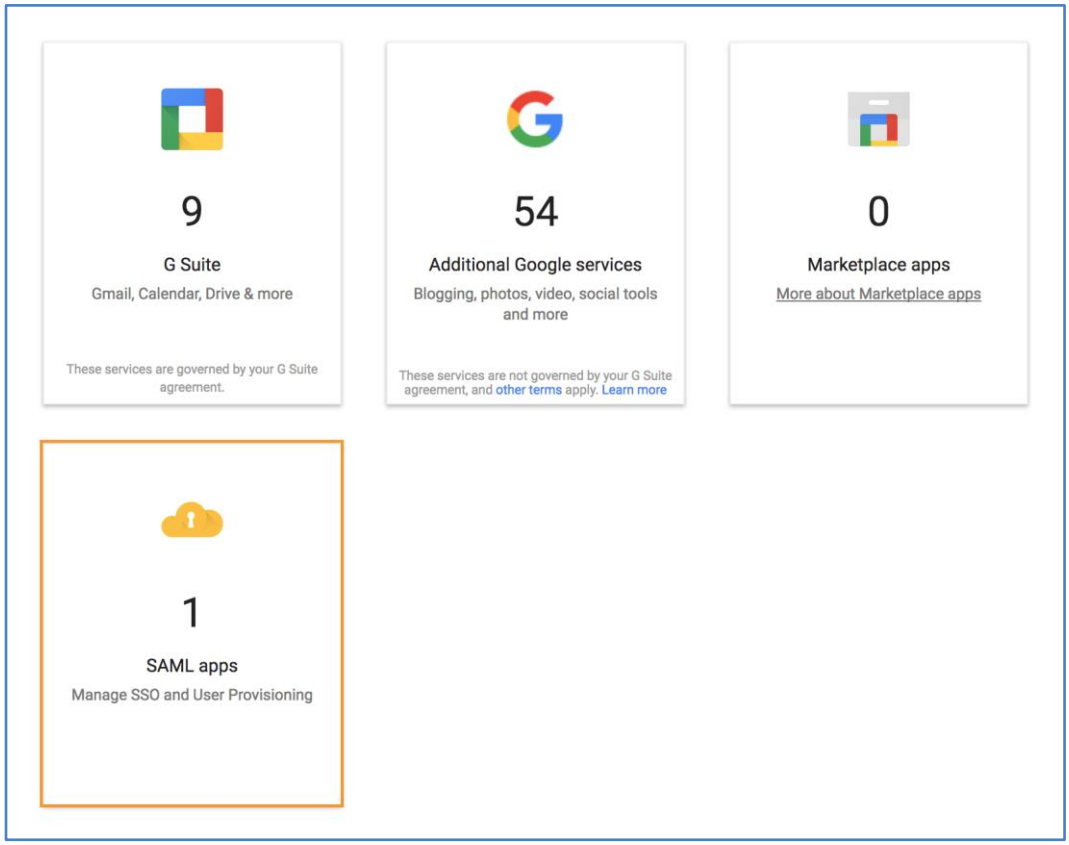
Application Setup

Log into the Google Admin portal at admin.google.com with an account with admin privileges for the organization.

At the main admin landing page, click the **Apps** icon.



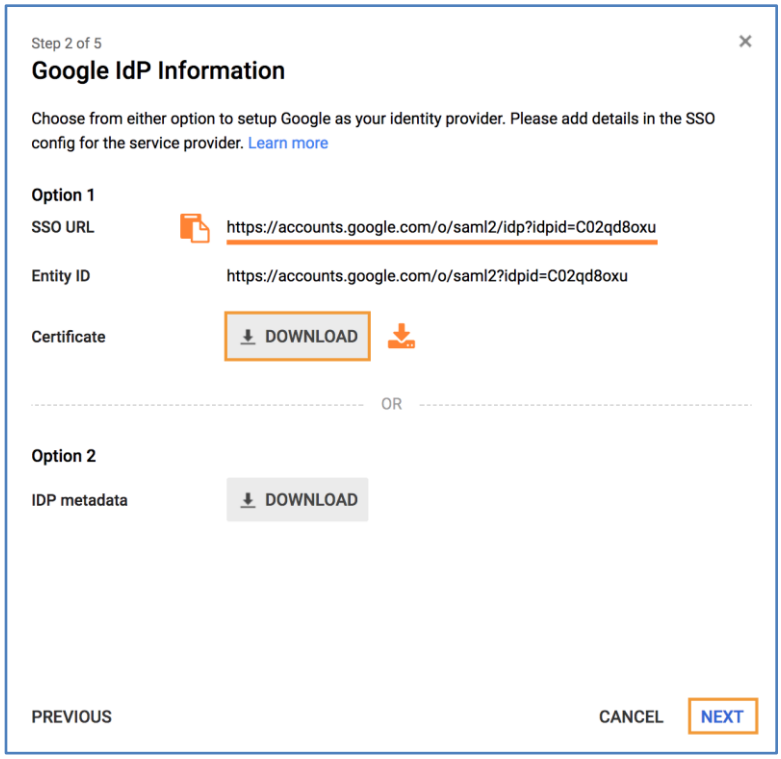
Choose **SAML apps** from the list.



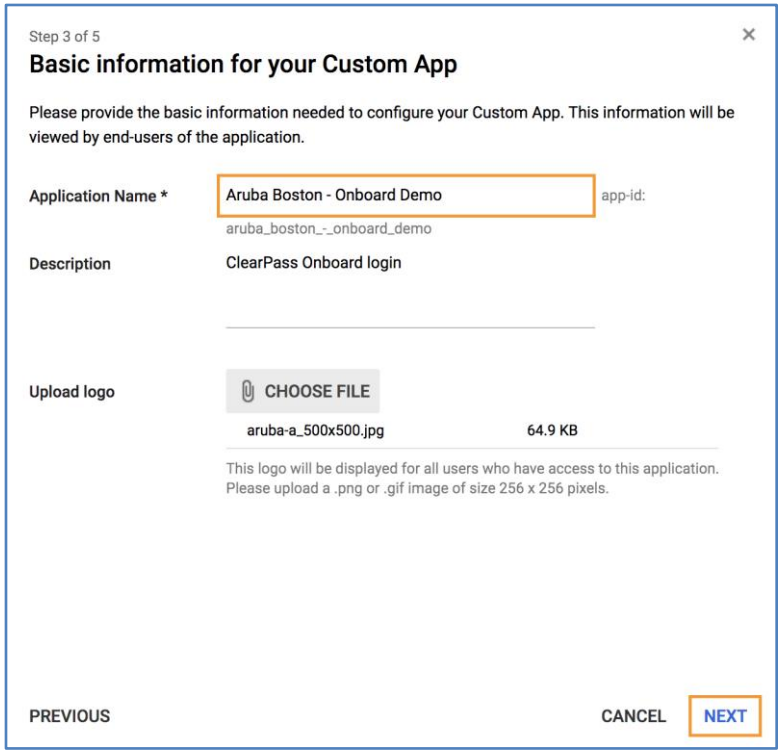
Click the button towards the bottom right.

Select **SETUP MY OWN CUSTOM APP** at the bottom of the window.

Copy and store the **SSO URL** and download the **Certificate** under Option 1 and then click **NEXT**.



Give the application a name, description (optional) and upload a logo (optional).



Step 4 is the ClearPass SAML service provider configuration.

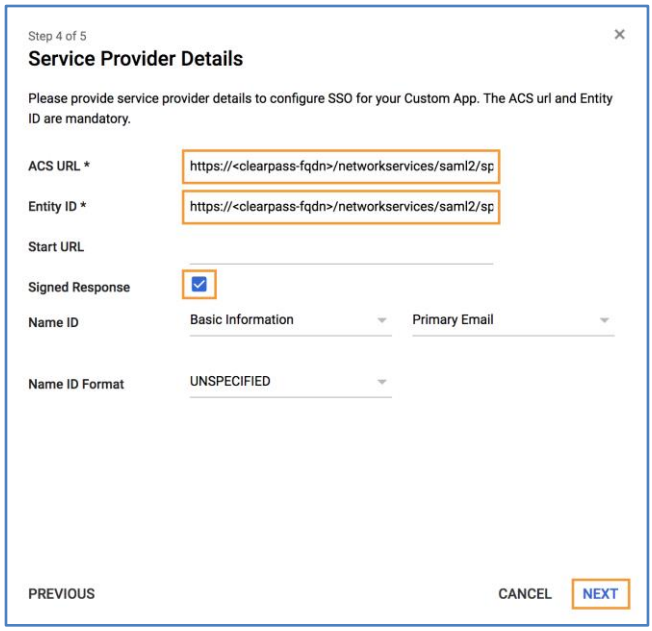
The **ACS URL** is the SAML Assertion Consumer Service and is the same in all ClearPass installations. Replace <clearpass-fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

```
https://<clearpass-fqdn>/networkservices/saml2/sp/acs
```

The **Entity ID** is the same in all ClearPass installations. Replace <clearpass-fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

```
https://<clearpass-fqdn>/networkservices/saml2/sp
```

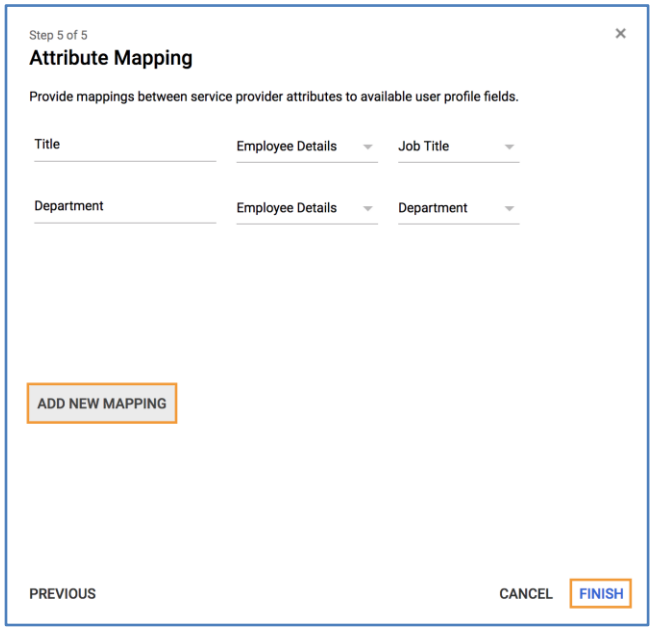
Check **Signed Response** and then click **NEXT**.



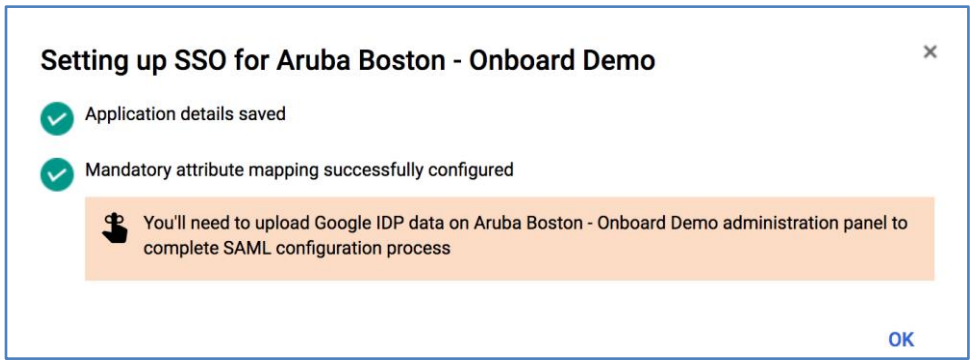
Step 5 is an optional configuration for sending back additional attributes from Cloud Identity or G Suite in the SAML response.

In the example below, the Job Title and Department attributes are being sent back as **Title** and **Department** respectively.

Click **FINISH** to end the SAML application setup.



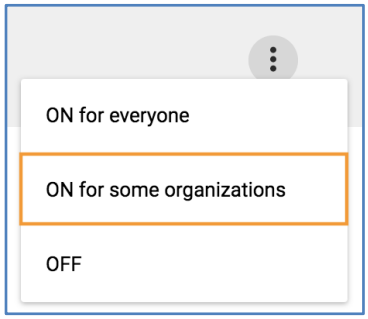
Click **OK** on the summary screen.



By default, the application will be turned off. In the SAML App list, click the triple dot menu for the app, and click **ON for everyone**. To restrict access to certain groups, see the next section.

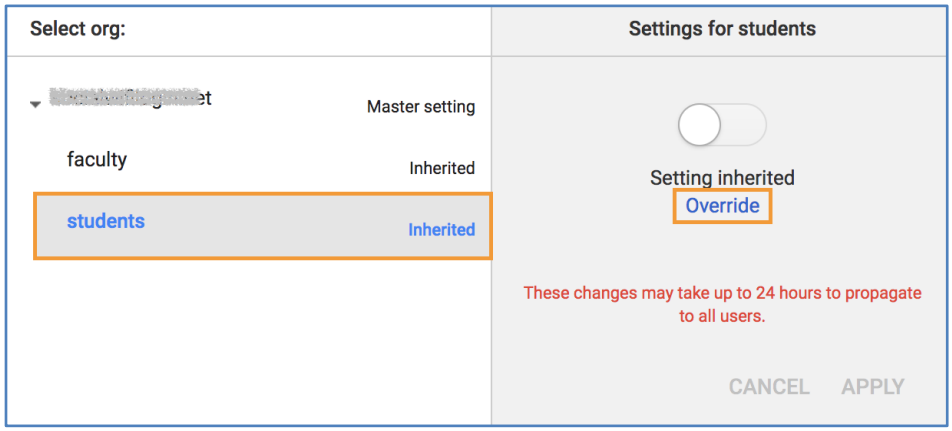
Restricting Access

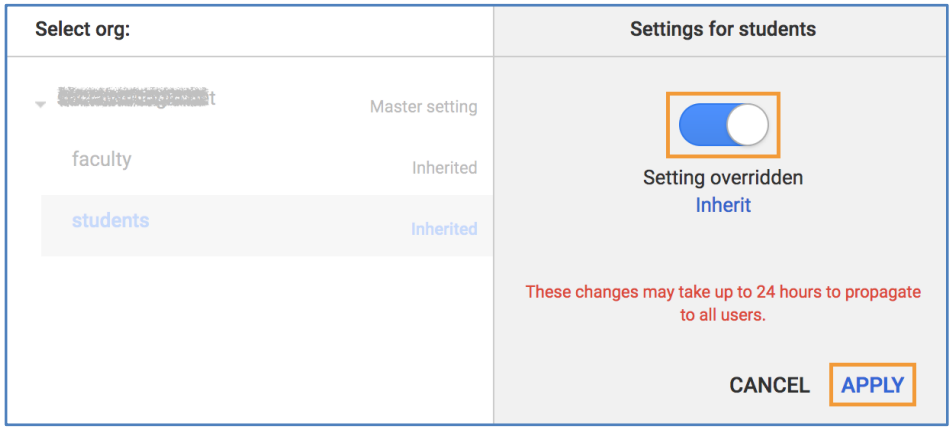
If there is a need to restrict access to certain organizational units at the IdP level, use the **ON for some organizations** option when enabling the SAML IdP.



This will allow access for certain organizational units.

Select the group name on the left under the organization name, click the **Override** link and then toggle the enable button and click **APPLY**. Repeat this for each organizational unit that needs access.





ClearPass Policy Manager Configuration

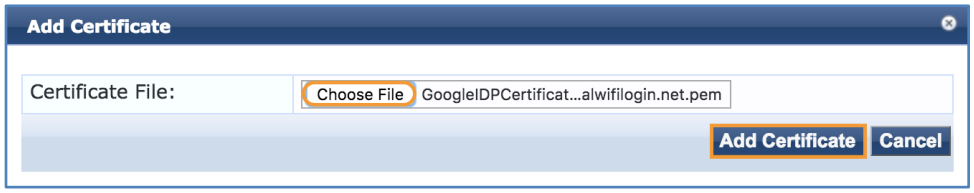
IdP Certificate

The first step in Policy Manager is to upload the identity provider certificate provided in the G Suite admin console.

Navigate to **Administration** » **Certificates** » **Trust List** and click **Add**.

Browse for the previously downloaded certificate and then click **Add Certificate**.

> **NOTE**: The certificate will be self-signed and have a common name of *Google* and the Organizational Unit will be *Google For Work*.



The certificate should now appear in the trust list as Enabled.

Service Provider Configuration

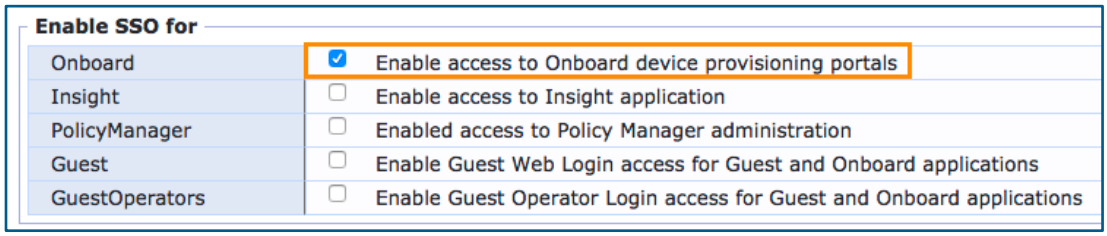
Next, Policy Manager needs to be configured to use Google as a SAML Identity Provider and enable it for use with Onboard workflows.

Navigate to **Configuration** » **Identity** » **Single Sign-On (SSO)**.

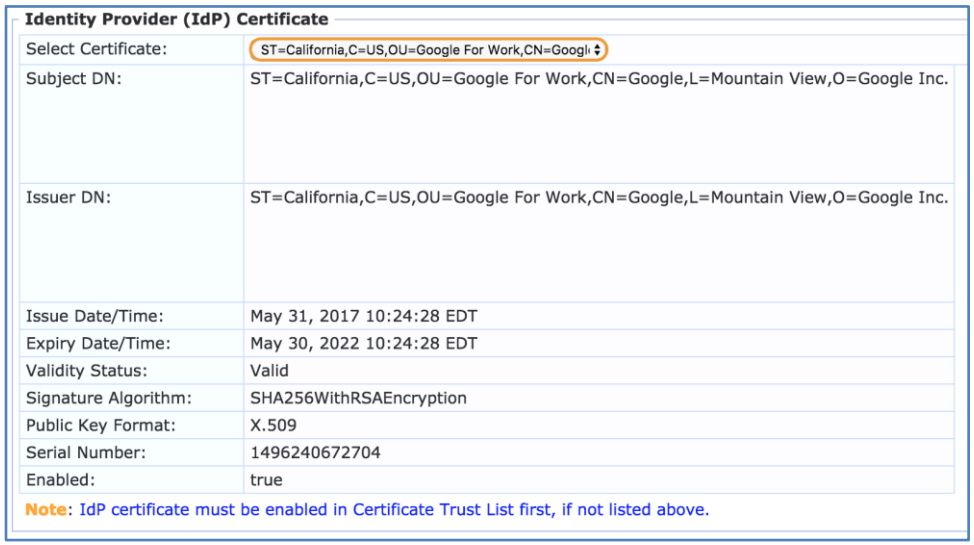
For **Identity Provider (IdP) URL**, enter in the **SSO URL** from the G Suite application configuration. The URL should look something like this:

https://accounts.google.com/o/saml2/idp?idpid=<GUID>

Check **Enable access to Onboard device provisioning portals**.



Finally, select the **Google** certificate from the down-down list under **Identity Provider (IdP) Certificate**.



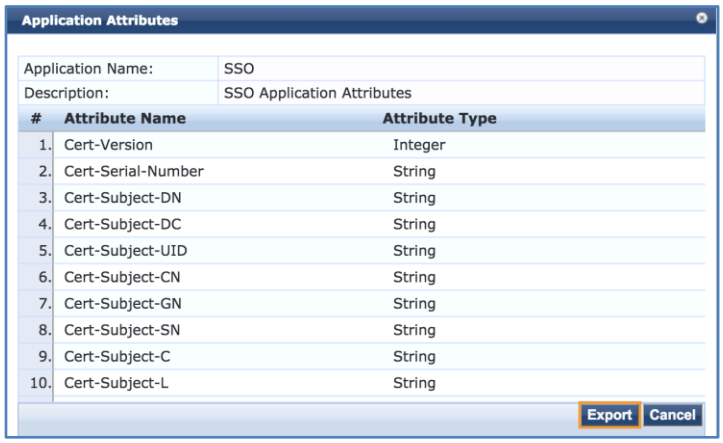
Click **Save** at the bottom.

Application Dictionary

If there is a need to assign different Onboard configuration overrides using SAML Token Attributes, the ClearPass SAML dictionary will need to be updated. Examples would be using a different certificate lifetime for different types of users or even using a different configuration profile. If SAML Token Attributes will not be used in Onboard pre-authentication, skip this step.

NOTE: Department, Title, and Company are available by default in ClearPass and do not require any changes to the SSO dictionary. Just be sure they are mapped in step 5 of the SAML app configuration in the Google Admin Console (Attribute Mapping).

Navigate to **Administration » Dictionaries » Applications**, click on SSO and then click **Export**.



Open the exported XML file in a text editor.

Add the SAML Token Attributes, following the same format as the existing entries. Below is an example for the Phone attribute.

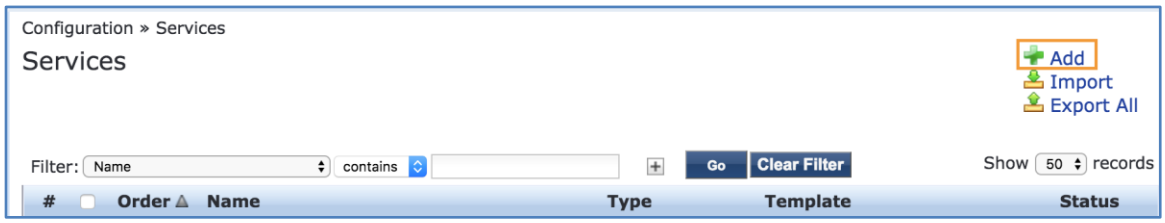
```
<ApplDictionaryAttributes attrType="String" attrName="Phone"/>
```

Once all of the desired attributes have been added, save the file and import it back into ClearPass.

Onboard Pre-Authentication Service

A new service will be required to handle the Onboard SAML pre-authentication.

Navigate to **Configuration » Services** and then click **Add**.

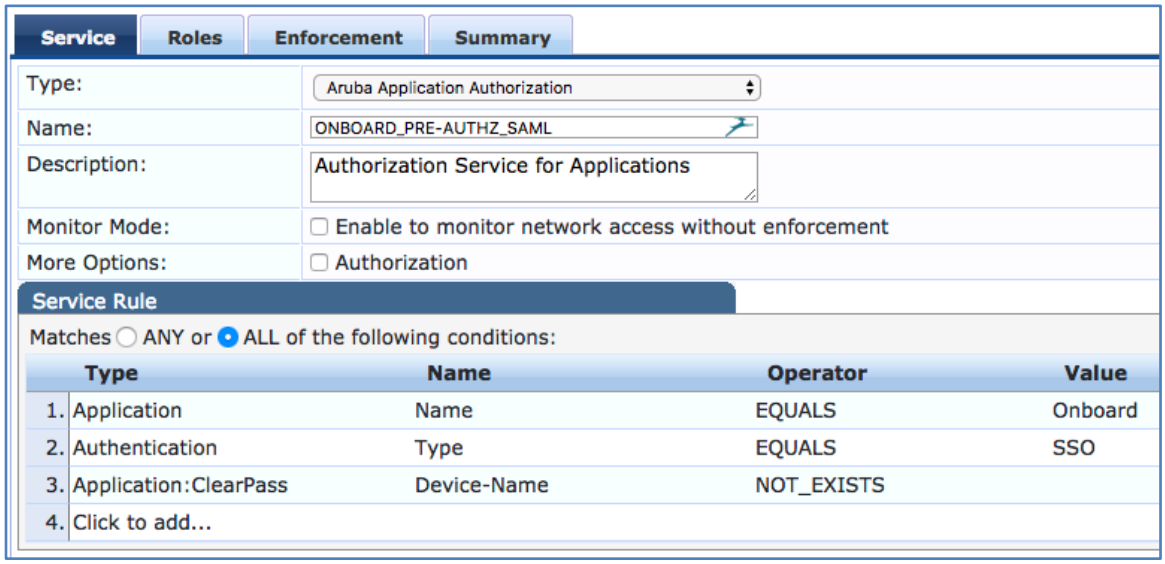


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD_PRE-AUTHZ_SAML* for example.

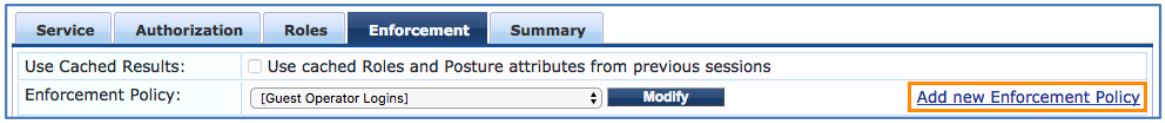
Uncheck the **Authorization** checkbox next to More Options.

Under **Service Rules**, use the following:

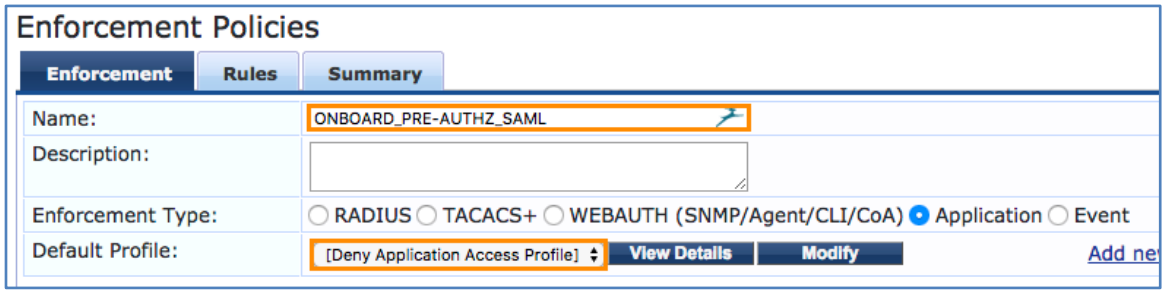
`Application`	`Name`	`EQUALS`	`Onboard`
`Authentication`	`Type`	`EQUALS`	`SSO`
`Application:ClearPass`	`Device-Name`	`NOT_EXISTS`	



Next skip over to the **Enforcement** tab and click **Add new Enforcement Policy**.



Give it the same name as the service and set the **Default Profile** to **[Deny Application Access Profile].**

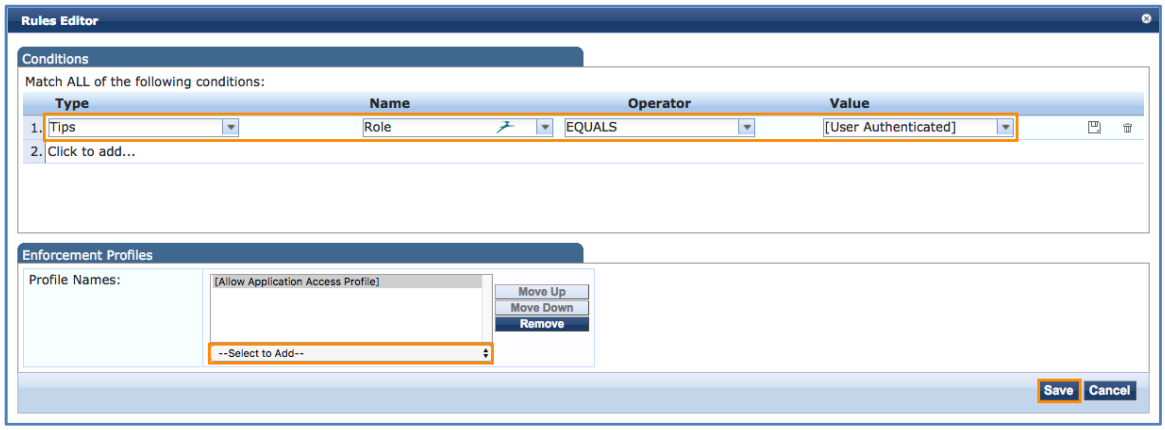


Move over to the **Rules** tab and click **Add Rule.**

Add the following condition:

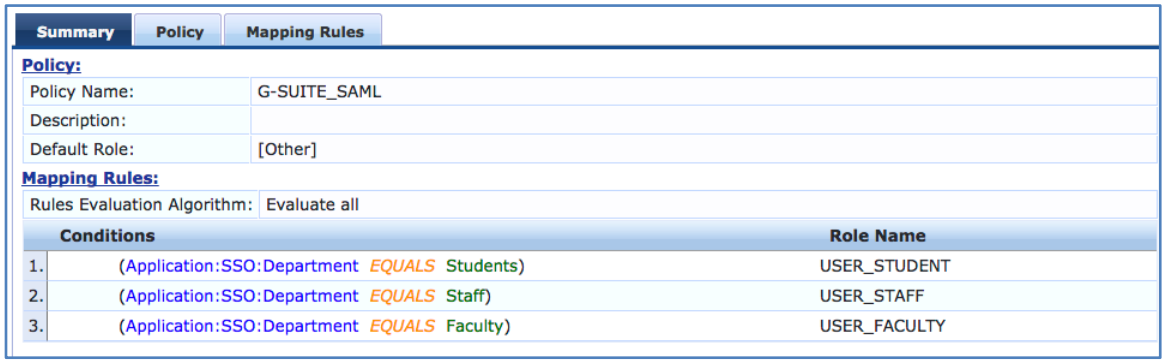
```
TIPS        Role        EQUALS        [User Authenticated]
```

Select **[Allow Application Access Profile]** under Enforcement Profiles. Click Save.



If return attributes from Google will be used in policy, add rules to reference the attributes in the Application:SSO namespace.

The screenshots below are examples of a role map and application enforcement policy leveraging group membership attributes to override certificate lifetime and device caps for certain users.



Summary | Policy | Mapping Rules

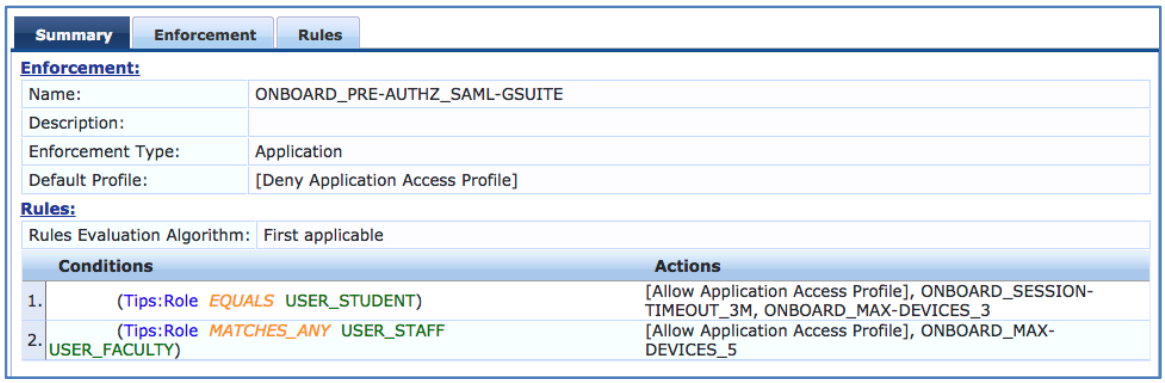
Policy:

Policy Name:	G-SUITE_SAML
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Application:SSO:Department *EQUALS* Students)	USER_STUDENT
2.	(Application:SSO:Department *EQUALS* Staff)	USER_STAFF
3.	(Application:SSO:Department *EQUALS* Faculty)	USER_FACULTY



Summary | Enforcement | Rules

Enforcement:

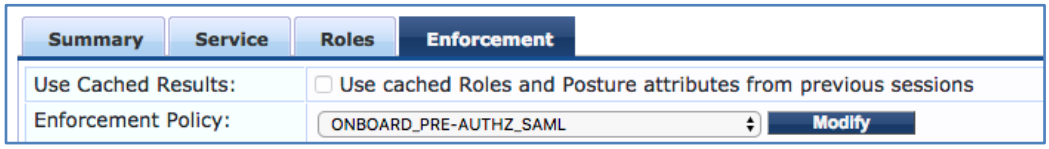
Name:	ONBOARD_PRE-AUTHZ_SAML-GSUITE
Description:	
Enforcement Type:	Application
Default Profile:	[Deny Application Access Profile]

Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* USER_STUDENT)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M, ONBOARD_MAX-DEVICES_3
2.	(Tips:Role *MATCHES_ANY* USER_STAFF USER_FACULTY)	[Allow Application Access Profile], ONBOARD_MAX-DEVICES_5

Now select the newly created Enforcement Policy from the drop-down list and then click **Save** at the bottom.



Summary | Service | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	ONBOARD_PRE-AUTHZ_SAML [Modify]

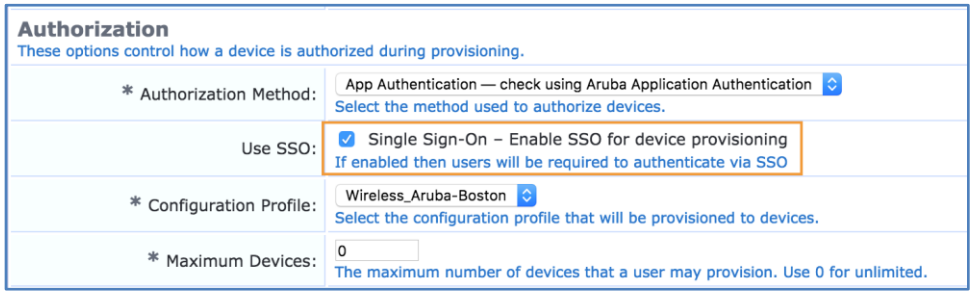
Move this newly created service above any other Onboard application services.

ClearPass Onboard Configuration

Very little configuration is required for SAML in Onboard.

Edit the Provisioning Settings under **Onboard » Deployment and Provisioning » Provisioning Settings**

In the authorization section, check **Single Sign-On – Enable SSO for device provisioning**, then click **Save Changes** at the bottom.



That's the only change required in the Onboard configuration.

NAD Whitelist

In order for clients to be able to reach the Google accounts login page and other embedded resources, certain domain names need to be whitelisted.

The most up to date version of this whitelist as well as examples for Aruba mobility controllers and Aruba Instant are available on the Aruba GitHub: https://github.com/aruba/clearpass-cloud-service-whitelists.

Direct Link: https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_google.md

Sample Request

Request Details

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W00000203-01-595fda8a
Date and Time:	Jul 07, 2017 15:01:31 EDT
End-Host Identifier:	-
Username:	bob@socialwifilogin.net
Access Device IP/Port:	-:-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	ONBOARD_PRE-AUTHZ_SAML
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	USER_STUDENT, [User Authenticated]
Enforcement Profiles:	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M, ONBOARD_MAX-DEVICES_3
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-32 records

Change Status | Show Configuration | Export | Show Logs | Close

Request Details

Summary | Input | Output

Username:	bob@socialwifilogin.net
End-Host Identifier:	-
Access Device IP/Port:	-:-

Computed Attributes

Application:Name	Onboard
Application:SSO:Department	Students
Application:SSO:Title	
Authentication:Full-Username	bob@socialwifilogin.net
Authentication:Full-Username-Normalized	bob@socialwifilogin.net
Authentication:Status	User
Authentication:Type	SSO
Authentication:Username	bob@socialwifilogin.net
Connection:Protocol	Application
Date:Date-of-Year	2017-07-07
Date:Date-Time	2017-07-07 15:01:31
Date:Day-of-Week	Friday

Showing 1 of 1-32 records

Change Status | Show Configuration | Export | Show Logs | Close

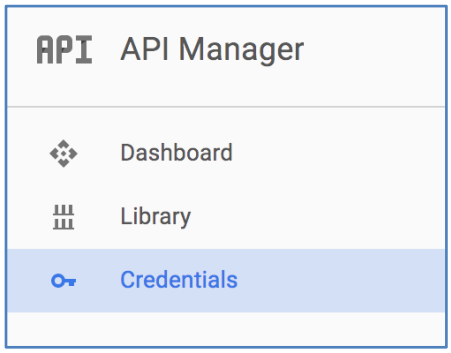
OAuth 2.0

Google Admin Console Configuration

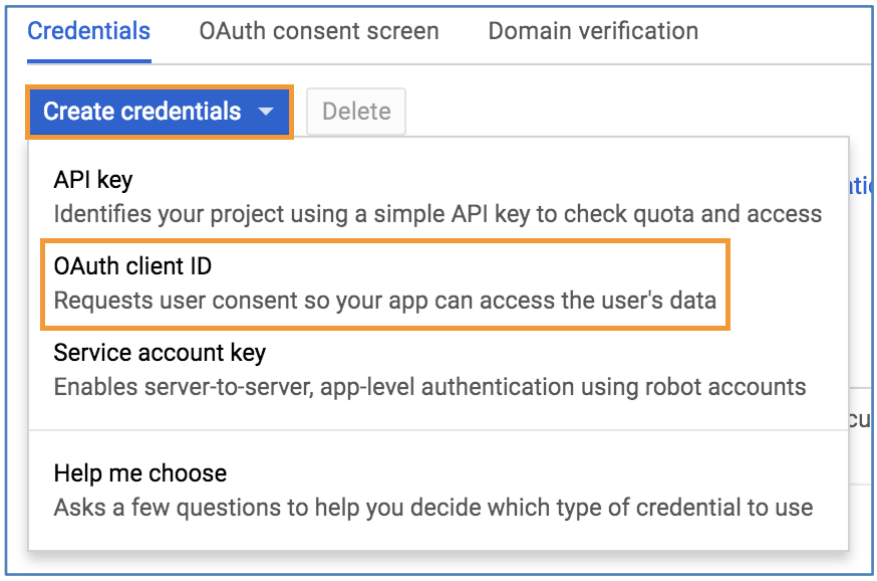
Application Setup

Log into the Google Developer Console at console.developers.google.com.

From the **API Manager** menu on the left, click **Credentials**.

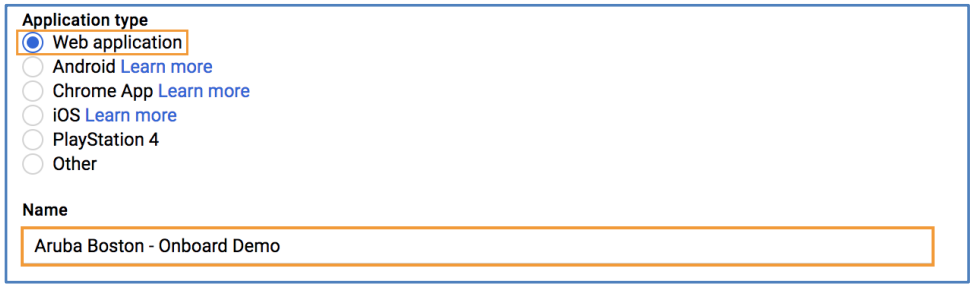


Click **Create credentials** and then **OAuth client ID**.



For **Application type**, choose **Web application**.

For name, use something user friendly as it will be presented to the end user the first time they access the service with their account.



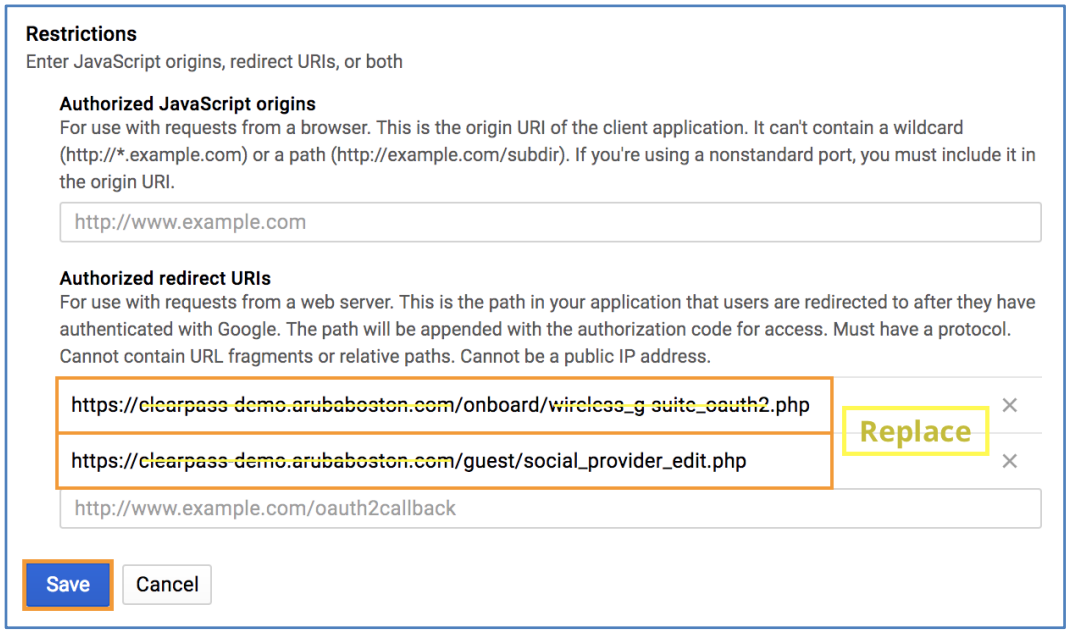
Down under **Restrictions** and then **Authorized redirect URIs**, enter the ClearPass FQDN with the planned Onboard page name (do not include any URL parameters after ".php" if present):

`https://<clearpass-fqdn>/onboard/<page-name>.php`

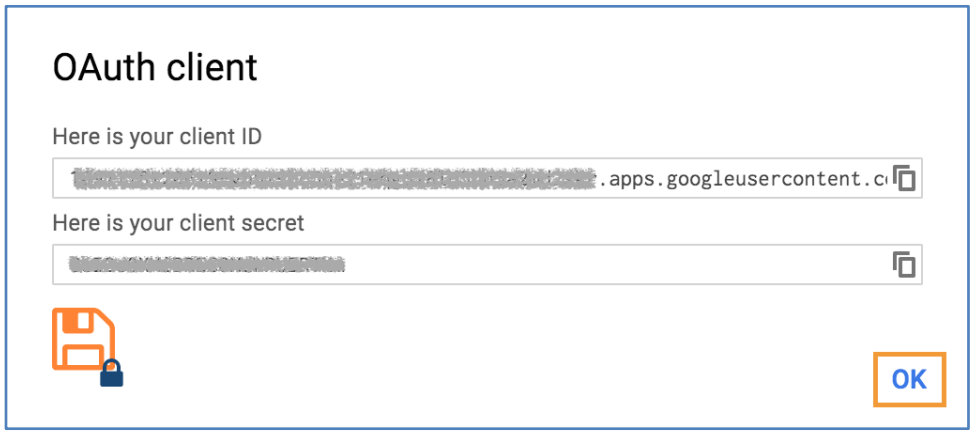
Add a second entry, replacing <clearpass-fqdn>:

`https://<clearpass-fqdn>/guest/social_provider_edit.php`

Click **Save** to finish.



A dialog box will appear with the Client ID and Client Secret. Store these securely. They will be required to configure the ClearPass side of things. Click **OK** to finish.



Google Developer Verification Override

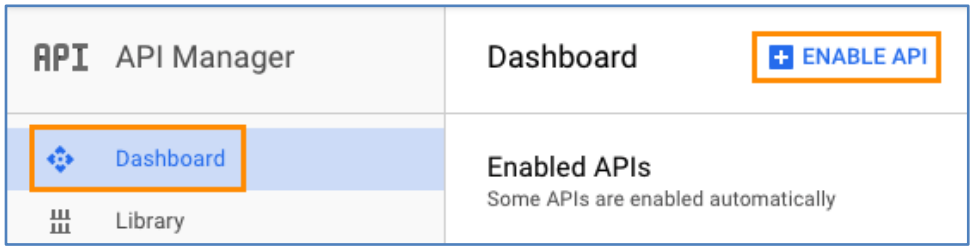
Google now requires that all OAuth web apps be verified. Because this is a custom configuration for each Cloud Identity or G Suite tenant, this web app must be enabled as an "Unreviewed" app.

While logged in with G Suite admin credentials, navigate to https://groups.google.com/forum/#!forum/risky-access-by-unreviewed-apps and click **Join group**. Now custom OAuth web apps will be allowed.

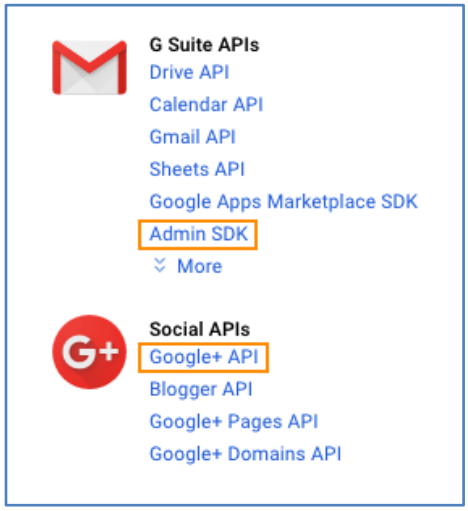
Enable APIs

The ClearPass OAuth 2.0 framework leverages the Google Admin SDK and Google+ APIs.

To enable these, click Dashboard on the left and then **+ ENABLE API** at the top.



Under **Social APIs**, click **Google+ API** and then click **ENABLE** at the top. Click the back arrow and under **G Suite APIs**, click **Admin SDK** and then click **ENABLE** at the top.

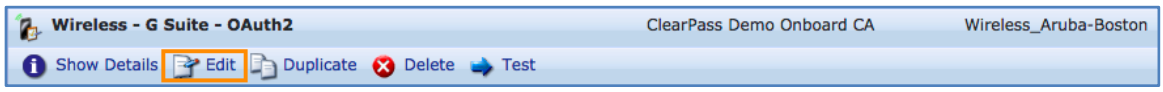


ClearPass Policy Manager Configuration

No specific configuration is required in Policy Manager. The standard Onboard authorization service will be used and pre-authentication will be handled automatically via the ClearPass OAuth 2.0 framework.

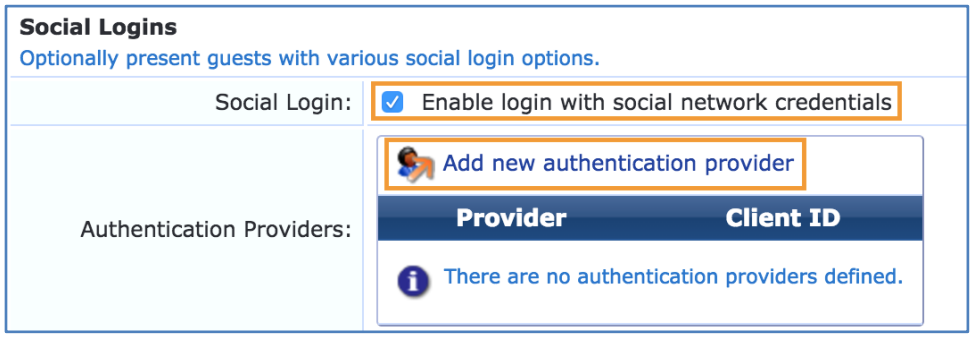
ClearPass Onboard Configuration

Navigate to **Onboard » Deployment and Provisioning » Provisioning Settings**, select the provisioning setting from the list and click **Edit**.



Go to the **Web Login** tab and scroll down to Social Logins.

Check **Enable login with social network credentials** and then click **Add new authentication provider**.

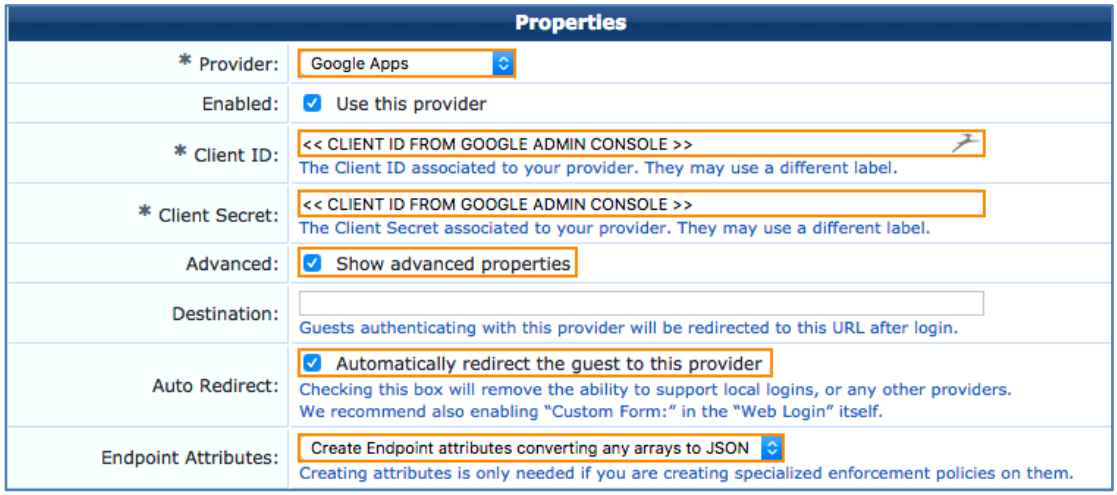


Select **Google Apps** as the **Provider**.

Enter the **Client ID** and **Client Secret** that were presented in the Google Admin Console in the previous section.

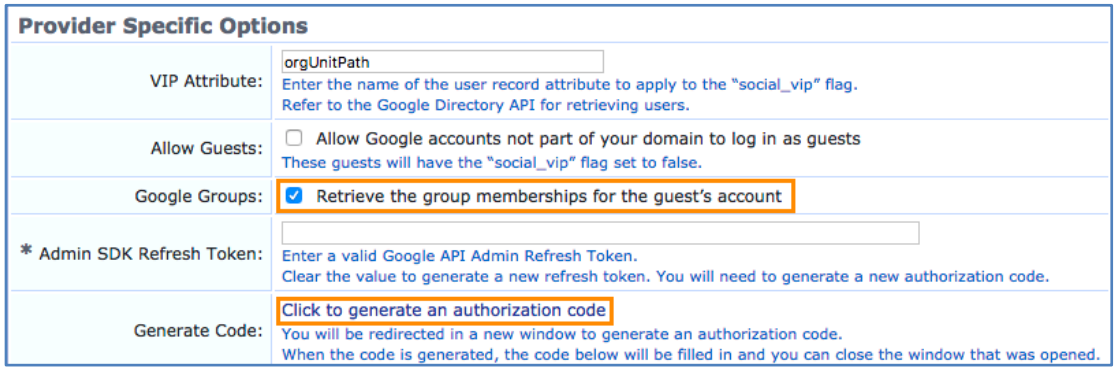
G Suite will be the only identity provider for Onboard so check **Show advanced properties** and then **Automatically redirect the guest to this provider**.

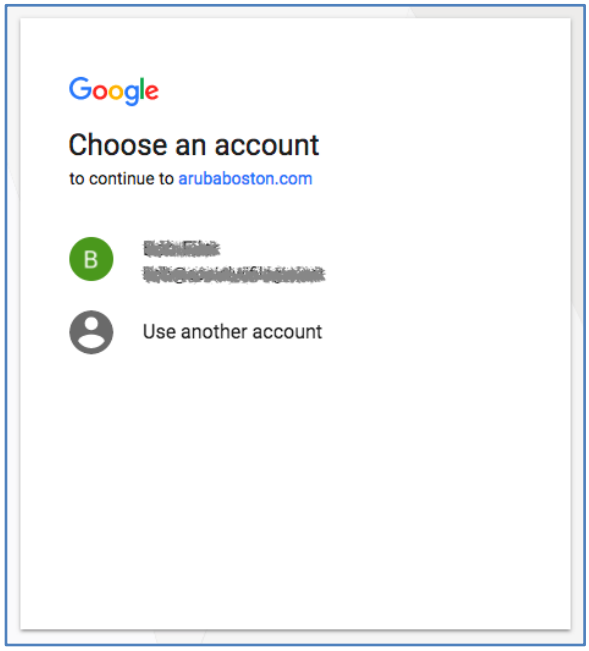
For **Endpoint Attributes**, select **Create Endpoint converting any arrays to JSON**.

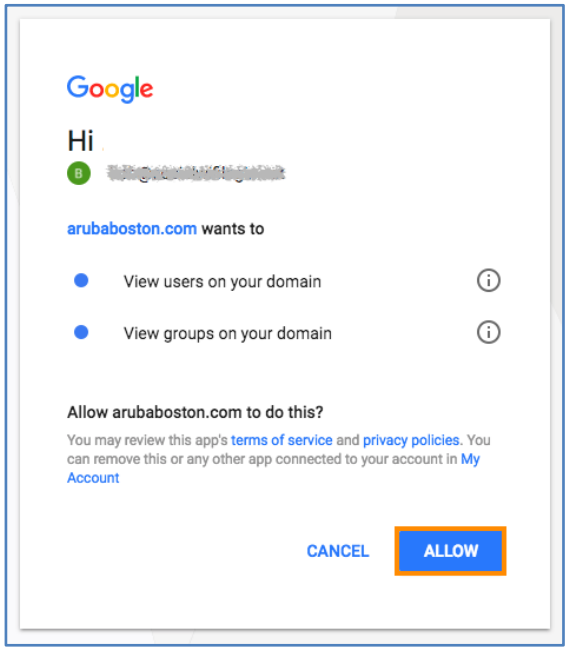


Check **Retrieve the group memberships for the guest's account**.

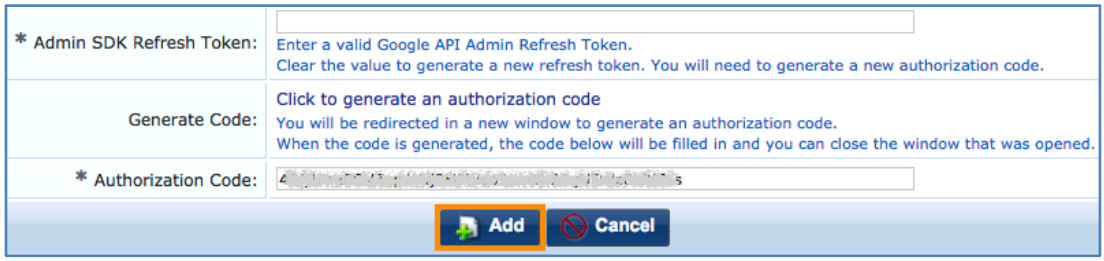
An authorization code is needed in order for ClearPass to be able to pull user and group information. **Click to generate an authorization code** to be redirected to the Google login to authorize the request.







The **Authorization Code** field will be auto populated from the response. Leave Admin SDK Refresh Token blank and click **Add**.



Because Google will be the only identity provider for Onboard, scroll up to the Login Form section and check **Provide a custom login form.** Then click **Save Changes** at the bottom of the page.

NAD Whitelist

In order for clients to be able to reach the Google accounts login page and other embedded resources, certain domain names need to be whitelisted.

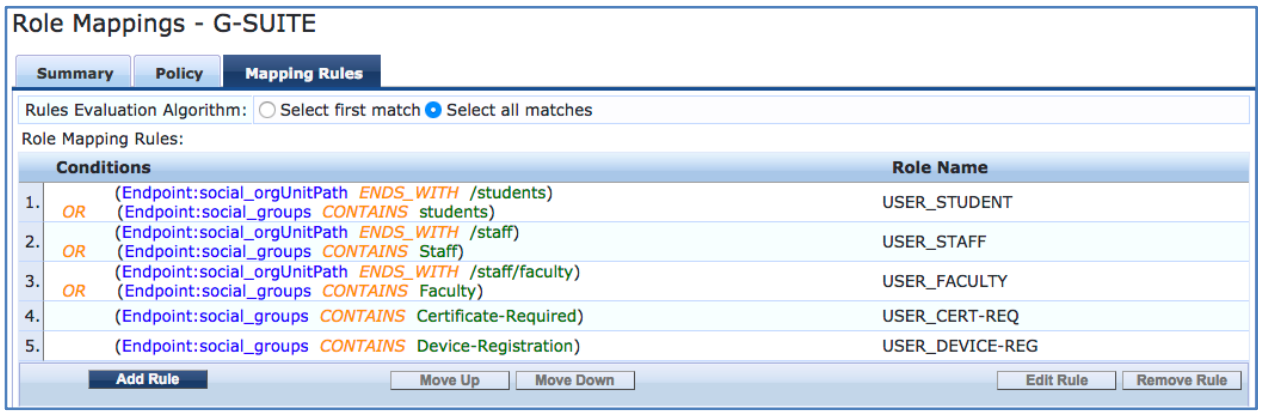
The most up to date version of this whitelist as well as examples for Aruba mobility controllers and Aruba Instant are available on the Aruba GitHub: https://github.com/aruba/clearpass-cloud-service-whitelists.

Direct Link: https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_google.md

Dynamic Policy Using Google Cloud Identity

If access to Google's Secure LDAP Service is not available, the attributes returned during Onboard pre-authentication can be leveraged post-Onboard as part of a role map or enforcement policy.

The screenshot below is an example of a role map in a standard 802.1X service, leveraging organizational unit and group membership attributes.



Okta

Okta is a popular cloud identity management solution and ClearPass can leverage it as a SAML Identity Provider for Onboard enrollment.

When a user initiates Onboarding, usually by clicking the Onboard link on a guest portal, they will be redirected straight to the Okta login page. After a successful authentication (and potential MFA challenge), they will be redirected to ClearPass Onboard to begin device enrollment.

During the redirection back to ClearPass, Okta will send various reply attributes about the user that can be used in the pre-authentication policy.

Feature	SAML
Requires User Consent Dialog	✗
Group Membership	✓
Custom reply attributes	✓
Workflow Specific Features	**SAML**
Evaluate return attributes during Onboard pre-authentication	✓
Evaluate return attributes during subsequent EAP-TLS authentication/authorization	✗

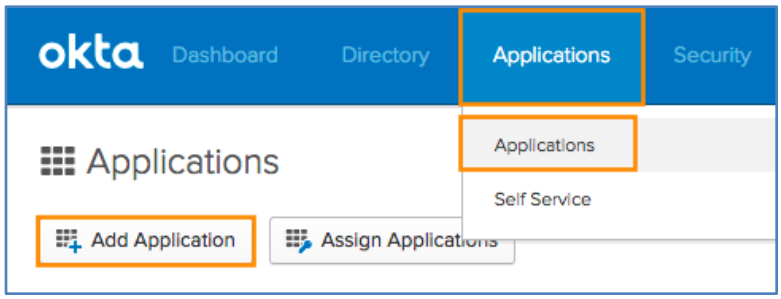
SAML

Okta Configuration

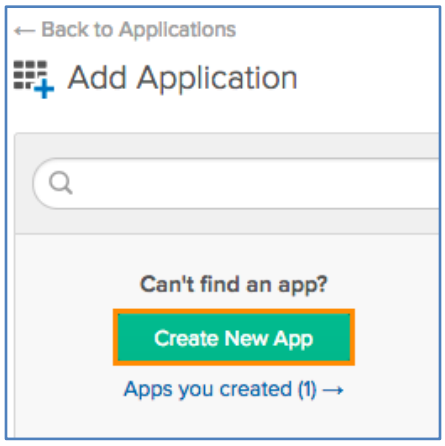
Application Setup

Log into the Okta admin portal using the custom admin FQDN (usually something like `<company>-admin.okta.com/admin`) with admin privileges for the organization.

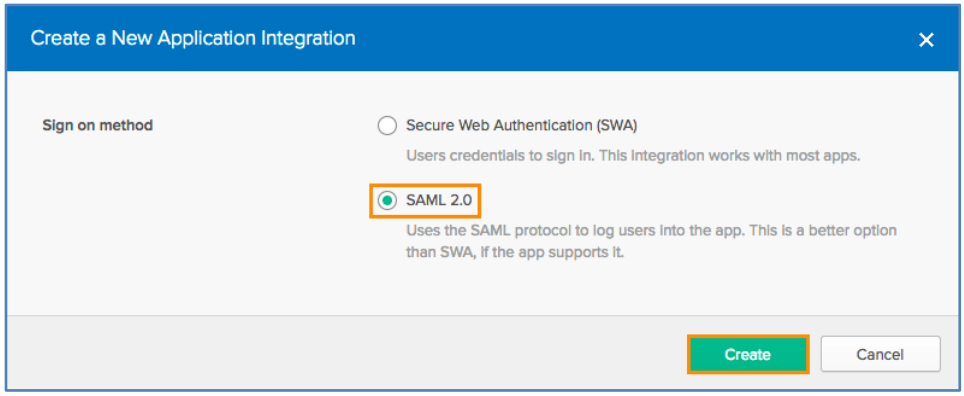
On the top menu bar, click **Applications**, and then **Applications** from the submenu. Then click **Add Application**.



Click **Create New App**.

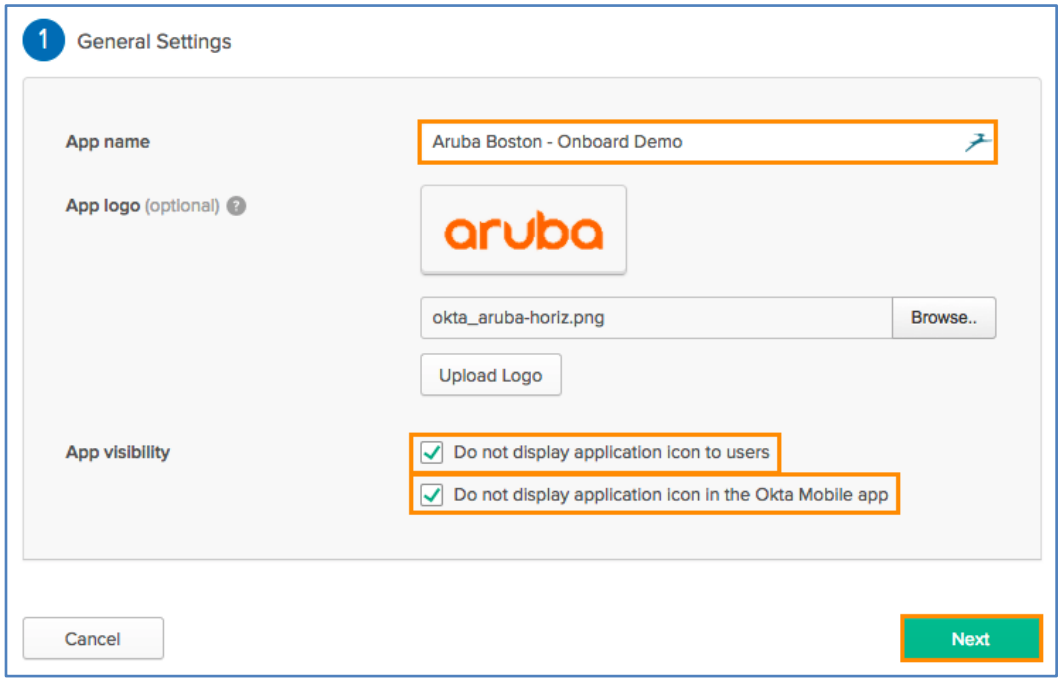


Select **SAML 2.0** and then click **Create**.



Give the application a user-friendly name as end users will see it briefly during the login process.

Optionally upload an app logo and then check **Do not display application icon to users** and **Do not display application icon in the Okta Mobile app.** Then click **Next.**

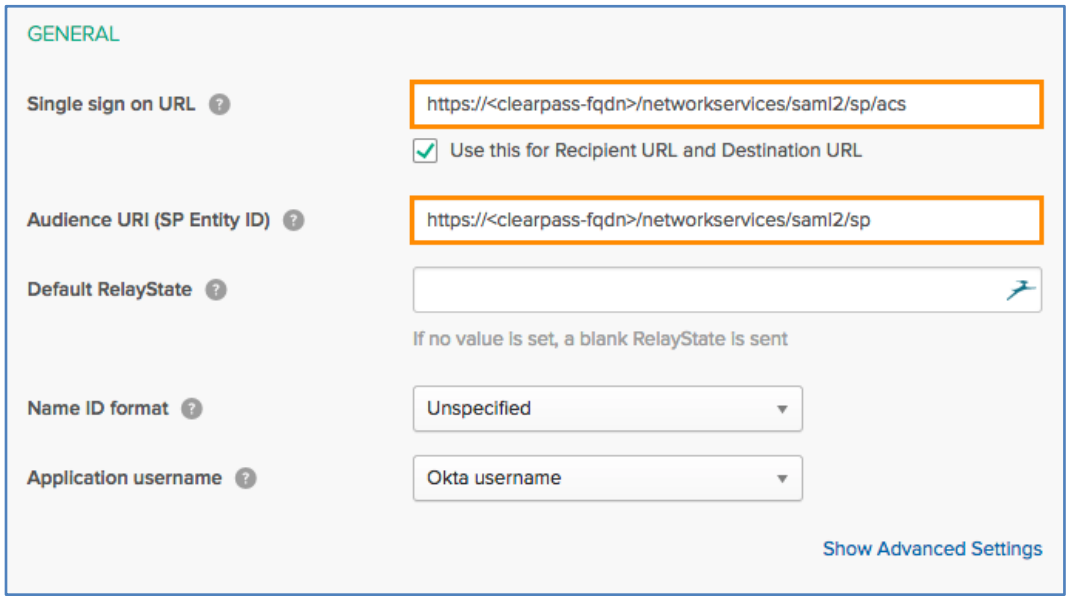


The **Single sign on URL** is the SAML Assertion Consumer Service and is the same URI path in all ClearPass installations. Replace <clearpass-fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

```
https://<clearpass-fqdn>/networkservices/saml2/sp/acs
```

The **Audience URI** is the service provider entity ID URI and is the same URI path in all ClearPass installations. Replace <clearpass-fqdn> with the user-facing ClearPass fully qualified domain name (FQDN):

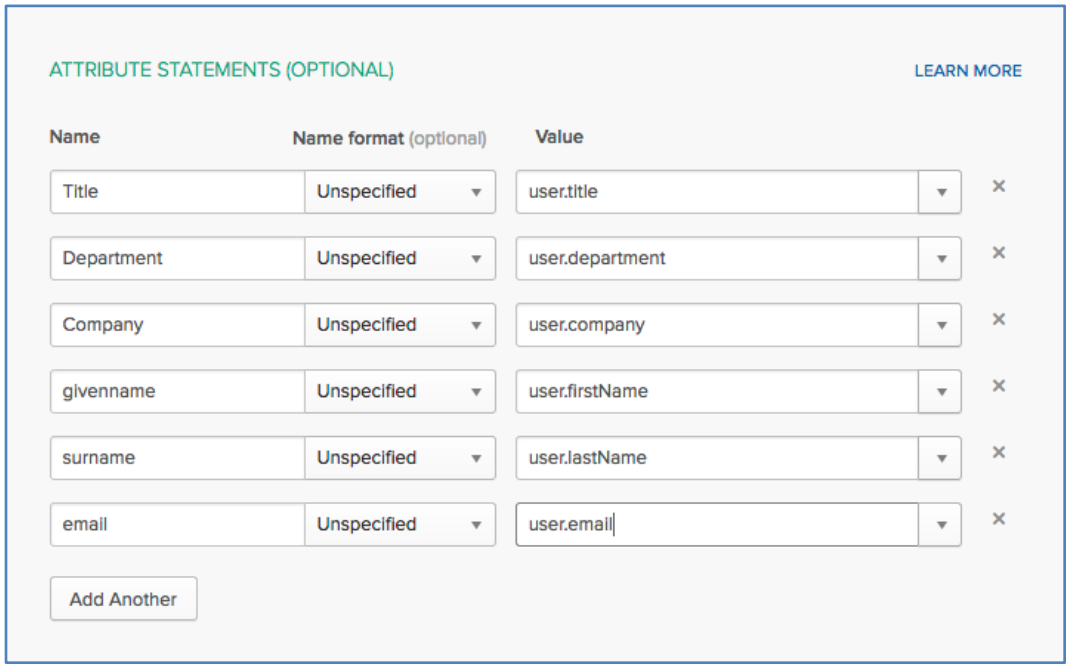
```
https://<clearpass-fqdn>/networkservices/saml2/sp
```



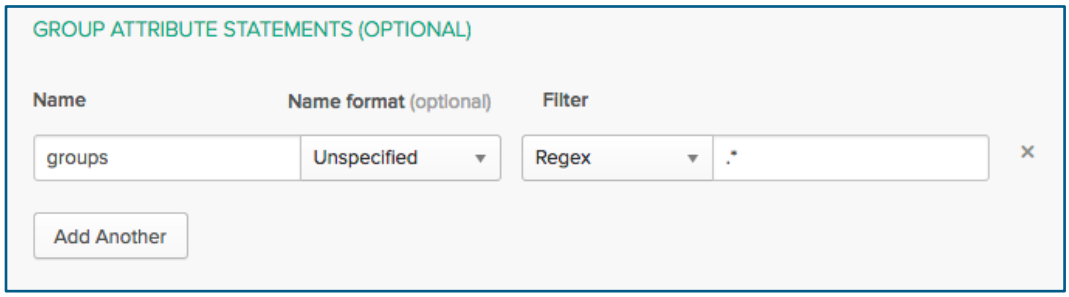
By default, only the username is passed in the SAML assertion. Additional attributes can be added using the **Attribute Statements**.

The **Name** field is the SAML Attribute name. **Name format** can stay **Unspecified**. The **Value** field is the Okta attribute name. The example below maps *Title*, *Department*, *Company*, *givenname*, *surname* and *email*.

NOTE: Not all Okta attributes are present in the dropdown.
They can be manually entered.

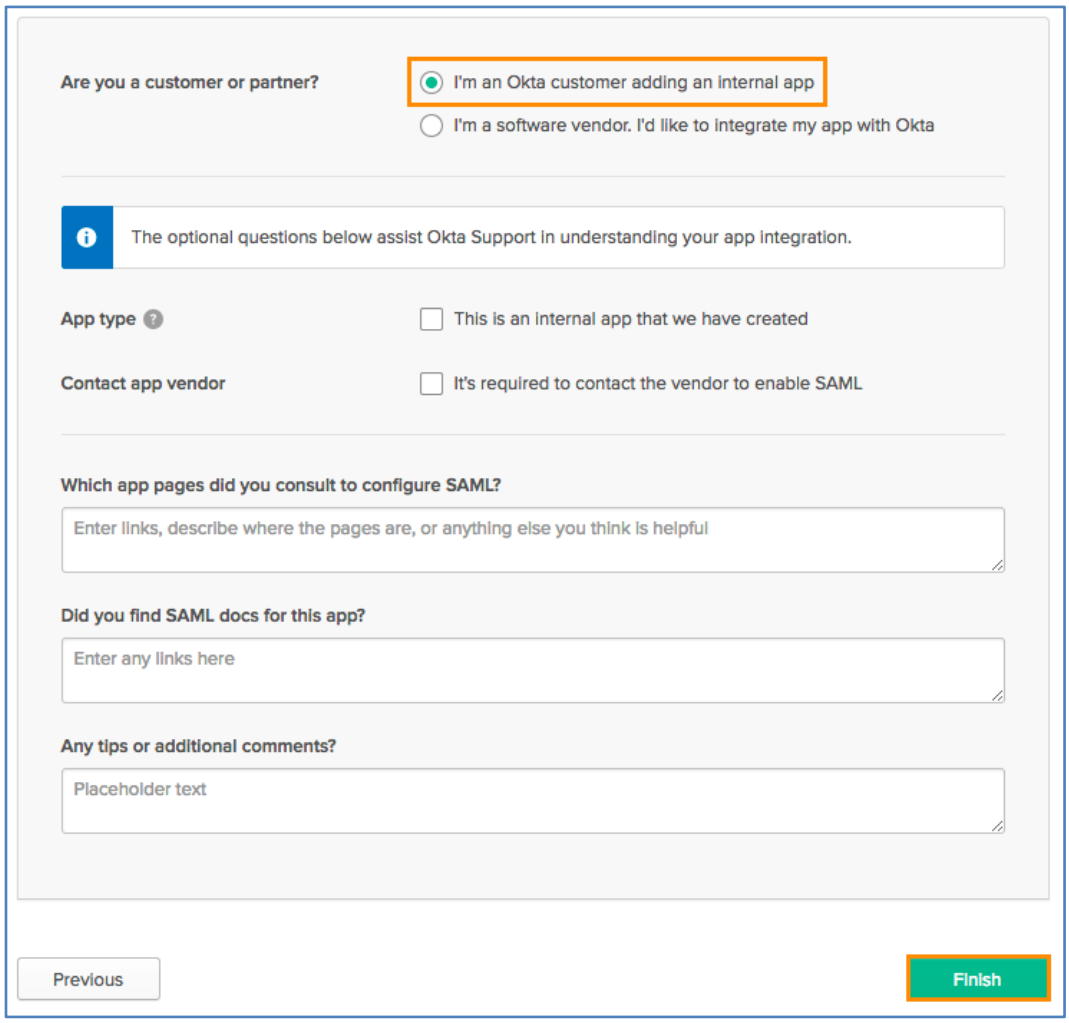


Group membership can also be returned. Under **Group Attribute Statements**, set the **Name** to **groups** and set the **Filter** to **Regex** with dot wildcard (**.***) as the value.



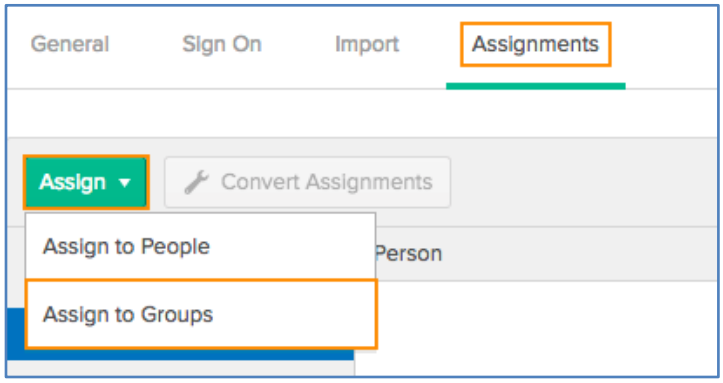
Click **Next** when finished.

On step 3, select **I'm an Okta customer adding an internal app** and then click **Finish**.



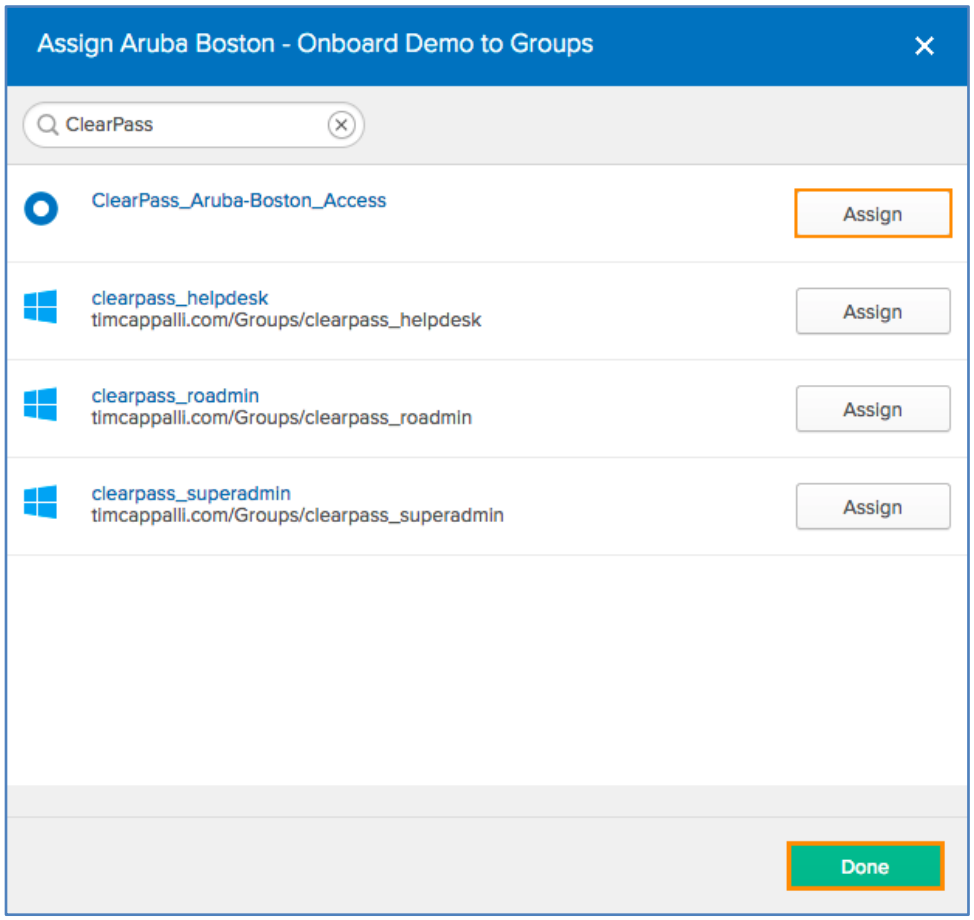
User Assignment

Okta requires that all applications be explicitly assigned to users or groups. Click the **Assignments** tab, the **Assign** button and then **Assign to Groups**.



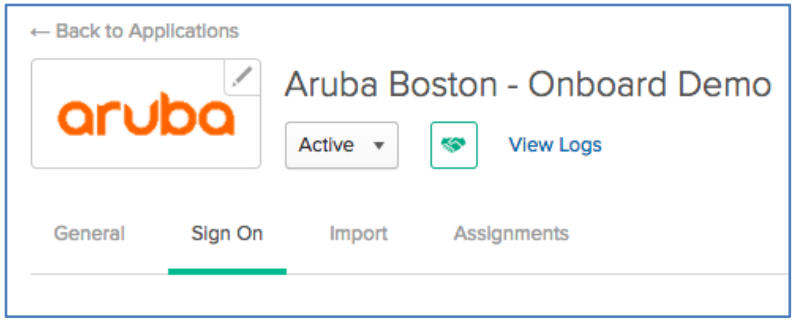
Search for the group(s) and then click **Assign**. Click **Done** when finished.

To assign individual users, repeat the process but choose **Assign to People** instead.

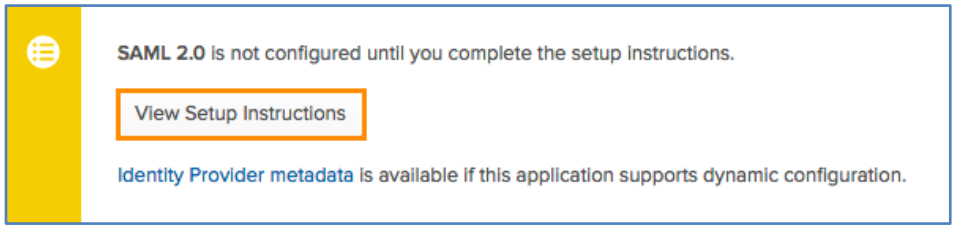


SAML Metadata

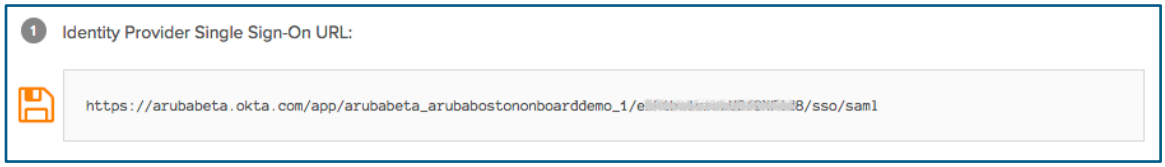
Now move over to the **Sign On** tab.



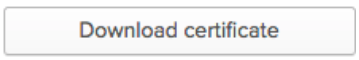
In the settings box, click the **View Setup Instructions** button.



Copy and store the URL provided in section 1, **Identity Provider Single Sign-On URL**. This will be required to configure the ClearPass side.



In section 3, **X.509 Certificate**, click **Download certificate**.



ClearPass Policy Manager Configuration

IdP Certificate

The first step in Policy Manager is to upload the identity provider certificate provided in the Okta setup.

Navigate to **Administration** » **Certificates** » **Trust List** and click **Add**.

Browse for the previously downloaded certificate and then click **Add Certificate**.

> **NOTE**: The certificate will be self-signed and the common name will be the Okta tenant name with an OU of *SSOProvider*.

The certificate should now appear in the trust list as Enabled.

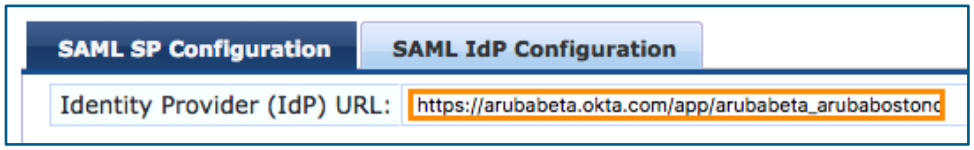
Service Provider Configuration

Next, Policy Manager needs to be configured to use Okta as a SAML Identity Provider and enable it for use with Onboard workflows.

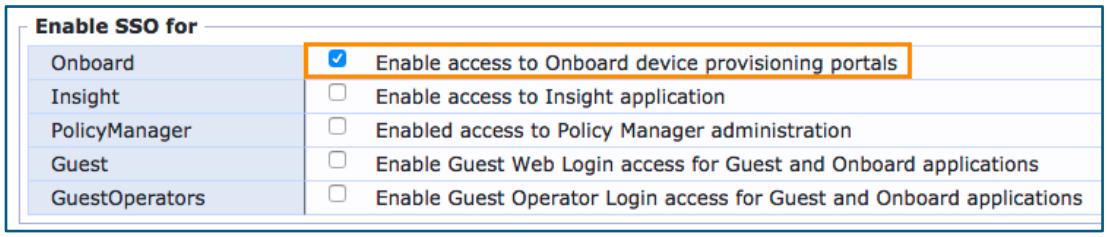
Navigate to **Configuration** » **Identity** » **Single Sign-On (SSO)**.

For **Identity Provider (IdP) URL**, enter in the **Login URL/SignOn URL** that was saved earlier from the Okta metadata page. The URL should look something like this:

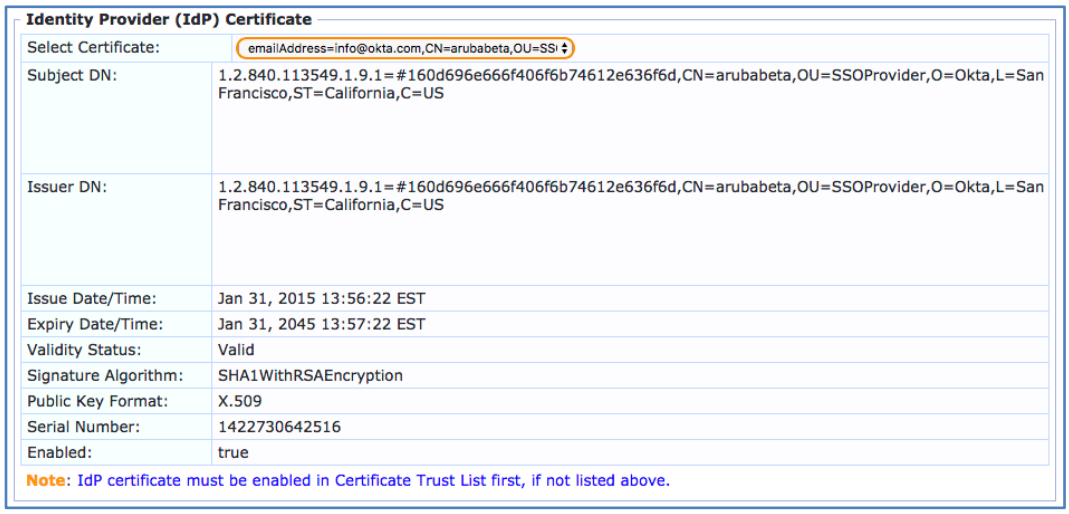
`https://<tenant-name>.okta.com/app/<app-name>/<GUID>/sso/saml`



Check **Enable access to Onboard device provisioning portals**.



Finally, select the **Okta** certificate from the down-down list under **Identity Provider (IdP) Certificate**.



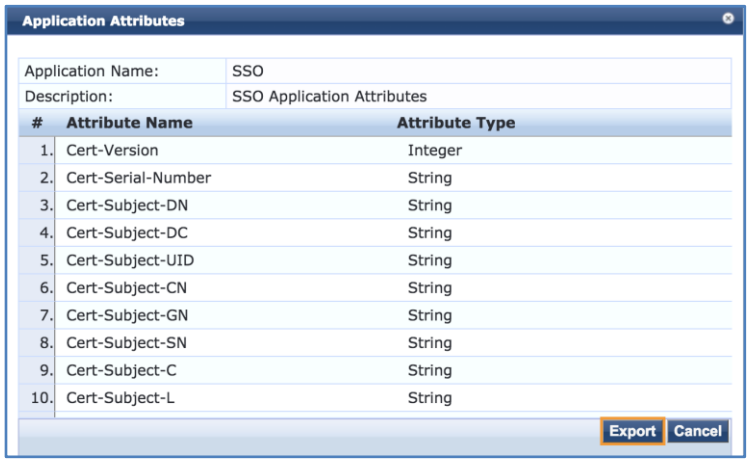
Click **Save** at the bottom.

Application Dictionary

If there is a need to assign different Onboard configuration overrides using SAML Token Attributes, the ClearPass SAML dictionary will need to be updated. Examples would be using a different certificate lifetime for different types of users or even using a different configuration profile. If SAML Token Attributes will not be used in Onboard pre-authentication, skip this step.

NOTE: Department, Title, and Company are available by default in ClearPass and do not require any changes to the SSO dictionary.

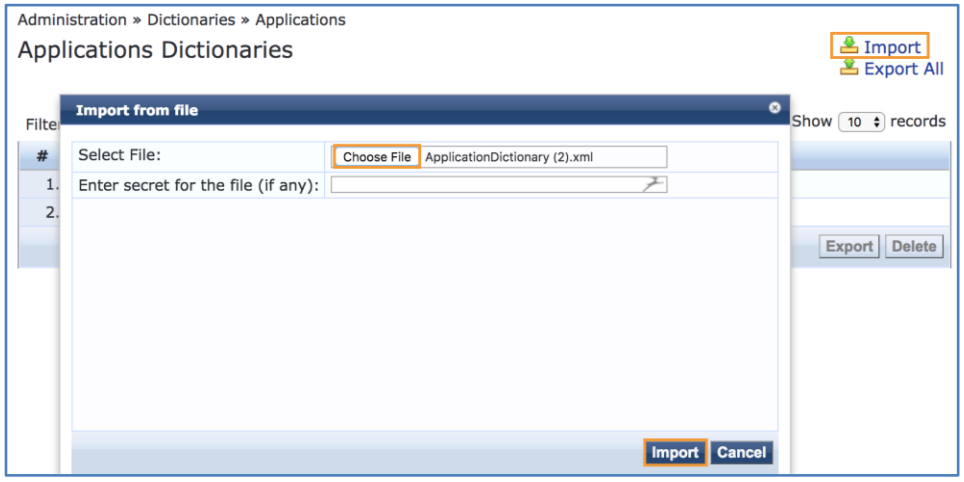
Navigate to **Administration » Dictionaries » Applications**, click on **SSO** and then click **Export**.



Open the exported XML file in a text editor. Add the SAML Token Attributes, following the same format as the existing entries. Below is an example for the ***groups*** attribute.

```
<ApplDictionaryAttributes attrType="String" attrName="groups"/>
```

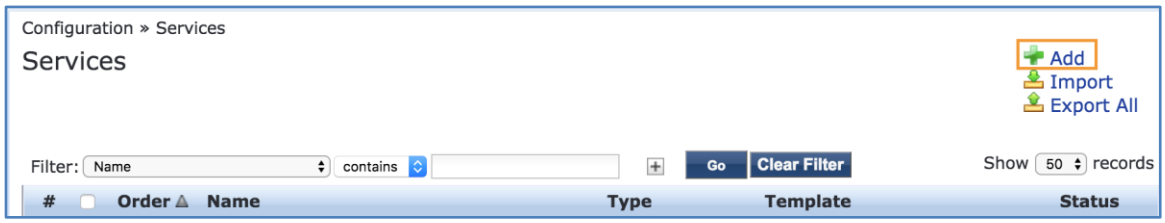
Once all of the desired attributes have been added, save the file and import it back into ClearPass.



Onboard Pre-Authentication Service

A new service will be required to handle the Onboard SAML pre-authentication.

Navigate to **Configuration » Services** and then click **Add**.

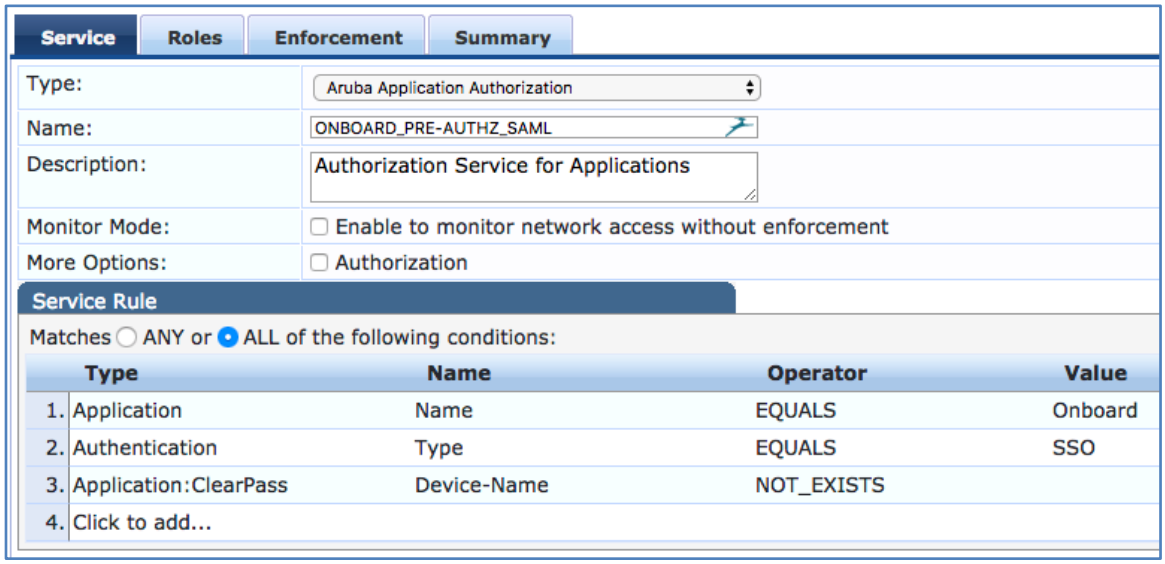


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD_PRE-AUTHZ_SAML* for example.

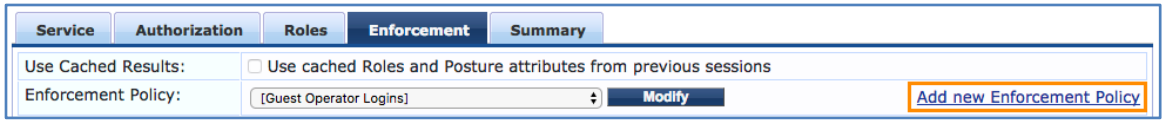
Uncheck the **Authorization** checkbox next to More Options.

Under **Service Rules**, use the following:

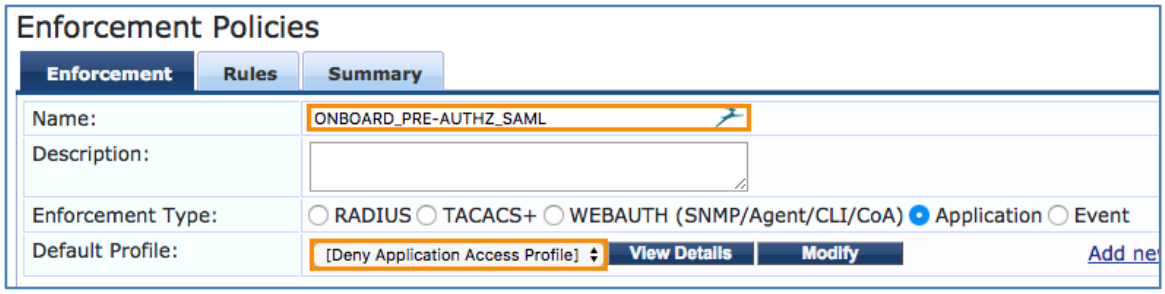
`Application`	`Name`	`EQUALS`	`Onboard`
`Authentication`	`Type`	`EQUALS`	`SSO`
`Application:ClearPass`	`Device-Name`	`NOT_EXISTS`	



Next skip over to the **Enforcement** tab and click **Add new Enforcement Policy**.



Give it the same name as the service and set the **Default Profile** to **[Deny Application Access Profile].**

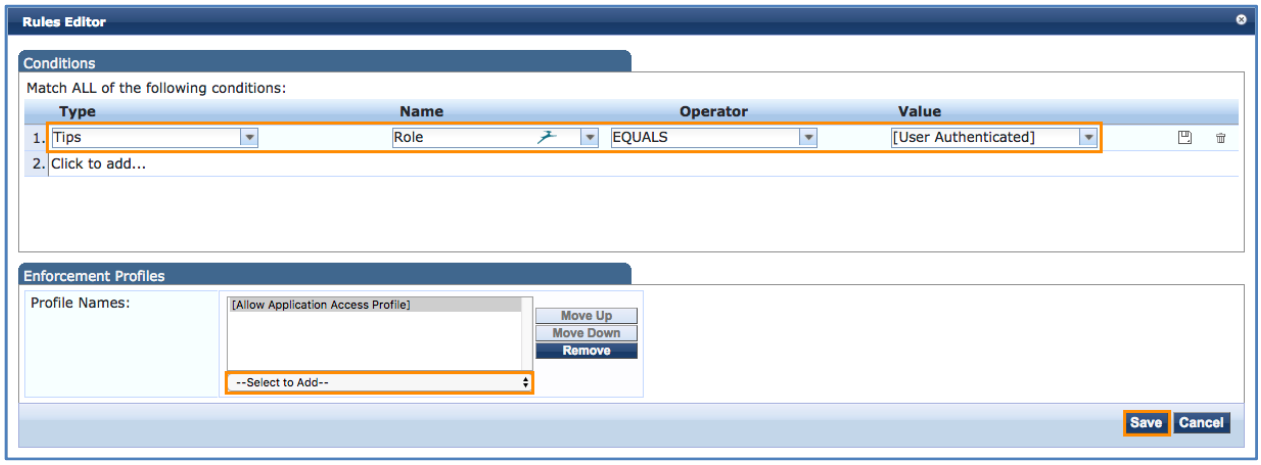


Move over to the **Rules** tab and click **Add Rule.**

Add the following condition:

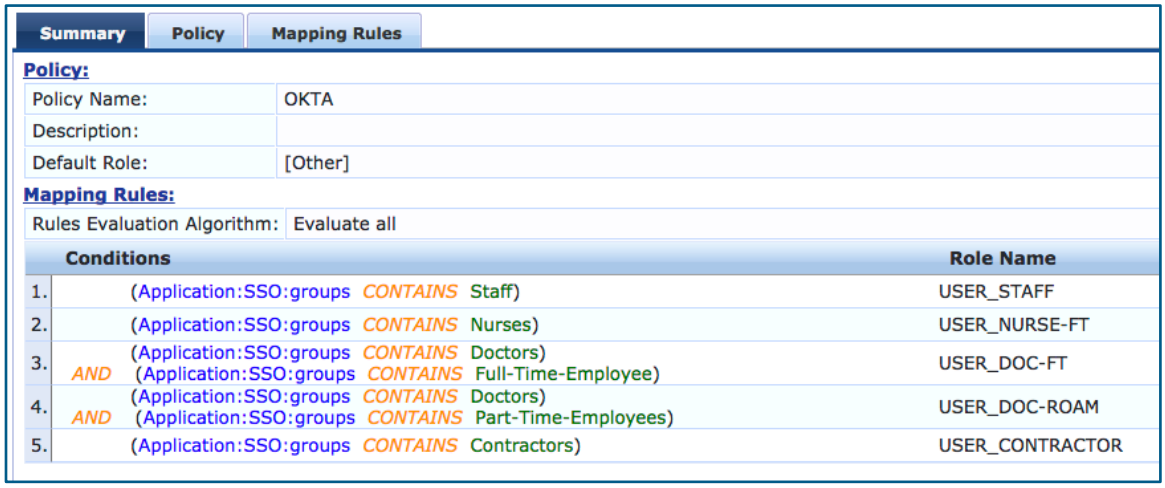
```
TIPS        Role        EQUALS        [User Authenticated]
```

Select **[Allow Application Access Profile]** under Enforcement Profiles. Click Save.



If return attributes from Okta will be used in policy, add rules to reference the attributes in the Application:SSO namespace.

The screenshots below are examples of a role map and application enforcement policy leveraging group membership attributes to override certificate lifetime and device caps for certain users.



Summary | Policy | Mapping Rules

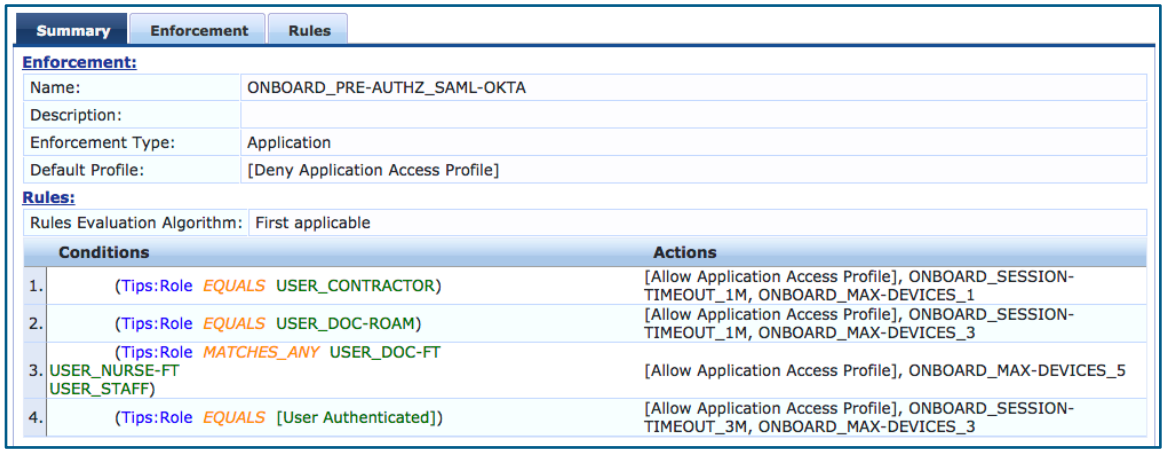
Policy:

Policy Name:	OKTA
Description:	
Default Role:	[Other]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

	Conditions	Role Name
1.	(Application:SSO:groups *CONTAINS* Staff)	USER_STAFF
2.	(Application:SSO:groups *CONTAINS* Nurses)	USER_NURSE-FT
3.	(Application:SSO:groups *CONTAINS* Doctors) *AND* (Application:SSO:groups *CONTAINS* Full-Time-Employee)	USER_DOC-FT
4.	(Application:SSO:groups *CONTAINS* Doctors) *AND* (Application:SSO:groups *CONTAINS* Part-Time-Employees)	USER_DOC-ROAM
5.	(Application:SSO:groups *CONTAINS* Contractors)	USER_CONTRACTOR



Summary | Enforcement | Rules

Enforcement:

Name:	ONBOARD_PRE-AUTHZ_SAML-OKTA
Description:	
Enforcement Type:	Application
Default Profile:	[Deny Application Access Profile]

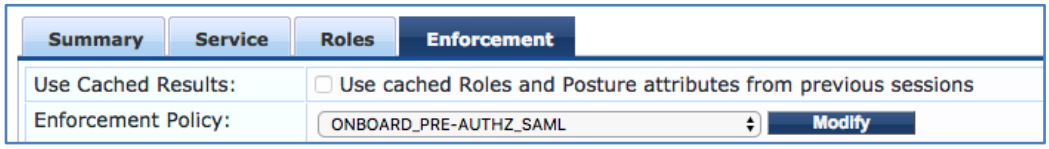
Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role *EQUALS* USER_CONTRACTOR)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_1M, ONBOARD_MAX-DEVICES_1
2.	(Tips:Role *EQUALS* USER_DOC-ROAM)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_1M, ONBOARD_MAX-DEVICES_3
3.	(Tips:Role *MATCHES_ANY* USER_DOC-FT USER_NURSE-FT USER_STAFF)	[Allow Application Access Profile], ONBOARD_MAX-DEVICES_5
4.	(Tips:Role *EQUALS* [User Authenticated])	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M, ONBOARD_MAX-DEVICES_3

After all the rules have been defined, click **Save** at the bottom.

Now select the newly created Enforcement Policy from the drop-down list and then click **Save** at the bottom.



Summary | Service | Roles | Enforcement

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	ONBOARD_PRE-AUTHZ_SAML ⇕ Modify

Move this newly created service above any other Onboard application services in the service list.

NAD Whitelist

In order for clients to be able to reach the Okta login page and other embedded resources, certain domain names need to be whitelisted.

The most up to date version of this whitelist as well as examples for Aruba mobility controllers and Aruba Instant are available on the Aruba GitHub: https://github.com/aruba/clearpass-cloud-service-whitelists.

Direct Link: https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_okta.md

Sample Request

Request Details

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	W0000037b-01-595e9a20
Date and Time:	Jul 06, 2017 16:21:34 EDT
End-Host Identifier:	-
Username:	tim@arubaboston.com
Access Device IP/Port:	-:-
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	ONBOARD_PRE-AUTHZ_SAML
Authentication Method:	Not applicable
Authentication Source:	-
Authorization Source:	-
Roles:	USER_STAFF, [User Authenticated]
Enforcement Profiles:	[Allow Application Access Profile], ONBOARD_MAX-DEVICES_5
Service Monitor Mode:	Disabled
Online Status:	Not Available

Showing 1 of 1-26 records

Change Status | Show Configuration | Export | Show Logs | Close

Request Details

Summary | Input | Output

Computed Attributes

Application:Name	Onboard
Application:SSO:Company	
Application:SSO:Department	timcappalli
Application:SSO:email	tim@arubaboston.com
Application:SSO:givenname	Tim
Application:SSO:groups	clearpass_superadmin, Okta-Sync, Azure-Enabled, Staff, Domain Users, nest-top, Everyone, REQUIRE-ONBOARD, FULL-ACCESS, nest-1, Airwave-Root, TACACS-ROOT, Azure-MFA, Allowed RODC Password Replication Group, PRTG-Admin, ClearPass_Aruba-Boston_Access
Application:SSO:surname	Cappalli
Application:SSO:Title	
Authentication:Full-Username	tim@arubaboston.com
Authentication:Full-Username-Normalized	tim@arubaboston.com
Authentication:Status	User
Authentication:Type	SSO

Showing 1 of 1-26 records

Change Status | Show Configuration | Export | Show Logs | Close

Additional Resources

Technologies

RFC 6749: The OAuth 2.0 Authorization Framework

RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage

SAML 2.0 OASIS Standard

ClearPass

ClearPass Policy Manager 6.7 User Guide

ClearPass Onboard 6.7 User Guide

TechNote: SAML Configuration Guide v1.5

TechNote: ClearPass REST APIs

Microsoft Azure Active Directory

Azure Active Directory Documentation Landing

Azure Active Directory + SAML

Azure Active Directory + OpenID Connect

Google Cloud Identity

G Suite Administrator Help Center

Google Secure LDAP service

Okta

Beginner's Guide to SAML

Single Sign-On

Adaptive MFA

Firewall Whitelisting

a Hewlett Packard
Enterprise company

www.arubanetworks.com
3333 Scott Blvd
Santa Clara, CA 95054
Phone: 1-800-WIFI-LAN (+800-943-4526)
Fax 408.227.4550