

# Onboard and Cloud Identity Providers



a Hewlett Packard  
Enterprise company

## ClearPass

Configuration Guide

# Onboard and Cloud Identity Providers

## 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

© Copyright 2018 Hewlett Packard Enterprise Development LP.

## Contents

Overview.....	4
Microsoft Azure Active Directory.....	5
SAML.....	7
OAuth 2.0.....	27
Google Cloud Identity .....	38
Google Secure LDAP Connector .....	40
SAML.....	52
OAuth 2.0.....	67
Okta.....	76
SAML.....	77
Additional Resources .....	92

## 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 city companyname country department displayname	objectType objectId accountEnabled assignedLicenses city companyName

dnsdomainname	country
facsimiletelephonenumber	department
givenname	dirSyncEnabled
jobtitle	displayName
mail	extension_*
mailnickname	facsimileTelephoneNumber
netbiosname	givenName
objectid	groups (Names)
onpremisesecurityidentifier	groups (Emails)
onpremisesamaccountname	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

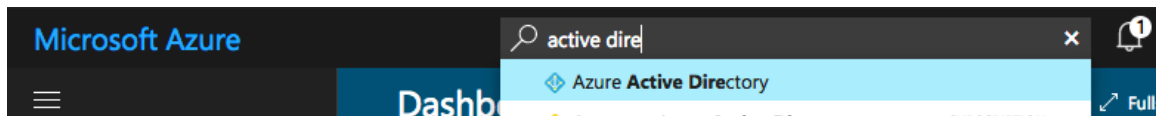
## SAML

### Azure Active Directory Configuration

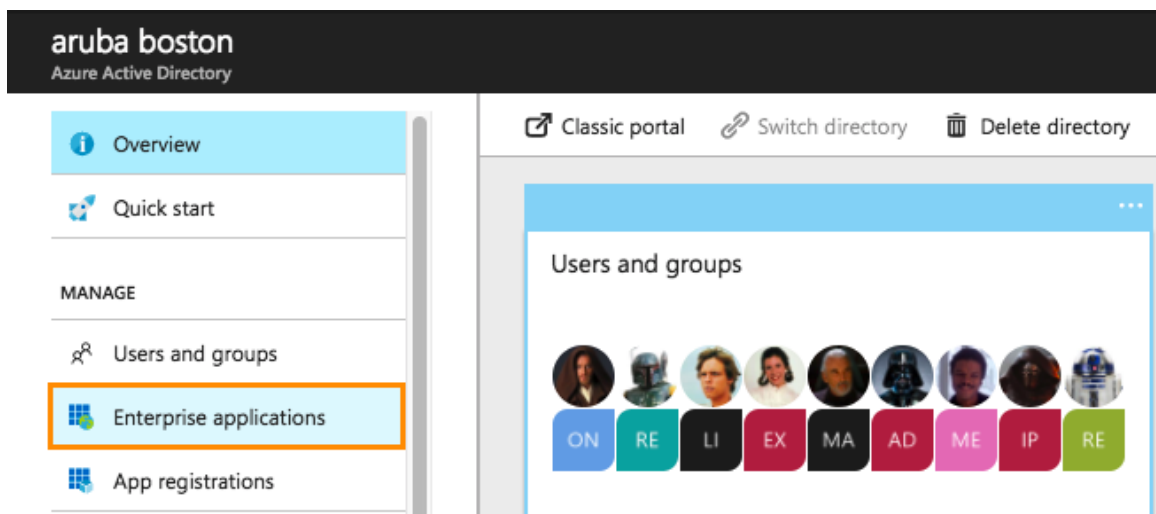
#### Application Setup

Log into the Microsoft Azure Portal at [portal.azure.com](https://portal.azure.com). Depending on the Azure IAM policy, you may need to log in as a Global Administrator.

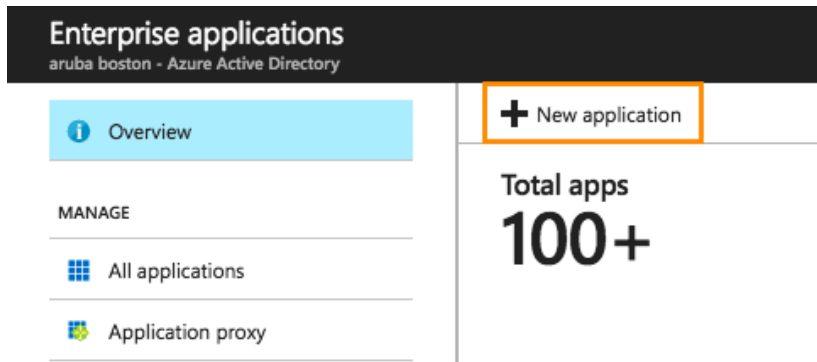
Using the search bar at the top, search for and select **Azure Active Directory**.



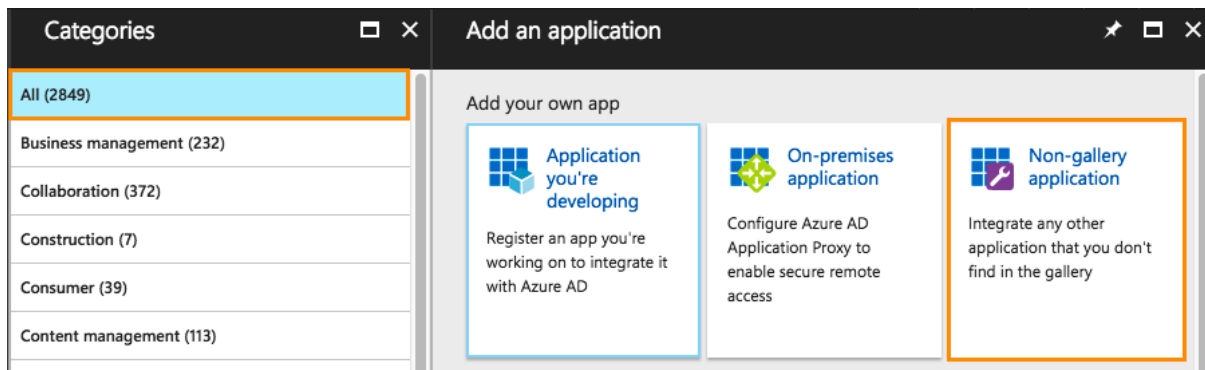
In the Azure Active Directory navigation blade, select **Enterprise applications**.



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**.

Add your own application

\*

Name

Aruba Boston Onboard Demo

✓

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

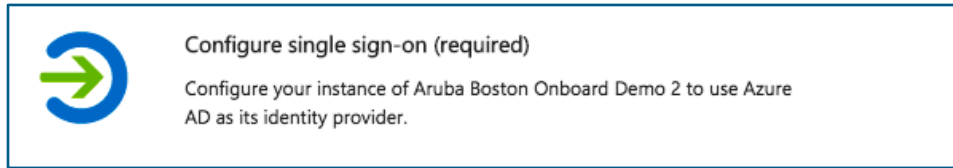
Supports:

- SAML-based single sign-on
- Application Proxy
- Automatic User Provisioning with SCIM
- Password-based single sign-on

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**.

Mode 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

Aruba Boston - Onboard Demo - SAML Domain and URLs

Input the URLs and other details about your Aruba Boston - Onboard Demo - SAML tenant into Azure AD.

\* Identifier ⓘ

\* Reply URL ⓘ

☐ Show advanced URL settings

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`

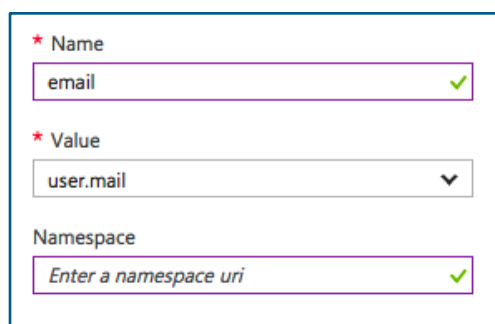
A few modifications need to be made and additional attributes can also be added. These changes to the SAML Token Attributes are only required if return attributes will be used as part of the Onboard enrollment policy decision.

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.

SAML Token Attributes		
NAME	VALUE	NAMESPACE
givenname	user.givenname	...
surname	user.surname	...
email	user.mail	...
name	user.userprincipalname	...
Department	user.department	...
Title	user.jobtitle	...
<a href="#">Add attribute</a>		

Add Attribute

\* Name

Company

✓

\* Value

user.companyname

▼

Namespace

Enter a namespace uri

Ok


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.

### SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to Aruba Boston - Onboard Demo - SAML.

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
New	6/21/2020	318FCB545657FA6DD5DBAF1D94138CD9E2F1B5F9	<a href="#">Certificate (Base64)</a> <a href="#">Certificate (Raw)</a> <a href="#">Metadata XML</a>

[Create new certificate](#)



Use the Aruba Boston - Onboard Demo - SAML Configuration section below to configure Aruba Boston - Onboard Demo - SAML to use the rollover certificate. Select the checkbox below and save when finished.

☒ Make new certificate active

★ Notification Email ⓘ

✓

☐ Show advanced certificate signing settings

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

### Aruba Boston - Onboard Demo - SAML Configuration

Aruba Boston - Onboard Demo - SAML must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.


Configure Aruba Boston - Onboard Demo - SAML

>



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.

3. During this process, you will be prompted to provide files and URLs that correspond to Azure Active Directory. When prompted, use the files and URLs shown below:

- **SAML Single Sign-On Service URL:** <https://login.microsoftonline.com/406a990a-06b2-4a9e-b00b-c3b95fe8d648/saml2>
- **SAML Entity ID:** <https://sts.windows.net/406a990a-06b2-4a9e-b00b-c3b95fe8d648/>
- **Sign-Out URL:** <https://login.microsoftonline.com/common/ws federation?wa=wsignout1.0>
- **SAML Signing Certificate - Base64 encoded** 
- **SAML Signing Certificate - Raw**
- **SAML XML Metadata**

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

 Save  Discard

Mode SAML-based Sign-on

Federated single sign-on enables rich and secure  
Salesforce to Azure AD using SAML.

## 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.

Aruba Boston - Onboard Demo - SAML - Properties

Enterprise Application

Overview Quick start

MANAGE

Properties Users and groups Single sign-on Provisioning Application proxy Self-service

SECURITY

Conditional access Permissions

ACTIVITY

Sign-ins

Save Discard

Enabled for users to sign-in? Yes No

Name Aruba Boston - Onboard Demo - SAML

Publisher Aruba Boston

Homepage URL

Logo

Select a file

User access URL https://myapps.microsoft.com/signin/Aruba%2...

Application ID b1ba3bf1-566b-4158-9bd1-8e79d800d25a

Object ID 9e298740-c2ee-418b-9379-8827208d4d3a

User assignment required? Yes No

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

Aruba Boston - Onboard Demo - SAML - Users and groups

Enterprise Application

Overview Quick start

MANAGE

Properties Users and groups

+ Add user Edit Remove

First 200 shown, to search all users & g

DISPLAY NAME

No application assignments found

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**.

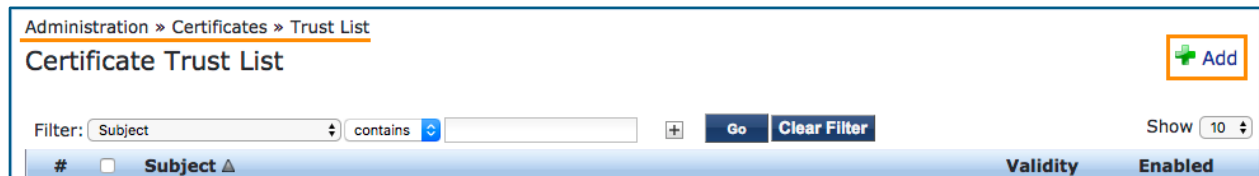
The image shows two side-by-side configuration windows. The left window, titled 'Add Assignment' with a subtitle 'aruba boston', contains a section 'Users and groups' with the text 'None Selected' and a right-pointing arrow. Below this is a 'Select Role' section with 'User' listed. At the bottom is an 'Assign' button. The right window, titled 'Users and groups', features a '+ Invite' button, a 'Select' dropdown menu with 'onboard-re' and a green checkmark, a toggle switch for 'Onboard-Required' which is currently 'ON' (checked), and a 'Selected' section showing 'Onboard-Required' with a right-pointing arrow. At the bottom is a 'Select' button.

## ClearPass Policy Manager Configuration

### IdP Certificate

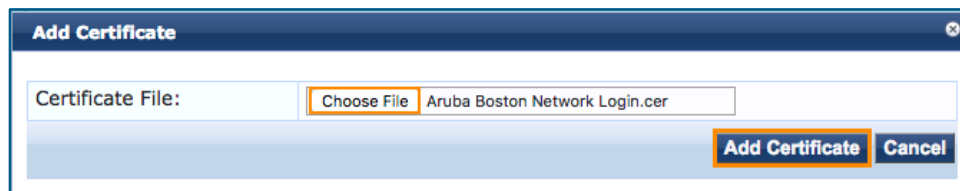
The first step in Policy Manager is to upload the identity provider certificate provided in the Azure portal.

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>*

<b>SAML SP Configuration</b>	<b>SAML IdP Configuration</b>
Identity Provider (IdP) URL: <a href="https://login.microsoftonline.com/406a990a-06b2-4a9e-">https://login.microsoftonline.com/406a990a-06b2-4a9e-</a>	

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

<b>Enable SSO for</b>	
Onboard	<input checked="" type="checkbox"/> Enable access to Onboard device provisioning portals
Insight	<input type="checkbox"/> Enable access to Insight application
PolicyManager	<input type="checkbox"/> Enable access to Policy Manager administration
Guest	<input type="checkbox"/> Enable Guest Web Login access for Guest and Onboard applications
GuestOperators	<input type="checkbox"/> Enable Guest Operator Login access for Guest and Onboard applications

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

<b>Identity Provider (IdP) Certificate</b>	
Select Certificate:	CN=Microsoft Azure Federated SSO Certificate
Subject DN:	CN=Microsoft Azure Federated SSO Certificate
Issuer DN:	CN=Microsoft Azure Federated SSO Certificate
Issue Date/Time:	Jun 15, 2017 14:45:08 EDT
Expiry Date/Time:	Jun 15, 2020 14:45:06 EDT
Validity Status:	Valid

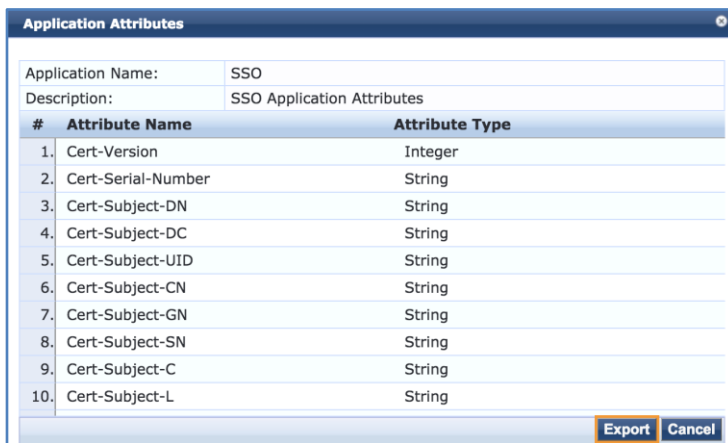
Click **Save** at the bottom.

## 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**.



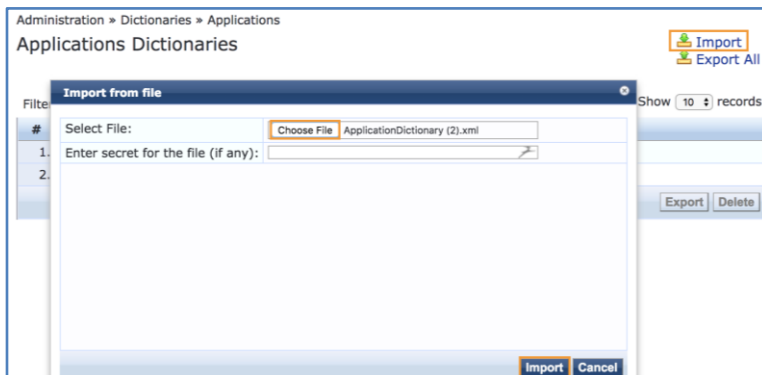
#	Attribute Name	Attribute Type
1.	Cert-Version	Integer
2.	Cert-Serial-Number	String
3.	Cert-Subject-DN	String
4.	Cert-Subject-DC	String
5.	Cert-Subject-UID	String
6.	Cert-Subject-CN	String
7.	Cert-Subject-GN	String
8.	Cert-Subject-SN	String
9.	Cert-Subject-C	String
10.	Cert-Subject-L	String

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.

```
<App1DictionaryAttributes 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**.

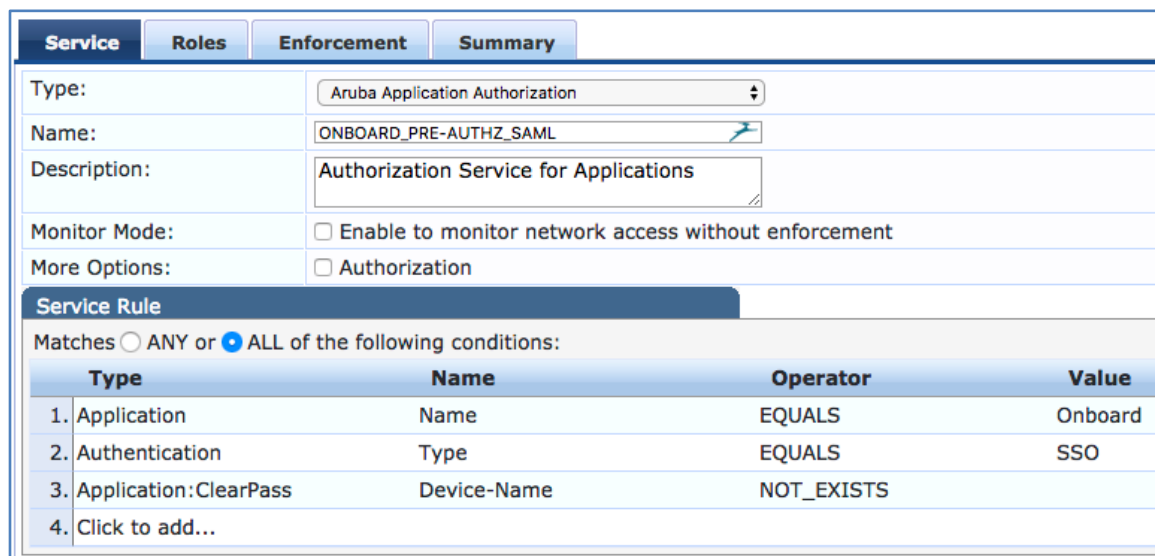


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD\_PRE-AUTHZ\_SAML* for example.

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	



Type	Name	Operator	Value
1. Application	Name	EQUALS	Onboard
2. Authentication	Type	EQUALS	SSO
3. Application:ClearPass	Device-Name	NOT_EXISTS	
4. Click to add...			

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

The screenshot shows the 'Enforcement' tab selected. It contains a 'Use Cached Results' checkbox (unchecked) and a 'Use cached Roles and Posture attributes from previous sessions' checkbox (checked). Below this is an 'Enforcement Policy' dropdown menu showing '[Guest Operator Logins]' with a 'Modify' button next to it. To the right is a button labeled 'Add new Enforcement Policy'.

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

The screenshot shows the 'Enforcement Policies' page with the 'Enforcement' tab selected. The 'Name' field is 'ONBOARD\_PRE-AUTHZ\_SAML'. The 'Description' field is empty. The 'Enforcement Type' has radio buttons for 'RADIUS', 'TACACS+', 'WEBAUTH (SNMP/Agent/CLI/CoA)', 'Application' (selected), and 'Event'. The 'Default Profile' dropdown is set to '[Deny Application Access Profile]'. There are 'View Details' and 'Modify' buttons, and a link to 'Add new Enforcement Policy'.

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**.

The screenshot shows the 'Rules Editor' window. Under the 'Conditions' section, there is a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row has 'Tips' in the Type column, 'Role' in the Name column, 'EQUALS' in the Operator column, and '[User Authenticated]' in the Value column. Below this is a section for 'Enforcement Profiles' with a list of profile names. '[Allow Application Access Profile]' is selected. There are 'Move Up', 'Move Down', and 'Remove' buttons. At the bottom right are 'Save' and 'Cancel' buttons.

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.

Enforcement Policies

Enforcement

Rules

Summary

Rules Evaluation Algorithm: ☒ Select first match ☐ Select all matches

Enforcement Policy Rules:

Conditions	Actions
1. (Application:SSO:Department EQUALS Management)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M
2. (Tips:Role EQUALS [User Authenticated])	[Allow Application Access Profile]

Add Rule

Move Up

Move Down

Edit Rule

Remove Rule

Back to Services

Next >

Save

Cancel

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

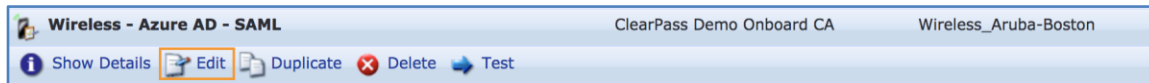
Modify

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.

Authorization	
These options control how a device is authorized during provisioning.	
* Authorization Method:	App Authentication — check using Aruba Application Authentication  <small>Select the method used to authorize devices.</small>
Use SSO:	<input checked="" type="checkbox"/> Single Sign-On – Enable SSO for device provisioning <small>If enabled then users will be required to authenticate via SSO</small>
* Configuration Profile:	Wireless_Aruba-Boston  <small>Select the configuration profile that will be provisioned to devices.</small>
* Maximum Devices:	0 <small>The maximum number of devices that a user may provision. Use 0 for unlimited.</small>

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](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**

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

**Request Details**

SummaryInputOutput

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.com/claims/authnmethodsreferences
Application:SSO:http://schemas.microsoft.com/identity/claims/displayname	Darth Vader
Application:SSO:http://schemas.microsoft.com/identity/claims/identityprovider	https://sts.windows.net/406a990a-06b2-4a9e-b0c0-ef301964-6060-466b-bcc0-406a990a-06b2-4a9e-b0c0
Application:SSO:http://schemas.microsoft.com/identity/claims/objectidentifier	ef301964-6060-466b-bcc0-406a990a-06b2-4a9e-b0c0
Application:SSO:http://schemas.microsoft.com/identity/claims/tenantid	406a990a-06b2-4a9e-b0c0-ef301964-6060-466b-bcc0
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	darth.vader@arubaboston.com
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.com
Application:SSO:http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Vader
Application:SSO:Title	Supreme Commander of the Galactic Empire
Authentication:Full-Username	darth.vader@arubaboston.com
Authentication:Full-Username-Normalized	darth.vader@arubaboston.com

Showing 1 of 1-10 records

Change StatusShow ConfigurationExportShow LogsClose

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

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

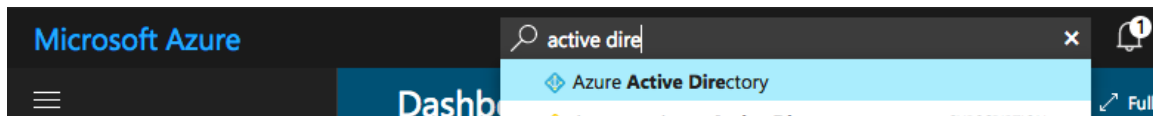
## OAuth 2.0

### Azure Active Directory Configuration

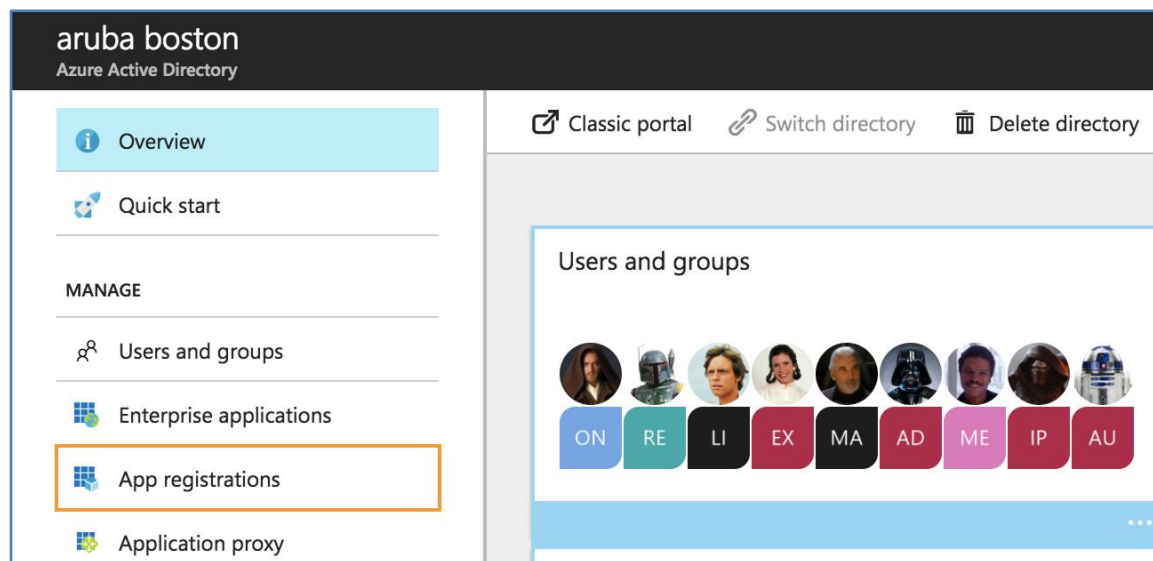
#### Application Setup

Log into the Microsoft Azure Portal at [portal.azure.com](https://portal.azure.com). Depending on the Azure IAM policy, you may need to log in as a Global Administrator.

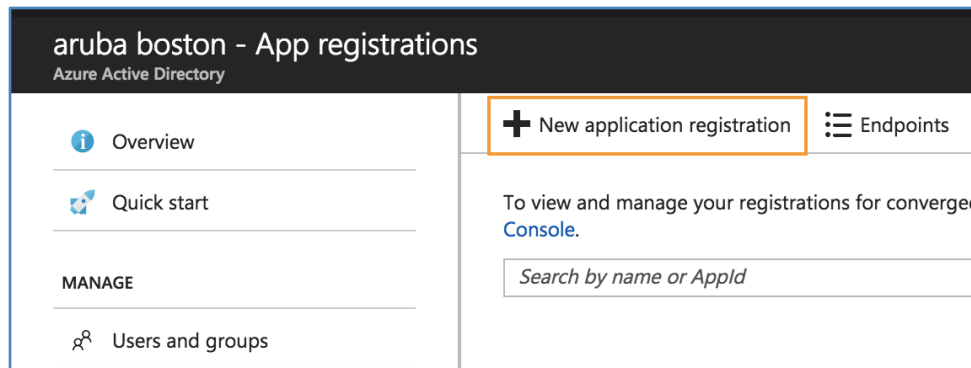
Using the search bar at the top, search for and select **Azure Active Directory**.



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**

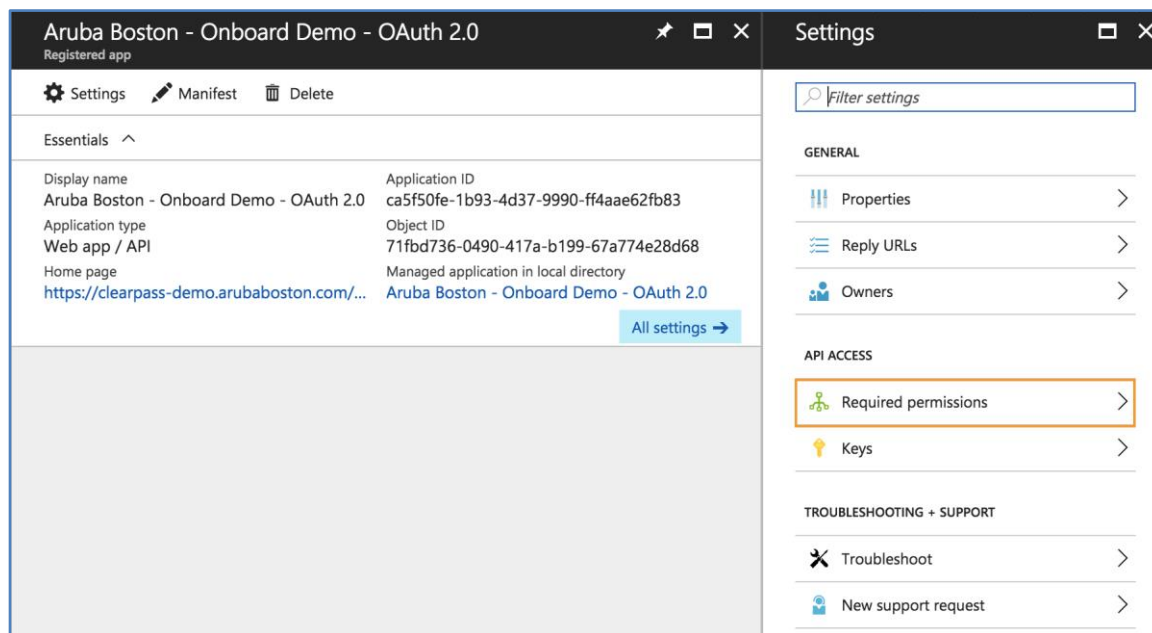
Click **Create** when done.

The screenshot shows a 'Create' dialog box with a dark header and window controls. It contains three main input fields: 'Name' with the value 'Aruba Boston - Onboard Demo - OAuth 2.0', 'Application type' set to 'Web app / API', and 'Sign-on URL' with the value 'https://clearpass-demo.arubaboston.com/...'. The 'Name' and 'Sign-on URL' fields are highlighted with orange borders and each has a green checkmark icon to its right. At the bottom left of the dialog is a blue 'Create' button.

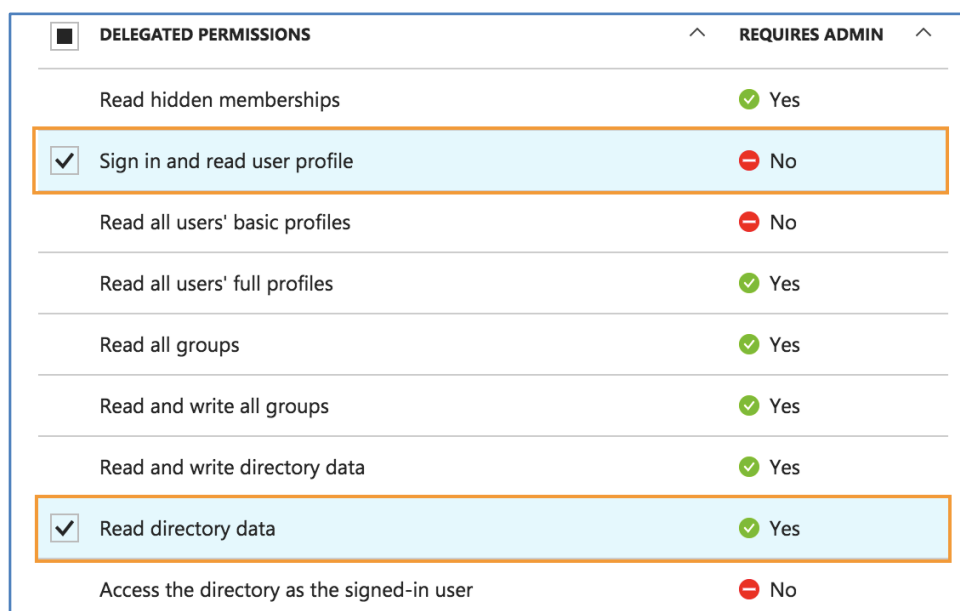
The page will redirect back to the application list. A refresh may be required if the newly created app does not appear.

Click the newly created app to access the configuration.

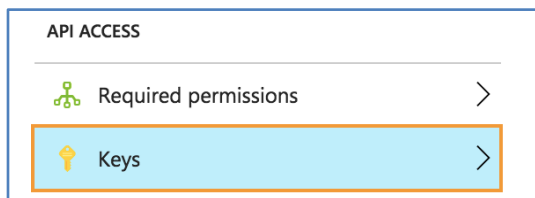
In the Settings blade under API access, click **Required permissions** and then choose **Windows Azure Active Directory**.



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.

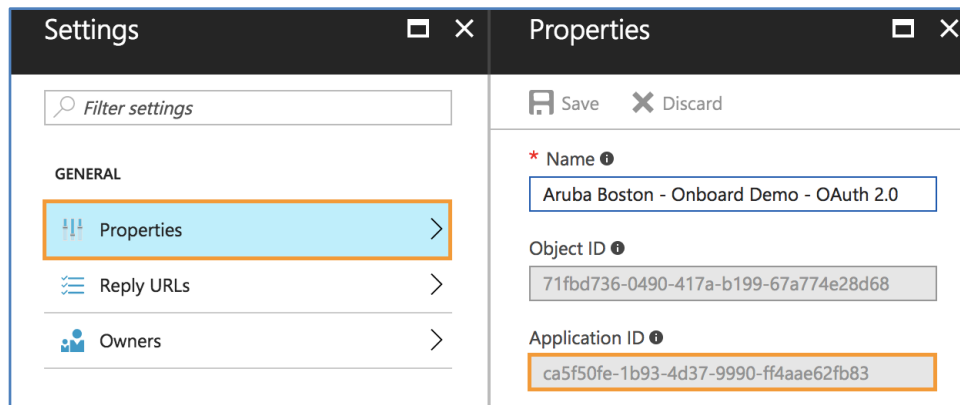
Click **Save** at the top and the key will be generated.

A screenshot of the key configuration form. At the top, there are 'Save' and 'Discard' buttons. Below is a table with three columns: 'DESCRIPTION', 'EXPIRES', and 'VALUE'. The 'DESCRIPTION' column contains 'ClearPass Boston'. The 'EXPIRES' column contains a dropdown menu set to 'In 1 year'. The 'VALUE' column contains a text box with the placeholder 'Value will be displayed on save' and a right-pointing chevron.

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.

A screenshot of the 'Keys' pane. At the top, there are 'Save' and 'Discard' buttons. Below is a yellow warning banner that says 'Copy the key value. You won't be able to retrieve after you leave this blade.' Below the banner is a table with three columns: 'DESCRIPTION', 'EXPIRES', and 'VALUE'. The 'DESCRIPTION' column contains 'ClearPass Boston'. The 'EXPIRES' column contains '7/3/2018'. The 'VALUE' column contains a text box with the generated key 'Yakgb14Q...' and a right-pointing chevron. The text box is highlighted with an orange border.

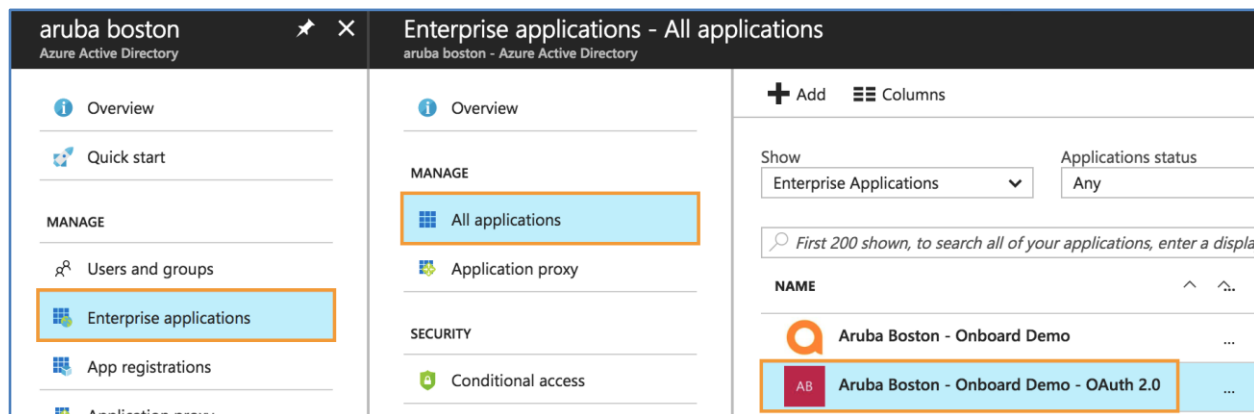
Close the **Keys** pane and then click **Properties**. Copy the **Application ID** and store it. This will be required to configure ClearPass along with the key from the previous step.



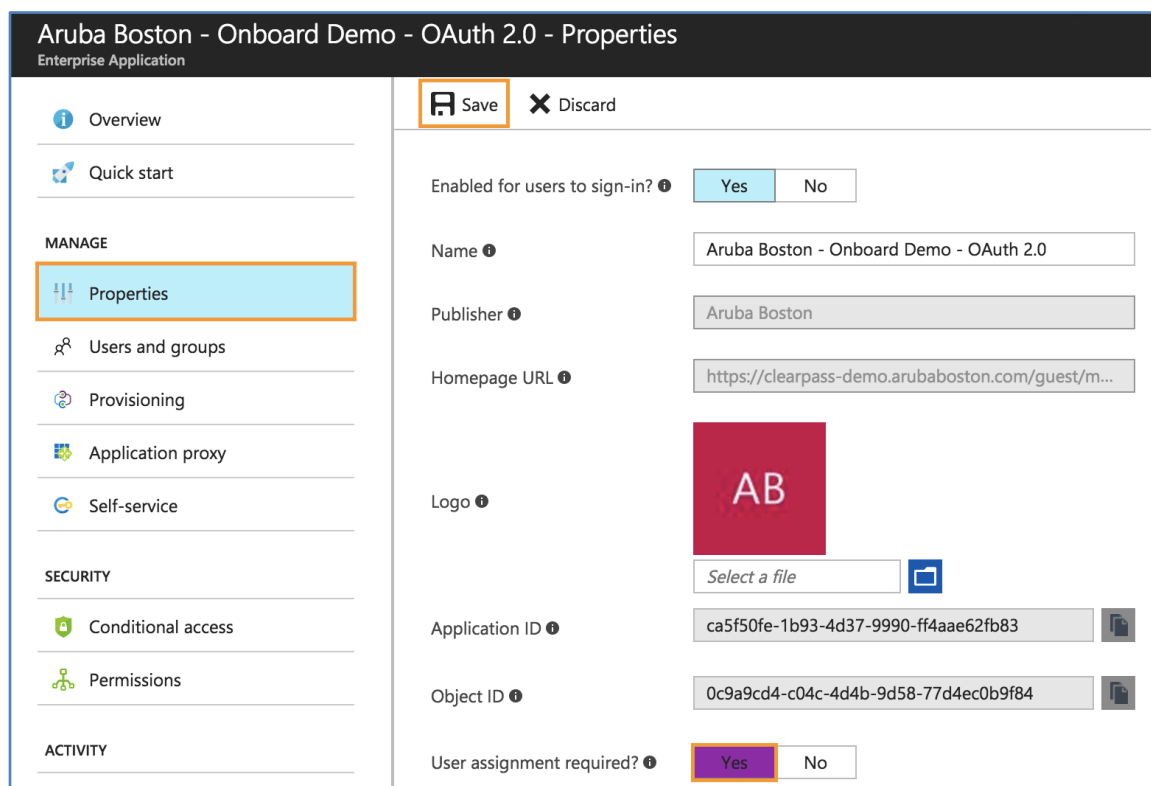
## Restricting Access

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.

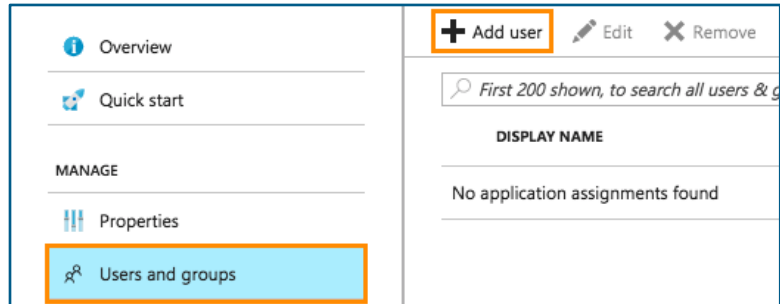
If there is a need to restrict access by group or user at the Azure Active Directory level, navigate back to the top-level Azure Active Directory blade, click **Enterprise applications**, **All applications** and then select the app created in the previous steps.



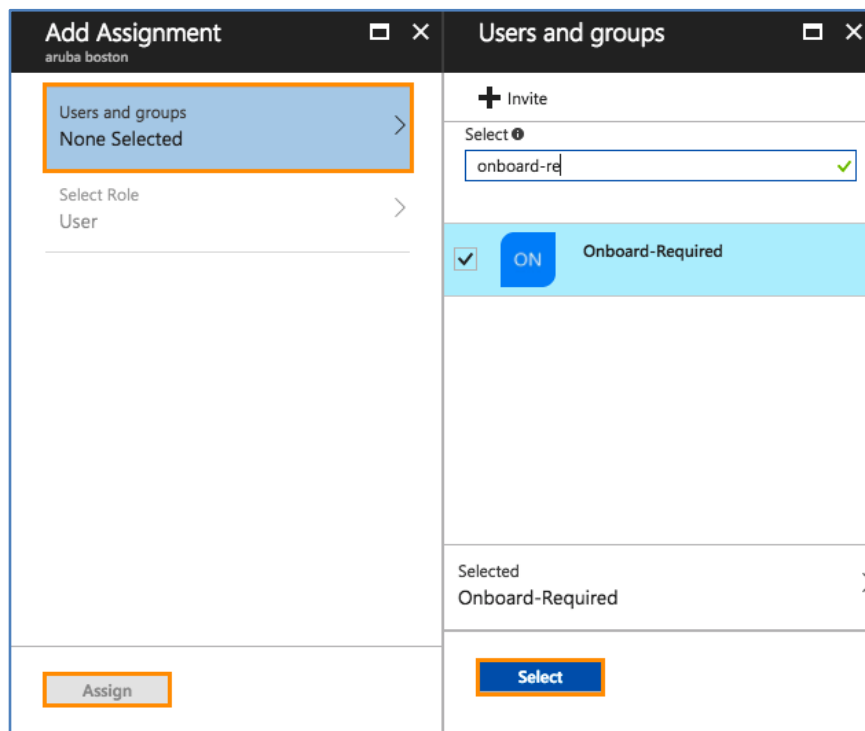
Click **Properties** and then change **User assignment required** to **Yes**, then click **Save** at the top.



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**.

Social Logins					
Optionally present guests with various social login options.					
Social Login:	<input checked="" type="checkbox"/> Enable login with social network credentials				
Authentication Providers:	<div><div> Add new authentication provider</div><table border="1"><thead><tr><th>Provider</th><th>Client ID</th></tr></thead><tbody><tr><td colspan="2"> There are no authentication providers defined.</td></tr></tbody></table></div>	Provider	Client ID	 There are no authentication providers defined.	
Provider	Client ID				
 There are no authentication providers defined.					

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:	<input checked="" type="checkbox"/> 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:	<input checked="" type="checkbox"/> Show advanced properties
Destination:	<input type="text"/> Guests authenticating with this provider will be redirected to this URL after login.
Auto Redirect:	<input checked="" type="checkbox"/> 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:	<input type="text"/> Prepend this text to all keys when flattening. If blank, 'social' is used.
Username Prefix:	<input type="text"/> 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:	<input type="text"/> Append this text to all usernames.
Icon Label:	<input type="text"/> Override the default label on this provider's icon.
Hostname:	<input type="text"/> If specified, use this hostname when redirecting the user to authenticate. This is optional – leave blank if unsure.
Notes:	<input type="text"/> 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:	<input checked="" type="checkbox"/> 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:	<input checked="" type="checkbox"/> 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
<b>Policy:</b>			
Policy Name:		AZURE-AD_OAUTH2	
Description:			
Default Role:		[Other]	
<b>Mapping Rules:</b>			
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](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	 <small>(with Google Secure LDAP connector)</small>	 <small>(with Google Secure LDAP connector)</small>
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	 <small>(with Google Secure LDAP connector)</small>	 <small>(with Google Secure LDAP connector)</small>

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

User Entity Return Attributes	
SAML	OAuth 2.0
address title department costcenter	groups group emails given name 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

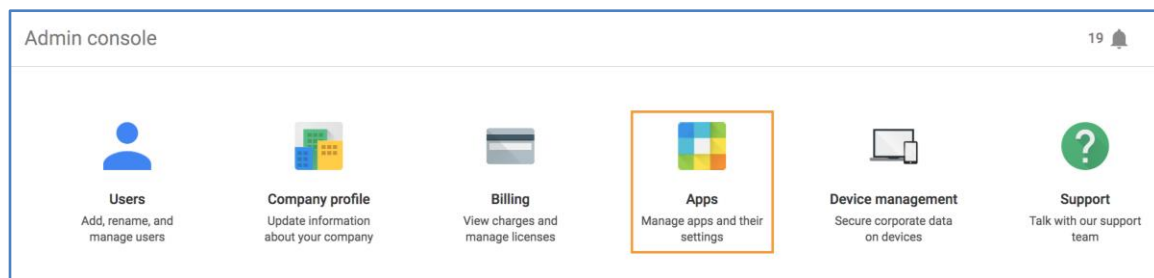
## Google Secure LDAP Connector

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.

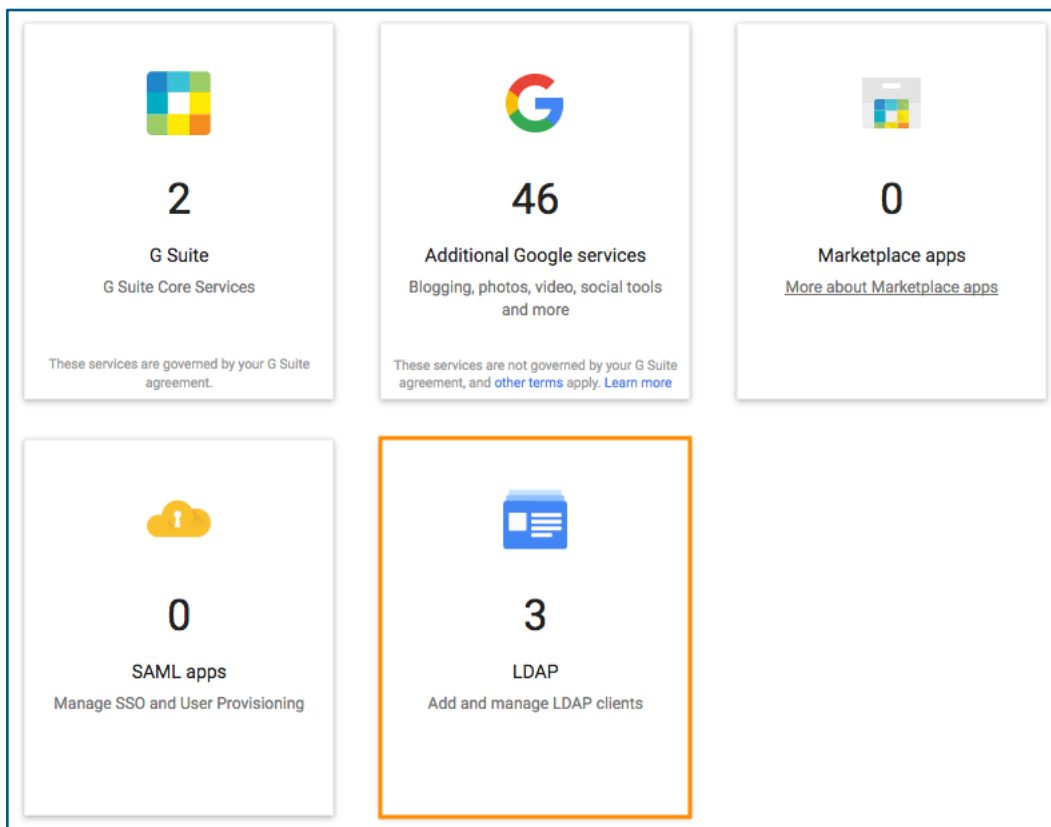
This connector uses the ClearPass Extensions framework. The Google Secure LDAP service is available to Cloud Premium, G Suite Enterprise, and all G Suite for Education organizations.

### Google Admin Console Configuration

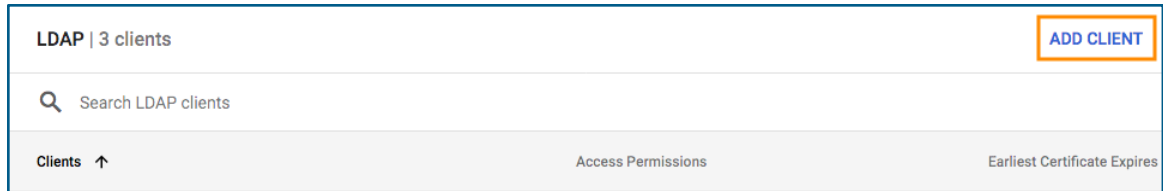
Log into the Google Admin portal at [admin.google.com](https://admin.google.com) with an account with admin privileges for the organization. At the main admin landing page, click the **Apps** icon.



Choose **LDAP** from the list.

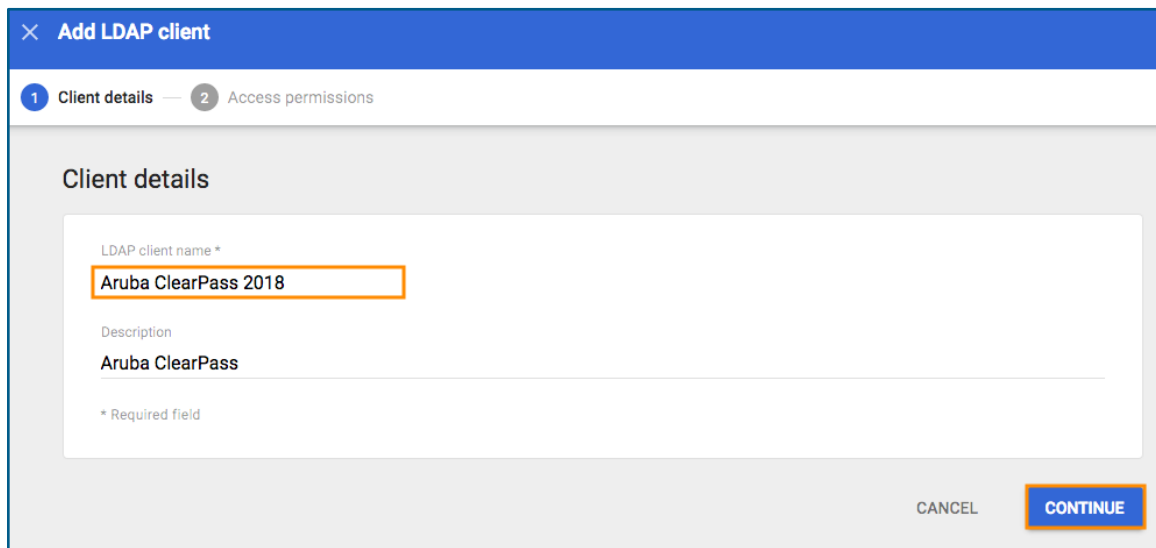


Click **ADD CLIENT**.



The screenshot shows a web interface for managing LDAP clients. At the top, it says "LDAP | 3 clients" on the left and an "ADD CLIENT" button on the right. Below this is a search bar with a magnifying glass icon and the text "Search LDAP clients". At the bottom, there is a table with three columns: "Clients" with an upward arrow, "Access Permissions", and "Earliest Certificate Expires".

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



The screenshot shows a "Add LDAP client" dialog box. It has a blue header with a close button (X) and the title "Add LDAP client". Below the header, there are two tabs: "1 Client details" (active) and "2 Access permissions". The "Client details" section contains a form with two fields: "LDAP client name \*" and "Description". The "LDAP client name \*" field is highlighted with an orange border and contains the text "Aruba ClearPass 2018". The "Description" field contains the text "Aruba ClearPass". Below the fields, there is a small asterisk and the text "\* Required field". At the bottom right of the dialog, there are two buttons: "CANCEL" and "CONTINUE" (highlighted with an orange border).

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.

**Add LDAP client**

Client details — 2 Access permissions

### Access permissions

**Verify user credentials**  
Specify client's access level for verifying user credentials. Changes can take up to 24 hours to take effect. ?

☒ Entire domain (clearpass.boston)

☐ Selected organizational units

☐ No access

**Read user information**  
Specify client's access level for reading user information. Some clients need additional information before authenticating users. ?

☒ Entire domain (clearpass.boston)

☐ Selected organizational units

☐ No access

**Read group information**  
Client can read group information. Some clients need additional information before authenticating users. ?

☒ On

BACK ADD LDAP CLIENT

**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**.

✓ Aruba ClearPass 2018 added

i

Next, connect your client to the LDAP service

1. Download the generated certificate (it might take a few minutes to generate).

Want to do this later? You can generate and download a certificate at any time from the client's details page.

Google\_2021\_11\_04\_74127

Expires: November 4, 2021

[Download certificate](#)

2. Upload the certificate to your LDAP client and configure the application. Configuration might require LDAP access credentials. [Learn more](#)

[CONTINUE TO CLIENT DETAILS](#)

Click **Authentication** to open the widget.

Aruba ClearPass 2018

Aruba ClearPass

Status

OFF

EDIT DETAILS

MORE

Service status

OFF

Access permissions

Verify user credentials

Read user information

Read group information

Entire domain

Entire domain

Has access

Authentication

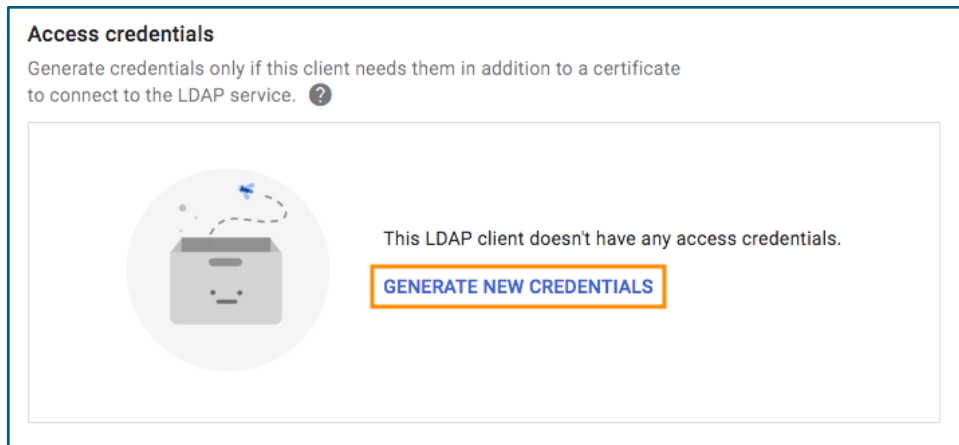
Certificates

1 certificate is associated with this LDAP client

Access credentials

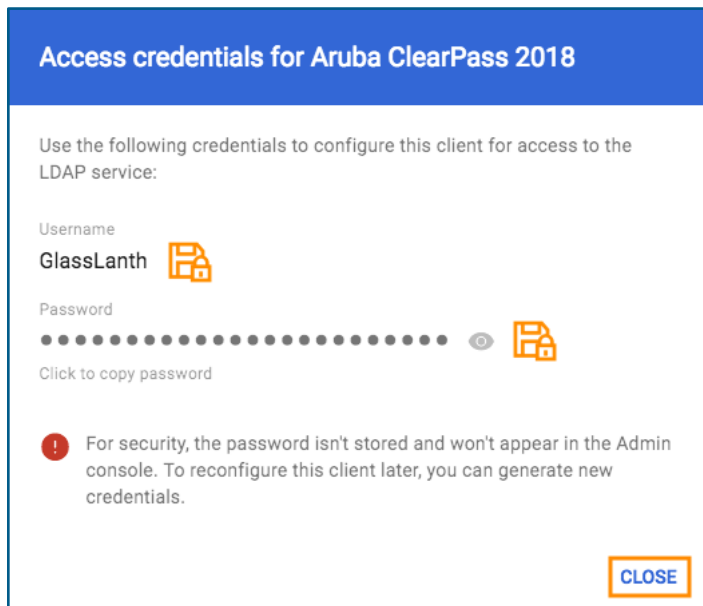
0 access credentials are associated with this LDAP client

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



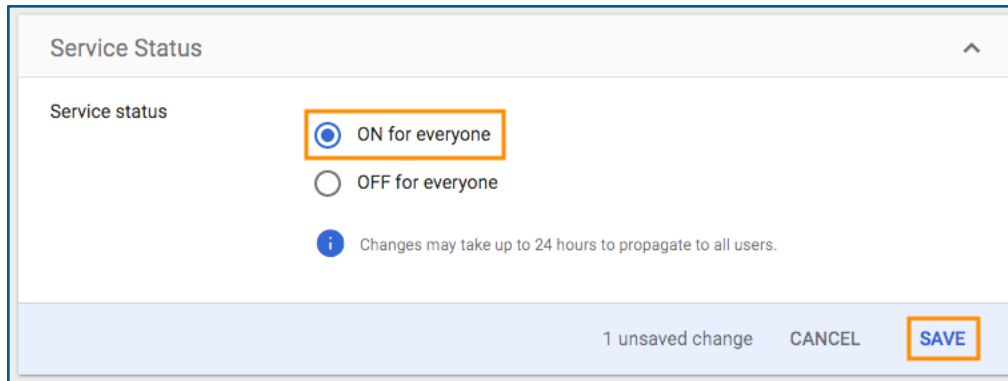
Securely store a copy of the generated credentials. They will be required to configure ClearPass.

Click **Close** when finished.



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

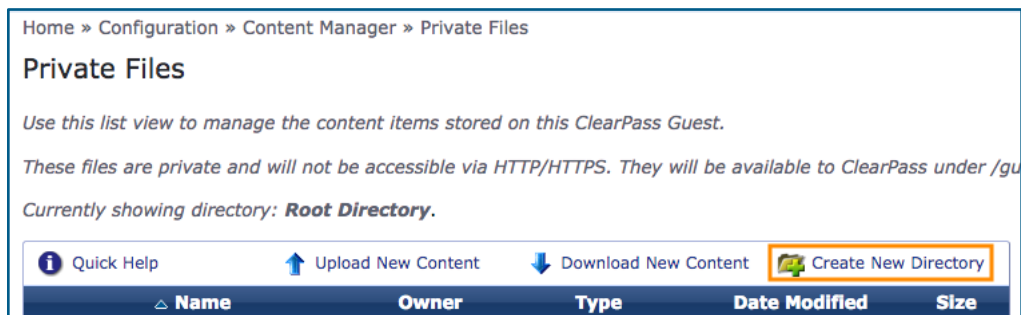
Lastly, click the **Service status** widget and choose **ON for everyone** and click **SAVE**.



The image shows a 'Service Status' configuration window. It has a title bar with 'Service Status' and a close button. The main area is titled 'Service status' and contains two radio buttons: 'ON for everyone' (selected) and 'OFF for everyone'. Below the radio buttons is an information icon and a note: 'Changes may take up to 24 hours to propagate to all users.' At the bottom right, there is a '1 unsaved change' indicator, a 'CANCEL' button, and a 'SAVE' button.

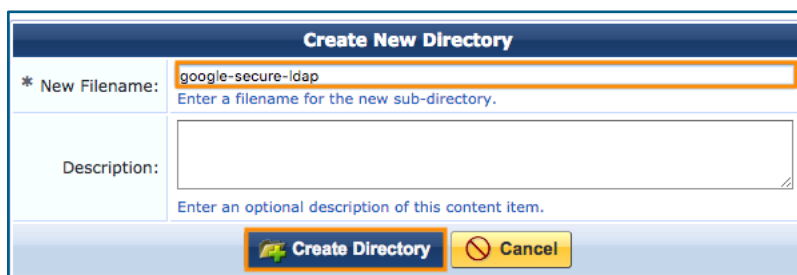
## ClearPass Extension Configuration

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



The image shows the 'Private Files' configuration page in ClearPass. The breadcrumb trail is 'Home » Configuration » Content Manager » Private Files'. The page title is 'Private Files'. Below the title is a description: 'Use this list view to manage the content items stored on this ClearPass Guest. These files are private and will not be accessible via HTTP/HTTPS. They will be available to ClearPass under /gu'. Below this is a note: 'Currently showing directory: **Root Directory**.' At the bottom, there is a navigation bar with buttons: 'Quick Help', 'Upload New Content', 'Download New Content', and 'Create New Directory' (highlighted with an orange box). Below the navigation bar is a table header with columns: 'Name', 'Owner', 'Type', 'Date Modified', and 'Size'.

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



The image shows the 'Create New Directory' dialog box. It has a title bar with 'Create New Directory'. The main area has two fields: '\* New Filename:' with the value 'google-secure-ldap' (highlighted with an orange box) and a description field. Below the fields is a 'Create Directory' button (highlighted with an orange box) and a 'Cancel' button.

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.

Quick Help **Upload New Content** Download New Content Create New Directory

Complete the form below to upload a new content item using your web browser.

**Add Content**

Size Limit: Maximum file upload size: 15.0 MB.

\* File: **Choose File** Google\_2021\_11\_04\_74127.crt  
Choose a file to upload from your computer.

Description:   
Enter an optional description of this content item.

Overwrite: ☒ Replace existing item with same name  
Select this option to overwrite an existing content item that has the same name.

**Upload Content** Cancel

\* required field

Name	Owner	Type	Date Modified	Size
0 items  Reload				

Show all rows

Currently showing directory: Root Directory > **google-secure-ldap.**

Quick Help **Upload New Content** Download New Content Create New Directory

Name	Owner	Type	Date Modified	Size
<b>Google_2021_11_04_74127.crt</b>	admin	application/octet-stream	2018-11-05 16:33	1.2 KB
<b>Google_2021_11_04_74127.key</b>	admin	application/octet-stream	2018-11-05 16:33	1.7 KB

2 items Reload

Show all rows

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

Home » Administration » Extensions

**Manage Extensions** **Install extension**

The extensions currently installed on this system are listed below.

Filter:

Name	Version	State	Hostname	IP Address
------	---------	-------	----------	------------

Search for **Google Secure LDAP Connector**.

Click **Install**.

The screenshot shows the 'Install Extension' interface. At the top, there is a search bar with the text '280008e1-64aa-4899-a547-19840bbabad0'. Below the search bar, a table displays the search results. The table has three columns: 'Name', 'Version', and 'State'. The first row shows the 'Google Secure LDAP Connector' with version '1.0.0' and state 'Not installed'. To the left of the table, there is a 'Results:' label and a small icon of the Google Secure LDAP Connector. Below the table, there is an 'Install' button with a green checkmark icon. At the bottom of the interface, there is a 'Search' button.

Name	Version	State
Google Secure LDAP Connector	1.0.0	Not installed

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.

The screenshot shows the 'Install Extension' configuration page for the 'Google Secure LDAP Connector'. The page is divided into several sections. The 'Extension' section shows the connector's name and logo. The 'Extension Settings' section includes a 'Start' checkbox labeled 'Start the extension after installation', which is checked. Below this is an 'IP Address' field with the value '172.17.0.90'. The 'Content Items Required' section includes two dropdown menus: one for 'certificate' and one for 'privateKey'. Both dropdowns are set to 'google-secure-ldap/Google\_2021\_11\_04\_74127.crt' and 'google-secure-ldap/Google\_2021\_11\_04\_74127.key' respectively. At the bottom of the page, there is an 'Install' button with a green checkmark icon.

Extension: Google Secure LDAP Connector

Extension Settings

Start: ☒ Start the extension after installation

IP Address: 172.17.0.90

Content Items Required

\* certificate: google-secure-ldap/Google\_2021\_11\_04\_74127.crt

\* privateKey: google-secure-ldap/Google\_2021\_11\_04\_74127.key

Install

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**.

Configuration » Authentication » Sources

Authentication Sources

An authentication source is the identity store (Active Directory, LDAP directory, etc.) against which users and devices are authenticated.

Add

Import

Export All

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

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

Configuration » Authentication » Sources » Add

Authentication Sources

General

Primary

Attributes

Summary

Name:	<div>Google LDAP</div>
Description:	<div></div>
Type:	<div>Generic LDAP</div>
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes

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.

Authentication Sources - Google LDAP			
Summary	General	Primary	Attributes
Connection Details			
Hostname:	172.17.0.90		
Connection Security:	None		
Port:	1636		
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection		
Bind DN:	CN=GlassLanth		
Bind Password:	.....		
Base DN:	dc=clearpass,dc=boston		Search Base Dn
Search Scope:	SubTree Search		
LDAP Referrals:	<input type="checkbox"/> Follow referrals		

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

Authentication Sources - Google LDAP			
Summary	General	Primary	Attributes
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	
1. Authentication	dn	UserDN	
2. Group	cn	Groups	

Replace the **Filter Query** with:

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

**Configure Filter**

Paging Control on the LDAP server is disabled. You will see a limited hierarchy.

**Configuration** | Attributes | Browse | Filter

Filter Name: Authentication

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

	Name	Alias Name	Data type	Enabled As
1.	dn	UserDN	String	-
2.	Click to add...			

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.

Type: EAP-TLS

**Method Details**

Session Resumption: ☐ Enable

Session Timeout: 6 hours

Authorization Required: ☒ Enable

Certificate Comparison: Compare CN or SAN

Verify Certificate using OCSP: Required

Override OCSP URL from Client: ☐ Enable

OCSP URL:

Save Cancel

## 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 <b>ENDS_WITH</b> ou=Staff,ou=Users,dc=clearpass,dc=boston)	USER_STAFF
2.	(Authorization:Google LDAP:UserDN <b>ENDS_WITH</b> ou=Faculty,ou=Users,dc=clearpass,dc=boston)	USER_FACULTY
3.	(Authorization:Google LDAP:Groups <b>EQUALS</b> employees)	USER_EMPLOYEE
4.	(Authorization:Google LDAP:Groups <b>EQUALS</b> 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	

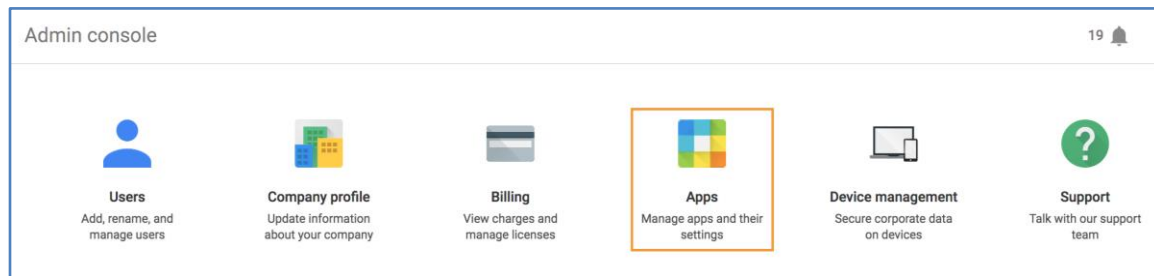
# SAML

## Google Admin Configuration

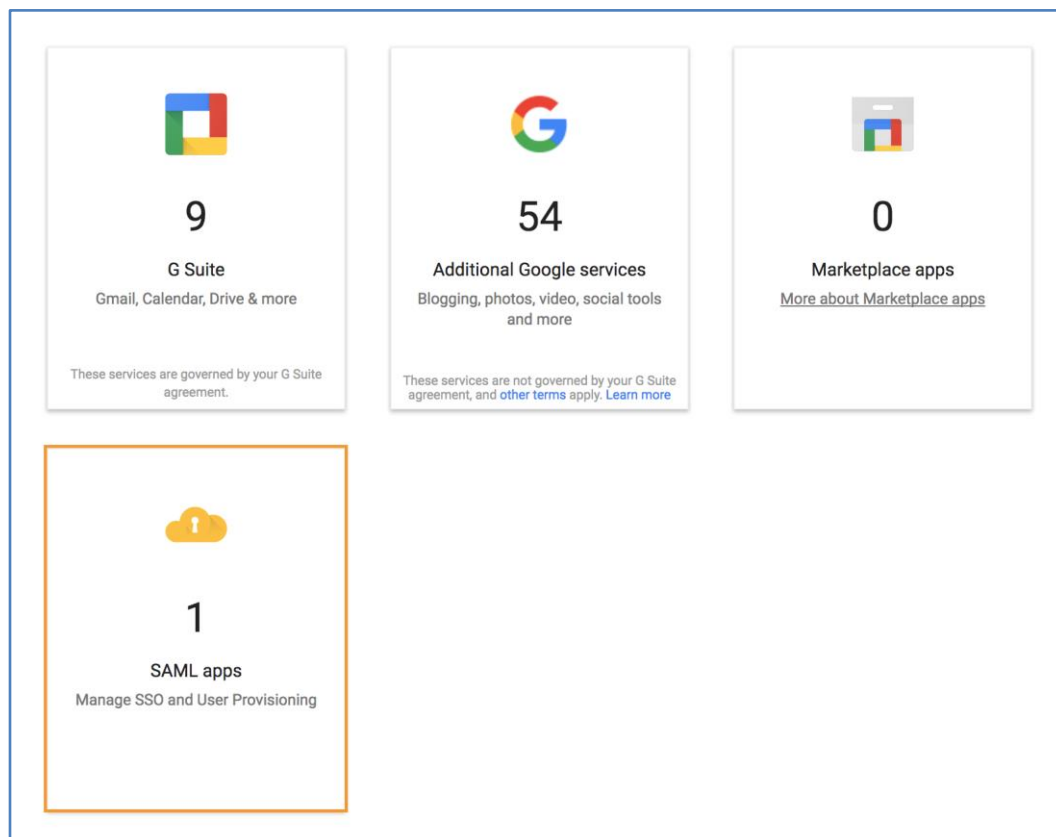
### Application Setup

Log into the Google Admin portal at [admin.google.com](https://admin.google.com) with an account with admin privileges for the organization.

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

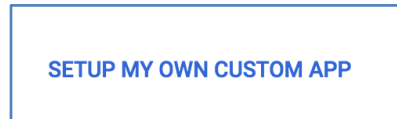


Choose **SAML apps** from the list.



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**.


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. [Learn more](#)

**Option 1**


SSO URL  <https://accounts.google.com/o/saml2/idp?idpid=C02qd8oxu>

Entity ID <https://accounts.google.com/o/saml2?idpid=C02qd8oxu>

Certificate  **DOWNLOAD** 

----- OR -----

**Option 2**

IDP metadata  **DOWNLOAD**

PREVIOUS

CANCEL **NEXT**

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

The screenshot shows a configuration window titled "Step 3 of 5" and "Basic information for your Custom App". It contains the following fields and elements:

- Application Name \***: A text input field containing "Aruba Boston - Onboard Demo". To its right, the text "app-id:" is displayed above the value "aruba\_boston\_-\_onboard\_demo".
- Description**: A text input field containing "ClearPass Onboard login".
- Upload logo**: A section with a "CHOOSE FILE" button. Below it, a file named "aruba-a\_500x500.jpg" is listed with a size of "64.9 KB".
- Footer**: Three buttons labeled "PREVIOUS", "CANCEL", and "NEXT". The "NEXT" button is highlighted with an orange border.

Below the file list, a note states: "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."

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 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 \*

Entity ID \*

Start URL

Signed Response ☒

Name ID Basic Information Primary Email

Name ID Format UNSPECIFIED

PREVIOUS CANCEL 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.

Step 5 of 5

### Attribute Mapping

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

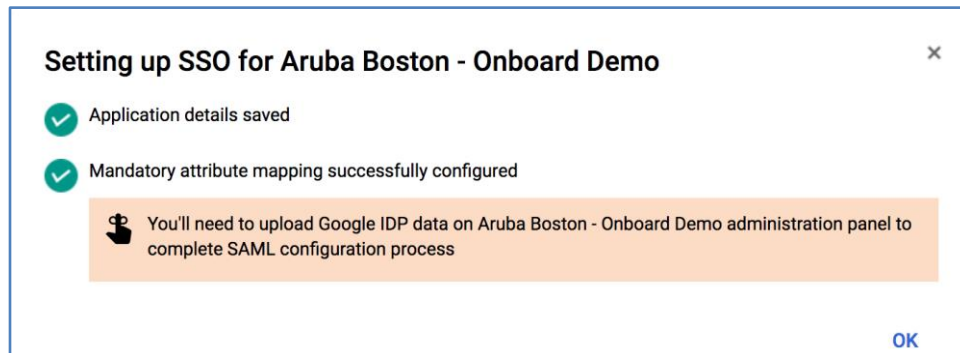
Title Employee Details Job Title

Department Employee Details Department

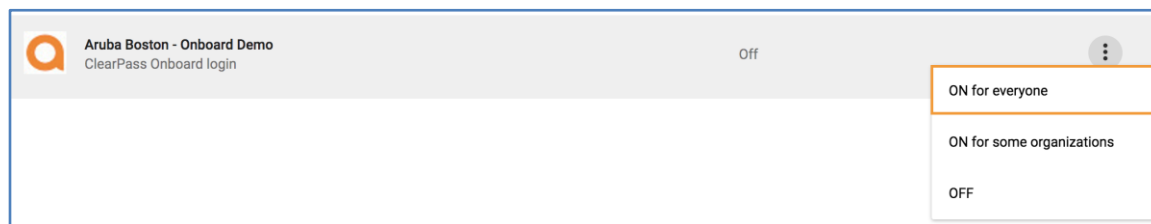
ADD NEW MAPPING

PREVIOUS CANCEL FINISH

Click **OK** on the summary screen.

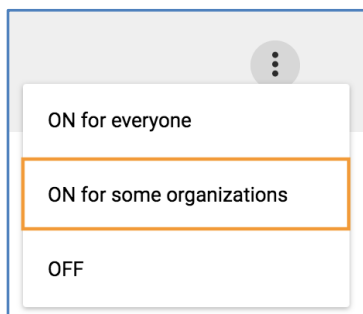


By default, the application will be turned off. In the SAML App list, click the triple dot menu for the app, and click **ON for everyone**. To restrict access to certain groups, see the next section.



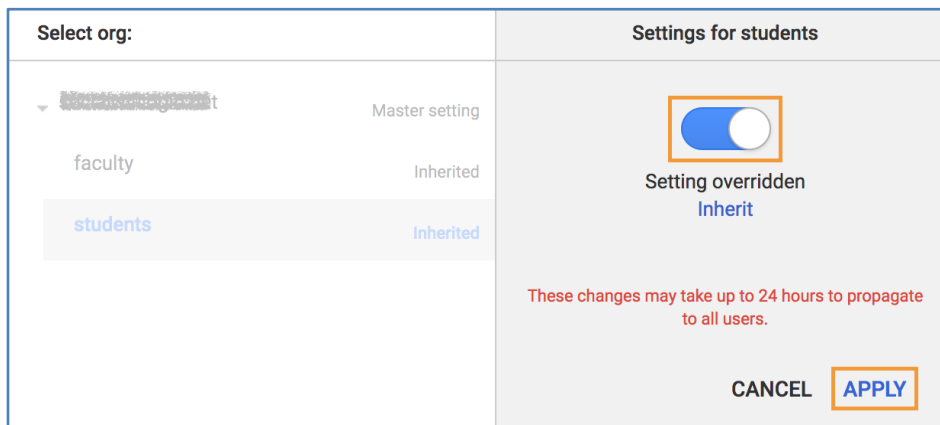
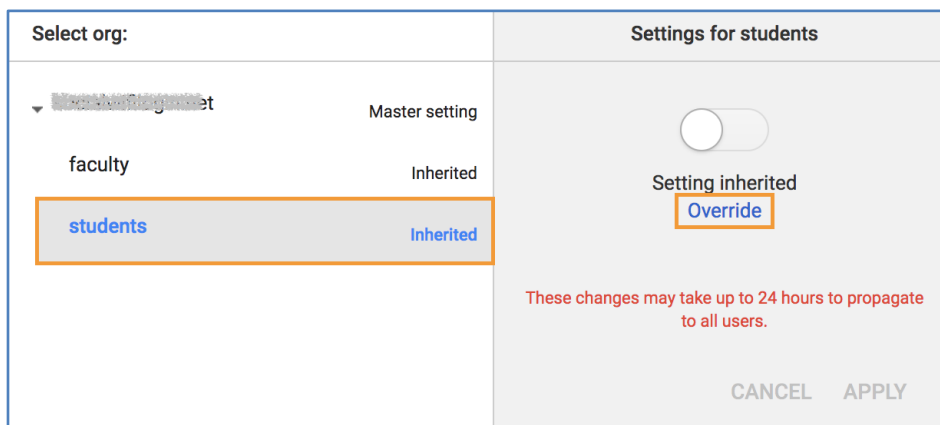
## Restricting Access

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

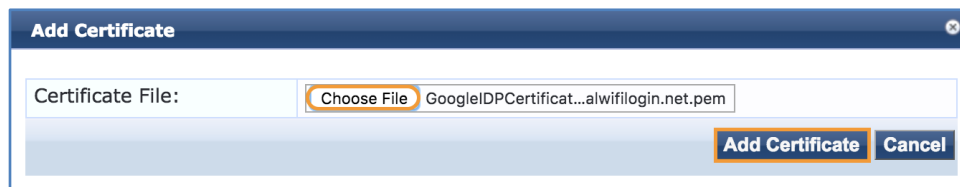
The first step in Policy Manager is to upload the identity provider certificate provided in the G Suite admin console.

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>>*

SAML SP Configuration	SAML IdP Configuration
Identity Provider (IdP) URL: <a href="https://accounts.google.com/o/saml2/idp?idpid=C02qd8">https://accounts.google.com/o/saml2/idp?idpid=C02qd8</a>	

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

Enable SSO for	
Onboard	<input checked="" type="checkbox"/> Enable access to Onboard device provisioning portals
Insight	<input type="checkbox"/> Enable access to Insight application
PolicyManager	<input type="checkbox"/> Enable access to Policy Manager administration
Guest	<input type="checkbox"/> Enable Guest Web Login access for Guest and Onboard applications
GuestOperators	<input type="checkbox"/> Enable Guest Operator Login access for Guest and Onboard applications

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

Identity Provider (IdP) Certificate	
Select Certificate:	ST=California,C=US,OU=Google For Work,CN=Google
Subject DN:	ST=California,C=US,OU=Google For Work,CN=Google,L=Mountain View,O=Google Inc.
Issuer DN:	ST=California,C=US,OU=Google For Work,CN=Google,L=Mountain View,O=Google Inc.
Issue Date/Time:	May 31, 2017 10:24:28 EDT
Expiry Date/Time:	May 30, 2022 10:24:28 EDT
Validity Status:	Valid
Signature Algorithm:	SHA256WithRSAEncryption
Public Key Format:	X.509
Serial Number:	1496240672704
Enabled:	true
<b>Note:</b> IdP certificate must be enabled in Certificate Trust List first, if not listed above.	

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**.

#	Attribute Name	Attribute Type
1.	Cert-Version	Integer
2.	Cert-Serial-Number	String
3.	Cert-Subject-DN	String
4.	Cert-Subject-DC	String
5.	Cert-Subject-UID	String
6.	Cert-Subject-CN	String
7.	Cert-Subject-GN	String
8.	Cert-Subject-SN	String
9.	Cert-Subject-C	String
10.	Cert-Subject-L	String

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.

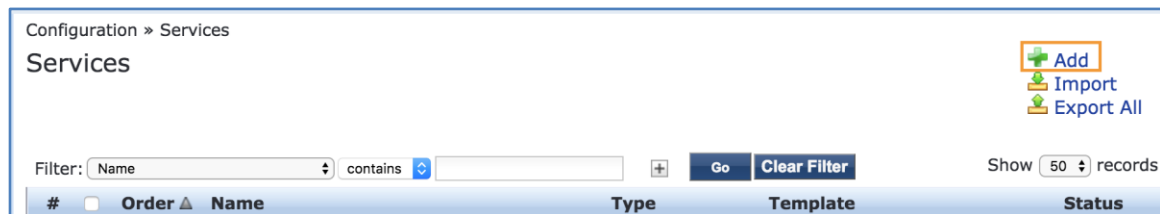
```
<ApplDictionaryAttributes attrType="String" attrName="Phone"/>
```

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**.

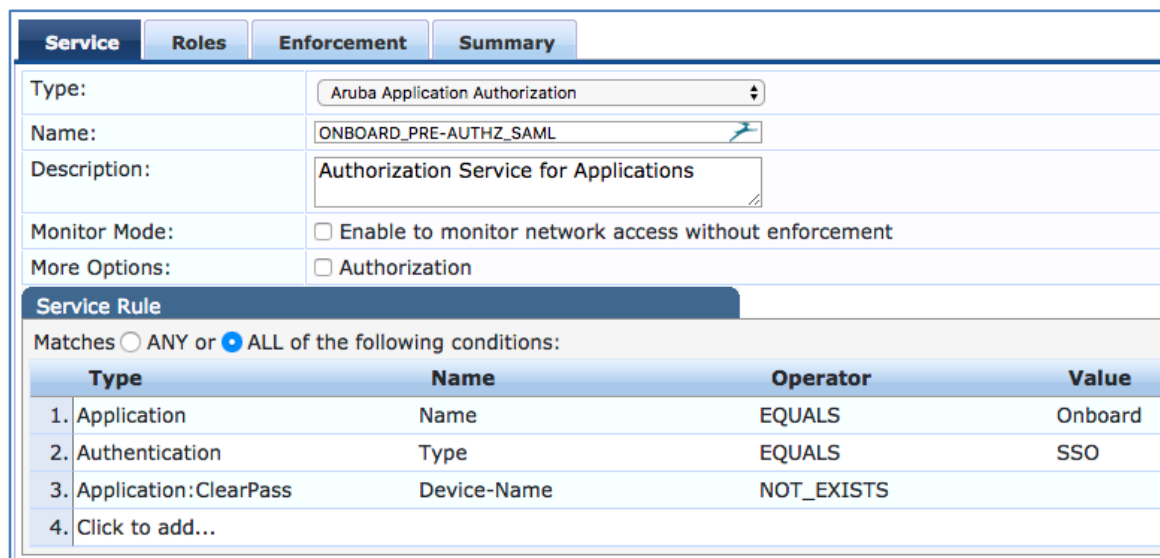


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD\_PRE-AUTHZ\_SAML* for example.

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	



Type	Name	Operator	Value
1. Application	Name	EQUALS	Onboard
2. Authentication	Type	EQUALS	SSO
3. Application:ClearPass	Device-Name	NOT_EXISTS	
4. Click to add...			

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

The screenshot shows the 'Enforcement' tab selected. It contains a 'Use Cached Results' checkbox (unchecked) and a 'Use cached Roles and Posture attributes from previous sessions' checkbox (checked). Below this is an 'Enforcement Policy' dropdown menu showing '[Guest Operator Logins]' with a 'Modify' button next to it. To the right is a button labeled 'Add new Enforcement Policy'.

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

The screenshot shows the 'Enforcement Policies' page with the 'Enforcement' tab selected. The 'Name' field is 'ONBOARD\_PRE-AUTHZ\_SAML'. The 'Description' field is empty. The 'Enforcement Type' has radio buttons for 'RADIUS', 'TACACS+', 'WEBAUTH (SNMP/Agent/CLI/CoA)', 'Application' (selected), and 'Event'. The 'Default Profile' dropdown is set to '[Deny Application Access Profile]'. There are 'View Details' and 'Modify' buttons, and a link to 'Add new Enforcement Policy'.

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.

The screenshot shows the 'Rules Editor' page. Under the 'Conditions' section, there is a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row has 'Tips' as Type, 'Role' as Name, 'EQUALS' as Operator, and '[User Authenticated]' as Value. Below this is a section for 'Enforcement Profiles' with a list of profile names. '[Allow Application Access Profile]' is selected. There are 'Move Up', 'Move Down', and 'Remove' buttons. At the bottom are 'Save' and 'Cancel' buttons.

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
<b>Policy:</b>		
Policy Name:	G-SUITE_SAML	
Description:		
Default Role:	[Other]	
<b>Mapping Rules:</b>		
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
<b>Enforcement:</b>		
Name:	ONBOARD_PRE-AUTHZ_SAML-GSUITE	
Description:		
Enforcement Type:	Application	
Default Profile:	[Deny Application Access Profile]	
<b>Rules:</b>		
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.

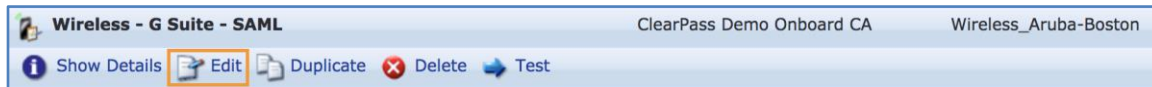
Summary	Service	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions		
Enforcement Policy:	ONBOARD_PRE-AUTHZ_SAML		<b>Modify</b>

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.

Authorization	
These options control how a device is authorized during provisioning.	
* Authorization Method:	App Authentication — check using Aruba Application Authentication  <a href="#">Select the method used to authorize devices.</a>
Use SSO:	<input checked="" type="checkbox"/> Single Sign-On – Enable SSO for device provisioning <a href="#">If enabled then users will be required to authenticate via SSO</a>
* Configuration Profile:	Wireless_Aruba-Boston  <a href="#">Select the configuration profile that will be provisioned to devices.</a>
* Maximum Devices:	0 <a href="#">The maximum number of devices that a user may provision. Use 0 for unlimited.</a>

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](https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_google.md)

## Sample Request

**Request Details**

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

**Request Details**

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

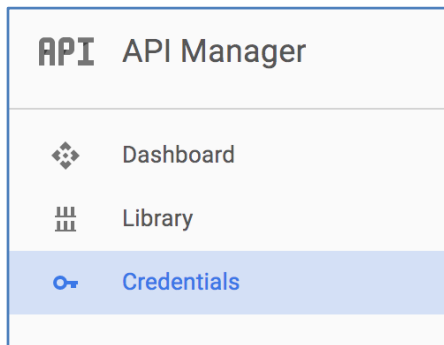
## OAuth 2.0

### Google Admin Console Configuration

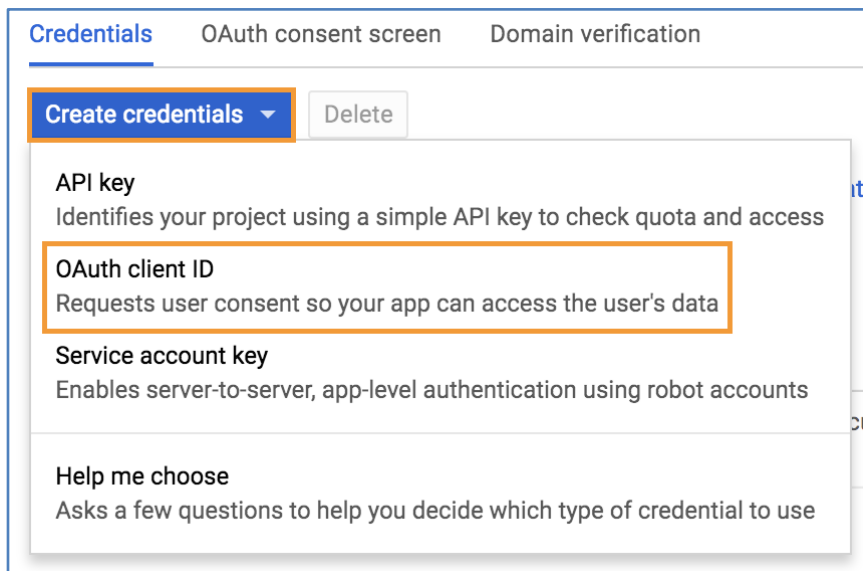
#### Application Setup

Log into the Google Developer Console at [console.developers.google.com](https://console.developers.google.com).

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

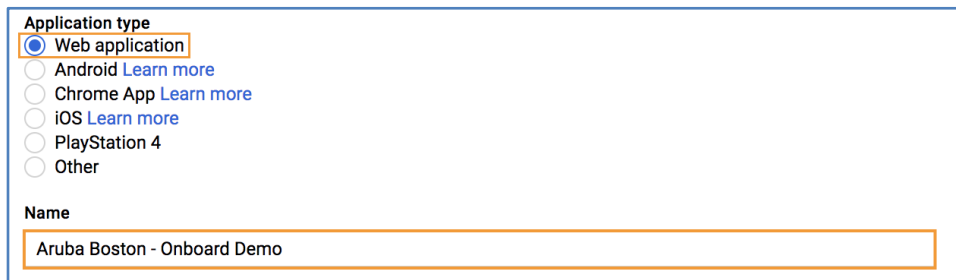


Click **Create credentials** and then **OAuth client ID**.



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.



**Application type**

- ☒ Web application
- ☐ Android [Learn more](#)
- ☐ Chrome App [Learn more](#)
- ☐ iOS [Learn more](#)
- ☐ PlayStation 4
- ☐ Other

**Name**

Aruba Boston - Onboard Demo

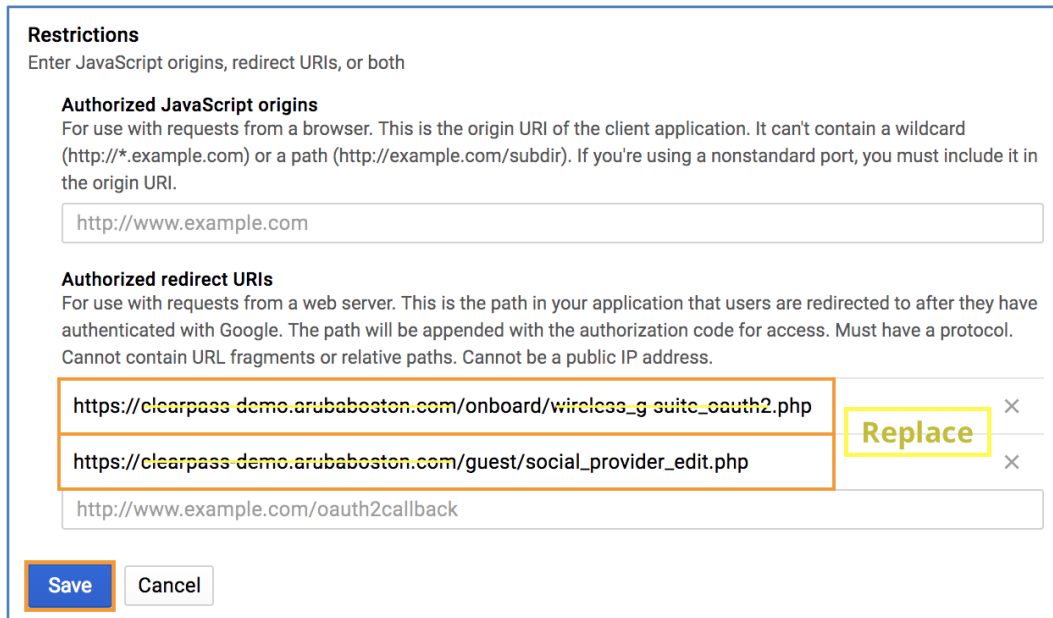
Down under **Restrictions** and then **Authorized redirect URIs**, enter the ClearPass FQDN with the planned Onboard page name (do not include any URL parameters after ".php" if present):

**`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.



**Restrictions**

Enter JavaScript origins, redirect URIs, or both

**Authorized JavaScript origins**

For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (`http://*.example.com`) or a path (`http://example.com/subdir`). If you're using a nonstandard port, you must include it in the origin URI.

`http://www.example.com`

**Authorized redirect URIs**

For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

`https://clearpass-demo.arubaboston.com/onboard/wireless_g_suite_oauth2.php` Replace ×

`https://clearpass-demo.arubaboston.com/guest/social_provider_edit.php` ×

`http://www.example.com/oauth2callback`

**Save** **Cancel**



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.

### OAuth client

Here is your client ID

.apps.googleusercontent.com

Here is your client secret



**OK**

## Google Developer Verification Override

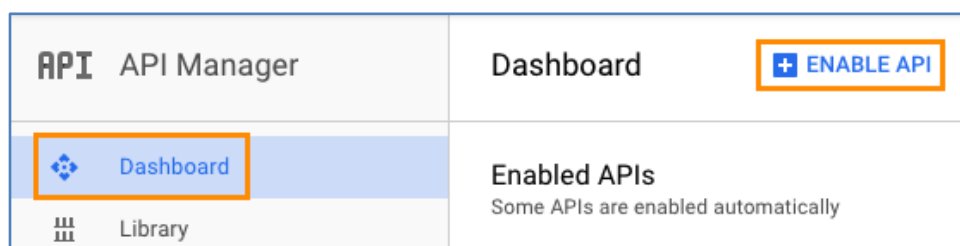
Google now requires that all OAuth web apps be verified. Because this is a custom configuration for each Cloud Identity or G Suite tenant, this web app must be enabled as an “Unreviewed” app.

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**.

Social Logins					
Optionally present guests with various social login options.					
Social Login:	<input checked="" type="checkbox"/> Enable login with social network credentials				
Authentication Providers:	<div> Add new authentication provider</div> <table border="1"><thead><tr><th>Provider</th><th>Client ID</th></tr></thead><tbody><tr><td colspan="2"> There are no authentication providers defined.</td></tr></tbody></table>	Provider	Client ID	 There are no authentication providers defined.	
Provider	Client ID				
 There are no authentication providers defined.					

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.


Properties	
* Provider:	Google Apps
Enabled:	<input checked="" type="checkbox"/> Use this provider
* Client ID:	<< CLIENT ID FROM GOOGLE ADMIN CONSOLE >> The Client ID associated to your provider. They may use a different label.
* Client Secret:	<< CLIENT ID FROM GOOGLE ADMIN CONSOLE >> The Client Secret associated to your provider. They may use a different label.
Advanced:	<input checked="" type="checkbox"/> Show advanced properties
Destination:	<input type="text"/> Guests authenticating with this provider will be redirected to this URL after login.
Auto Redirect:	<input checked="" type="checkbox"/> 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.


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.



Provider Specific Options	
VIP Attribute:	<input type="text" value="orgUnitPath"/> Enter the name of the user record attribute to apply to the "social_vip" flag. Refer to the Google Directory API for retrieving users.
Allow Guests:	<input type="checkbox"/> Allow Google accounts not part of your domain to log in as guests These guests will have the "social_vip" flag set to false.
Google Groups:	<input checked="" type="checkbox"/> <b>Retrieve the group memberships for the guest's account</b>
* Admin SDK Refresh Token:	<input type="text"/> Enter a valid Google API Admin Refresh Token. Clear the value to generate a new refresh token. You will need to generate a new authorization code.
Generate Code:	<b>Click to generate an authorization code</b> You will be redirected in a new window to generate an authorization code. When the code is generated, the code below will be filled in and you can close the window that was opened.


  
**Choose an account**  
to continue to [arubaboston.com](#)








 Use another account

  
Hi   
**arubaboston.com** wants to



View users on your domain 





View groups on your domain 

**Allow arubaboston.com to do this?**  
You may review this app's [terms of service](#) and [privacy policies](#). You can remove this or any other app connected to your account in [My Account](#)

CANCEL **ALLOW**

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

* Admin SDK Refresh Token:	<input type="text"/> Enter a valid Google API Admin Refresh Token. Clear the value to generate a new refresh token. You will need to generate a new authorization code.
Generate Code:	Click to generate an authorization code You will be redirected in a new window to generate an authorization code. When the code is generated, the code below will be filled in and you can close the window that was opened.
* Authorization Code:	<input type="text"/>
<div> <b>Add</b>  <b>Cancel</b></div>	

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.

Custom Form:	<input checked="" type="checkbox"/> Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
--------------	--

## 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](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.

### Role Mappings - G-SUITE

Summary

Policy

Mapping Rules

Rules Evaluation Algorithm: ☐ Select first match ☒ Select all matches

Role Mapping Rules:

	Conditions	Role Name
1.	<div>OR</div> <div>(Endpoint:social_orgUnitPath ENDS_WITH /students)</div> <div>(Endpoint:social_groups CONTAINS students)</div>	USER_STUDENT
2.	<div>OR</div> <div>(Endpoint:social_orgUnitPath ENDS_WITH /staff)</div> <div>(Endpoint:social_groups CONTAINS Staff)</div>	USER_STAFF
3.	<div>OR</div> <div>(Endpoint:social_orgUnitPath ENDS_WITH /staff/faculty)</div> <div>(Endpoint:social_groups CONTAINS Faculty)</div>	USER_FACULTY
4.	<div>(Endpoint:social_groups CONTAINS Certificate-Required)</div>	USER_CERT-REQ
5.	<div>(Endpoint:social_groups CONTAINS Device-Registration)</div>	USER_DEVICE-REG

Add Rule

Move Up

Move Down

Edit Rule






Remove Rule

## 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	

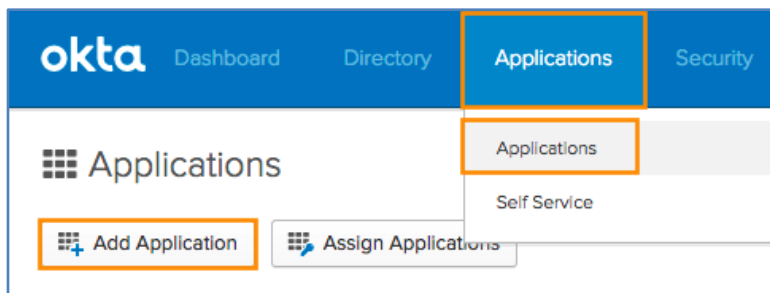
# SAML

## Okta Configuration

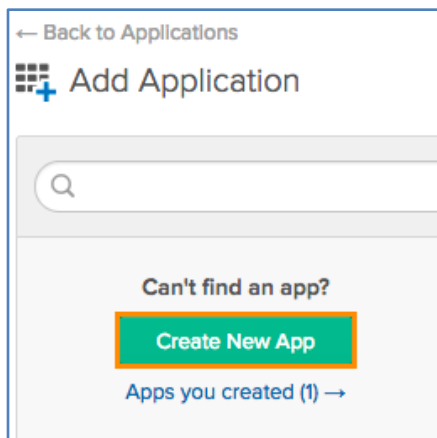
### Application Setup

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.

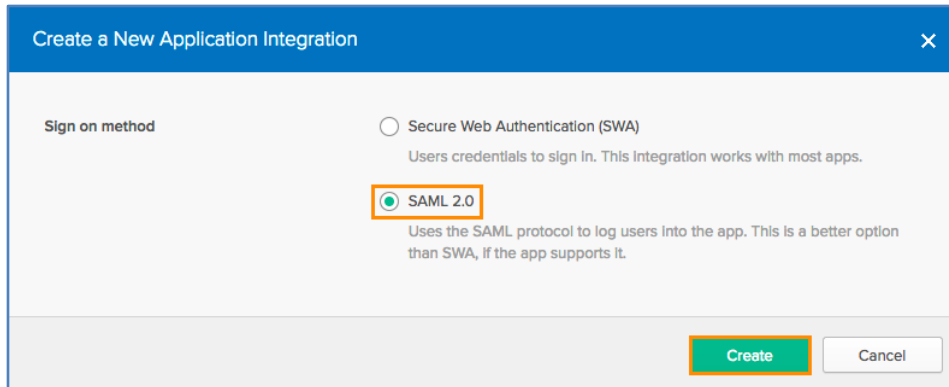
On the top menu bar, click **Applications**, and then **Applications** from the submenu. Then click **Add Application**.



Click **Create New App**.



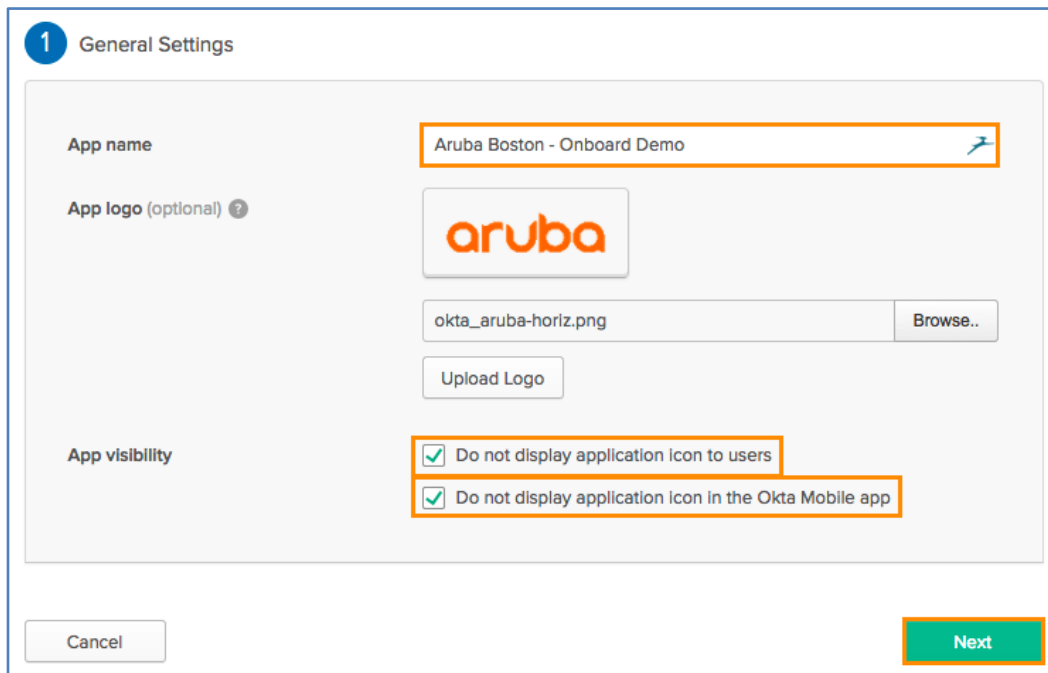
Select **SAML 2.0** and then click **Create**.



The dialog titled "Create a New Application Integration" has a close button (X) in the top right. Under "Sign on method", there are two radio buttons. The first is "Secure Web Authentication (SWA)" with the description "Users credentials to sign in. This integration works with most apps." The second is "SAML 2.0", which is selected and highlighted with an orange box; its description is "Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it." At the bottom right are "Create" and "Cancel" buttons, with "Create" highlighted in orange.

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 "General Settings" form is titled "1 General Settings". It contains three main sections: "App name" with a text field containing "Aruba Boston - Onboard Demo" and a blue arrow icon; "App logo (optional) ?" with a logo preview showing the "aruba" logo, a text field with "okta\_aruba-horiz.png", a "Browse.." button, and an "Upload Logo" button; and "App visibility" with two checked checkboxes, "Do not display application icon to users" and "Do not display application icon in the Okta Mobile app", both highlighted with orange boxes. At the bottom are "Cancel" and "Next" buttons, with "Next" highlighted in orange.

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`

The screenshot shows a configuration interface with a 'GENERAL' tab. It contains several fields for SAML configuration. The 'Single sign on URL' field is highlighted with an orange border and contains the text 'https://<clearpass-fqdn>/networkservices/saml2/sp/acs'. Below it is a checked checkbox labeled 'Use this for Recipient URL and Destination URL'. The 'Audience URI (SP Entity ID)' field is also highlighted with an orange border and contains 'https://<clearpass-fqdn>/networkservices/saml2/sp'. The 'Default RelayState' field is empty, with a note below it stating 'If no value is set, a blank RelayState is sent'. The 'Name ID format' dropdown is set to 'Unspecified'. The 'Application username' dropdown is set to 'Okta username'. A 'Show Advanced Settings' link is located at the bottom right of the configuration area.

GENERAL

Single sign on URL ?

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Show Advanced Settings](#)

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.

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value	
Title	Unspecified ▼	user.title ▼	×
Department	Unspecified ▼	user.department ▼	×
Company	Unspecified ▼	user.company ▼	×
givenname	Unspecified ▼	user.firstName ▼	×
surname	Unspecified ▼	user.lastName ▼	×
email	Unspecified ▼	user.email ▼	×

Add Another

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.

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter	
groups	Unspecified ▼	Regex ▼ .*	×

Add Another

Click **Next** when finished.

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

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app

☐ I'm a software vendor. I'd like to integrate my app with Okta

**i** The optional questions below assist Okta Support in understanding your app integration.

**App type** ? ☐ This is an internal app that we have created

**Contact app vendor** ☐ It's required to contact the vendor to enable SAML

**Which app pages did you consult to configure SAML?**

Enter links, describe where the pages are, or anything else you think is helpful

**Did you find SAML docs for this app?**

Enter any links here

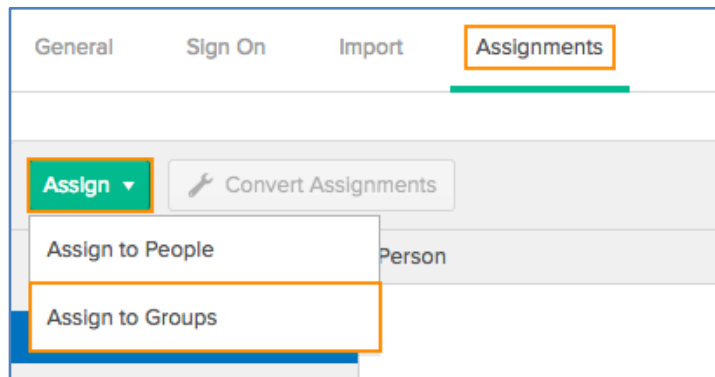
**Any tips or additional comments?**

Placeholder text

Previous Finish

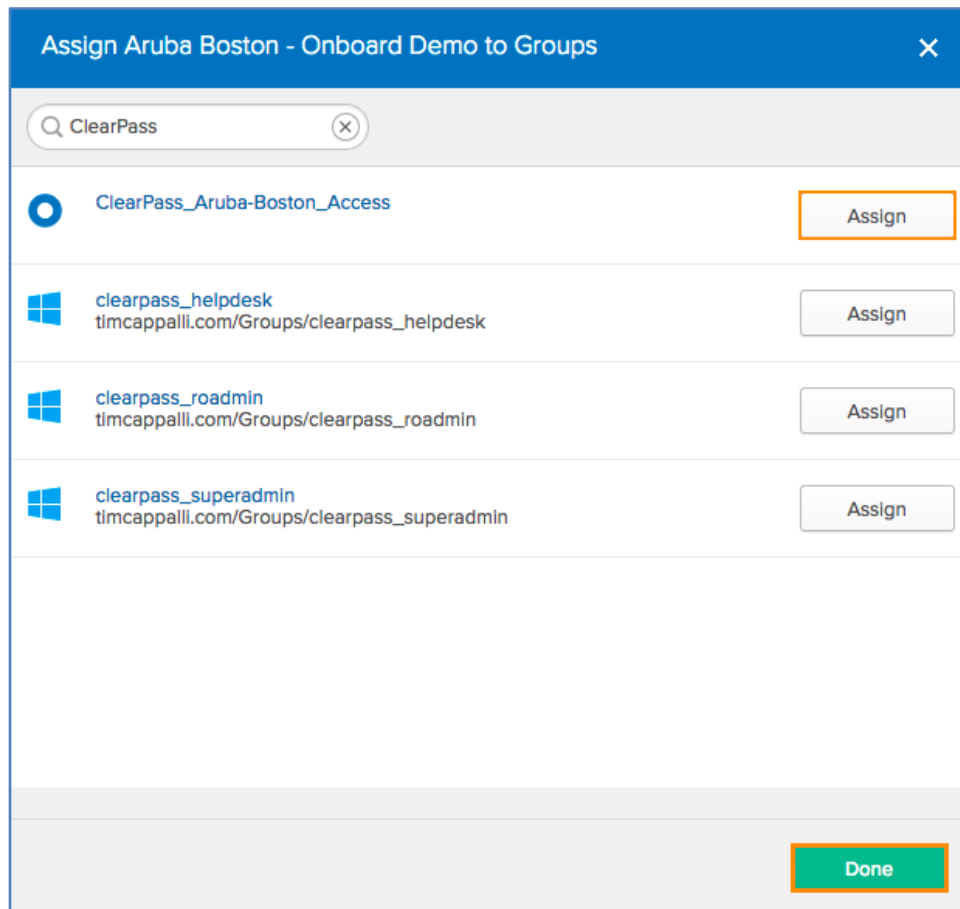
## User Assignment

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



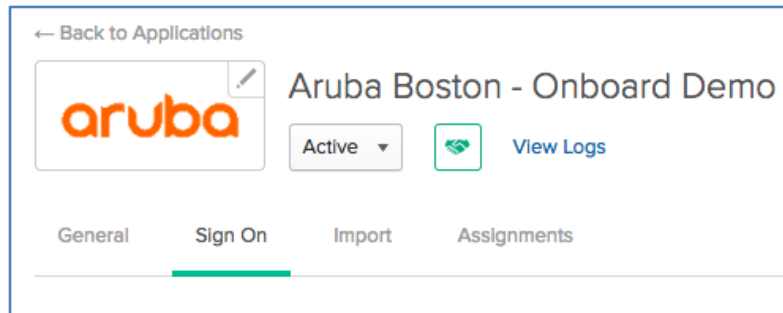
Search for the group(s) and then click **Assign**. Click **Done** when finished.

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

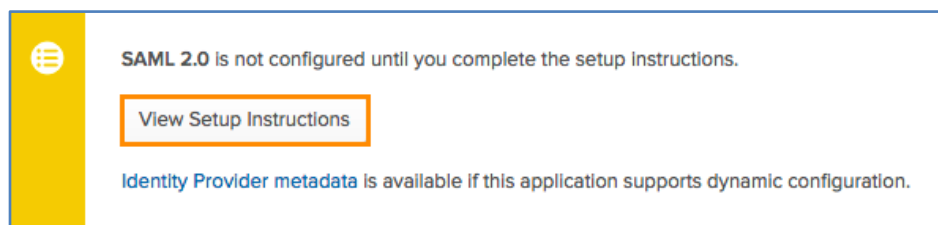


## SAML Metadata

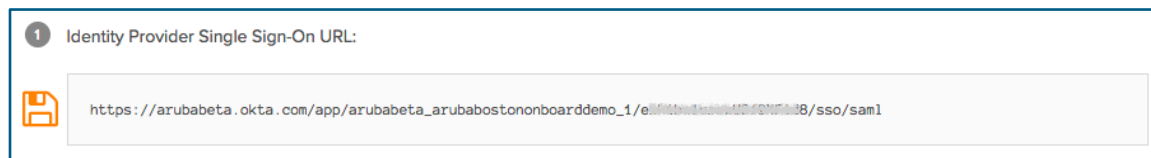
Now move over to the **Sign On** tab.



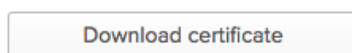
In the settings box, click the **View Setup Instructions** button.



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**.

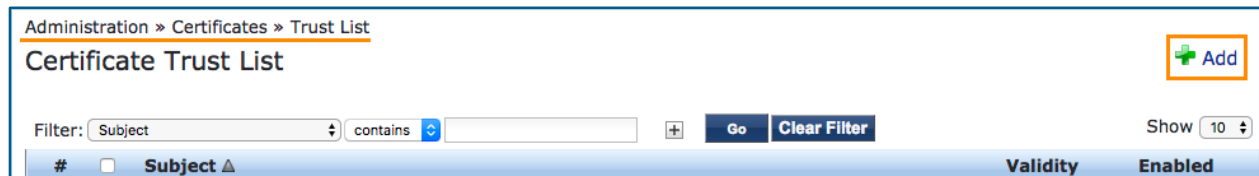


## ClearPass Policy Manager Configuration

### IdP Certificate

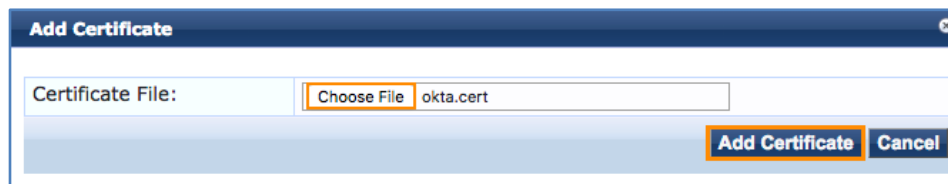
The first step in Policy Manager is to upload the identity provider certificate provided in the Okta setup.

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`

<b>SAML SP Configuration</b>	<b>SAML IdP Configuration</b>
Identity Provider (IdP) URL: <code>https://arubabeta.okta.com/app/arubabeta_arubabostonc</code>	

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

Enable SSO for	
Onboard	<input checked="" type="checkbox"/> Enable access to Onboard device provisioning portals
Insight	<input type="checkbox"/> Enable access to Insight application
PolicyManager	<input type="checkbox"/> Enable access to Policy Manager administration
Guest	<input type="checkbox"/> Enable Guest Web Login access for Guest and Onboard applications
GuestOperators	<input type="checkbox"/> Enable Guest Operator Login access for Guest and Onboard applications

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

Identity Provider (IdP) Certificate	
Select Certificate:	emailAddress=info@okta.com,CN=arubabeta,OU=SSP
Subject DN:	1.2.840.113549.1.9.1=#160d696e666f406f6b74612e636f6d,CN=arubabeta,OU=SSOProvider,O=Okta,L=San Francisco,ST=California,C=US
Issuer DN:	1.2.840.113549.1.9.1=#160d696e666f406f6b74612e636f6d,CN=arubabeta,OU=SSOProvider,O=Okta,L=San Francisco,ST=California,C=US
Issue Date/Time:	Jan 31, 2015 13:56:22 EST
Expiry Date/Time:	Jan 31, 2045 13:57:22 EST
Validity Status:	Valid
Signature Algorithm:	SHA1WithRSAEncryption
Public Key Format:	X.509
Serial Number:	1422730642516
Enabled:	true

**Note:** IdP certificate must be enabled in Certificate Trust List first, if not listed above.

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**.

#	Attribute Name	Attribute Type
1.	Cert-Version	Integer
2.	Cert-Serial-Number	String
3.	Cert-Subject-DN	String
4.	Cert-Subject-DC	String
5.	Cert-Subject-UID	String
6.	Cert-Subject-CN	String
7.	Cert-Subject-GN	String
8.	Cert-Subject-SN	String
9.	Cert-Subject-C	String
10.	Cert-Subject-L	String

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.

Administration » Dictionaries » Applications

Applications Dictionaries

Import from file

Select File: Choose File ApplicationDictionary (2).xml

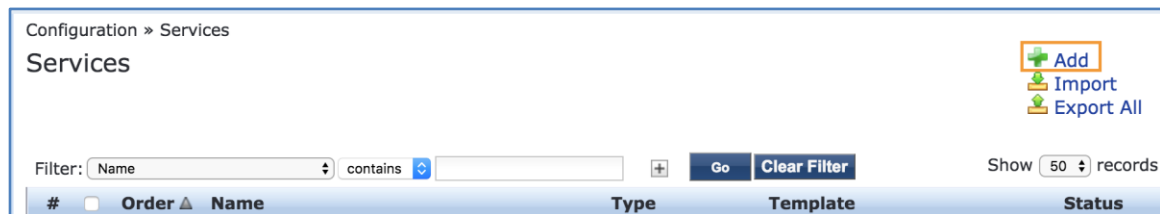
Enter secret for the file (if any):

Import Cancel

## 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**.

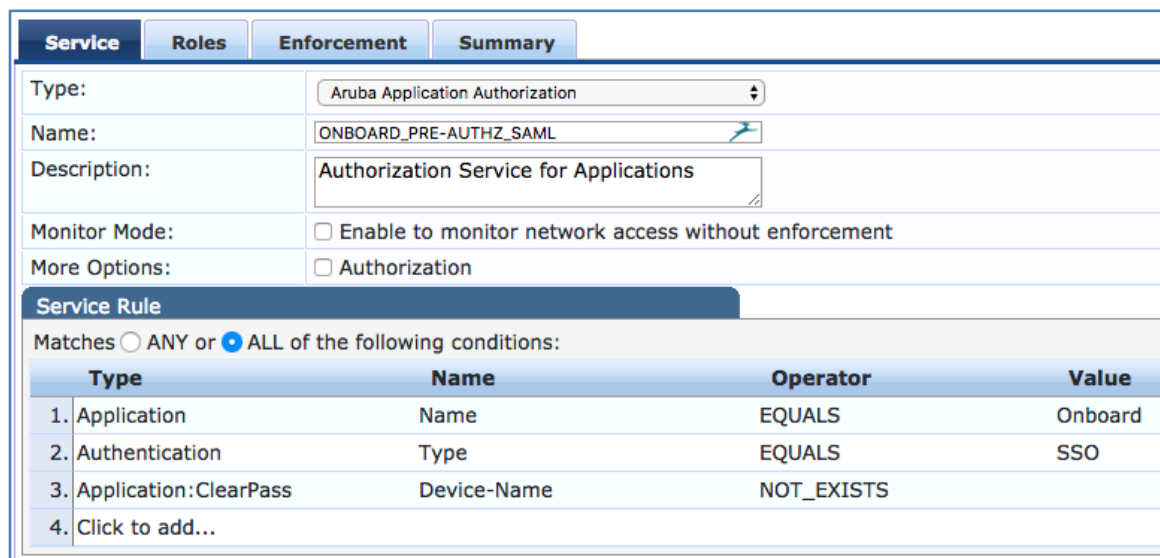


Select **Aruba Application Authorization** from the Type drop-down list and give the service a name, *ONBOARD\_PRE-AUTHZ\_SAML* for example.

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	



Type	Name	Operator	Value
1. Application	Name	EQUALS	Onboard
2. Authentication	Type	EQUALS	SSO
3. Application:ClearPass	Device-Name	NOT_EXISTS	
4. Click to add...			

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

The screenshot shows the 'Enforcement' tab selected. It contains a 'Use Cached Results' checkbox, a 'Use cached Roles and Posture attributes from previous sessions' checkbox, an 'Enforcement Policy' dropdown menu showing '[Guest Operator Logins]', a 'Modify' button, and a highlighted 'Add new Enforcement Policy' button.

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

The screenshot shows the 'Enforcement Policies' form with the 'Enforcement' tab selected. The 'Name' field is 'ONBOARD\_PRE-AUTHZ\_SAML'. The 'Description' field is empty. The 'Enforcement Type' has radio buttons for 'RADIUS', 'TACACS+', 'WEBAUTH (SNMP/Agent/CLI/CoA)', 'Application' (selected), and 'Event'. The 'Default Profile' dropdown is set to '[Deny Application Access Profile]'. There are 'View Details', 'Modify', and 'Add new' buttons.

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.

The screenshot shows the 'Rules Editor' window. Under the 'Conditions' tab, it says 'Match ALL of the following conditions:'. There is a table with columns 'Type', 'Name', 'Operator', and 'Value'. The first row has 'Tips' as Type, 'Role' as Name, 'EQUALS' as Operator, and '[User Authenticated]' as Value. Below the table is a 'Click to add...' button. Under the 'Enforcement Profiles' tab, there is a 'Profile Names' list containing '[Allow Application Access Profile]'. There are 'Move Up', 'Move Down', and 'Remove' buttons. At the bottom, there is a '--Select to Add--' dropdown, 'Save', and 'Cancel' buttons.

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
<b>Policy:</b>		
Policy Name:	OKTA	
Description:		
Default Role:	[Other]	
<b>Mapping Rules:</b>		
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. AND (Application:SSO:groups CONTAINS Doctors) (Application:SSO:groups CONTAINS Full-Time-Employee)	USER_DOC-FT	
4. AND (Application:SSO:groups CONTAINS Doctors) (Application:SSO:groups CONTAINS Part-Time-Employees)	USER_DOC-ROAM	
5. (Application:SSO:groups CONTAINS Contractors)	USER_CONTRACTOR	

Summary	Enforcement	Rules
<b>Enforcement:</b>		
Name:	ONBOARD_PRE-AUTHZ_SAML-OKTA	
Description:		
Enforcement Type:	Application	
Default Profile:	[Deny Application Access Profile]	
<b>Rules:</b>		
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:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions		
Enforcement Policy:	ONBOARD_PRE-AUTHZ_SAML		<b>Modify</b>

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](https://github.com/aruba/clearpass-cloud-service-whitelists/blob/master/cloud-login/cloud-login_okta.md)

## Sample Request

**Request Details**

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

**Request Details**

SummaryInputOutput

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 StatusShow ConfigurationExportShow LogsClose

## 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](#)



[www.arubanetworks.com](http://www.arubanetworks.com)  
3333 Scott Blvd  
Santa Clara, CA 95054

Phone: 1-800-WIFI-LAN (+800-943-4526)  
Fax 408.227.4550