

Onboard and Cloud Identity Providers

aruba

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	objectType
city	objectId
companyname	accountEnabled
country	assignedLicenses
department	city
displayname	companyName

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

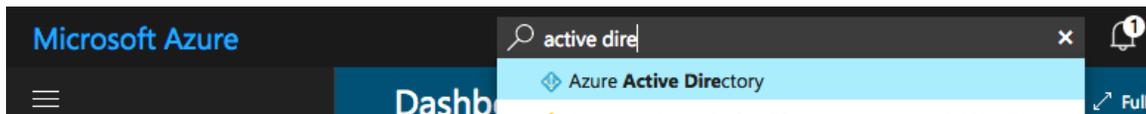
SAML

Azure Active Directory Configuration

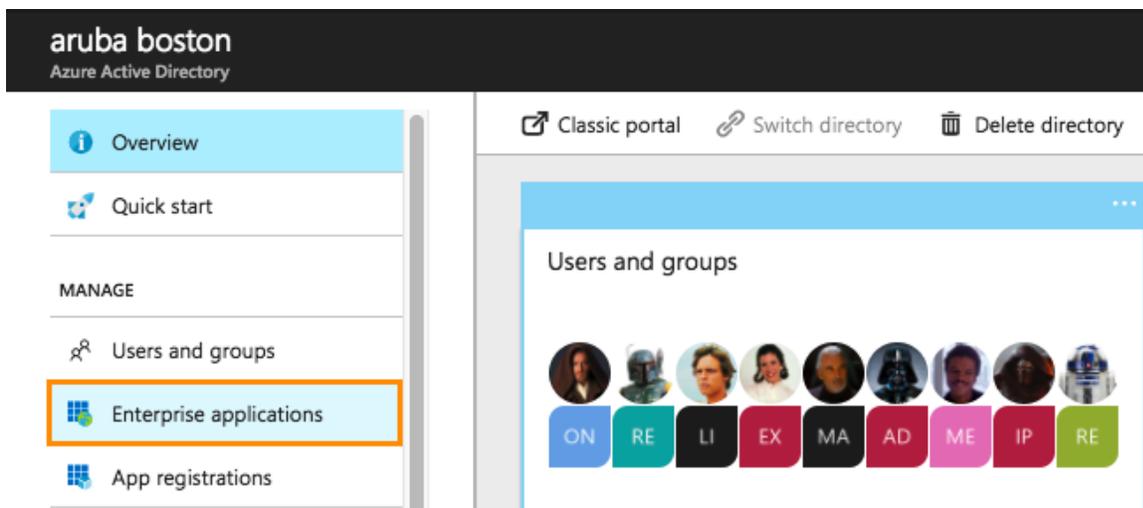
Application Setup

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

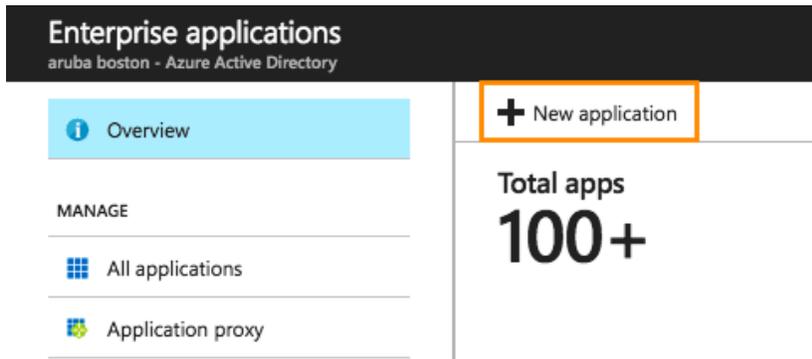
Using the search bar at the top, search for and select **Azure Active Directory**.



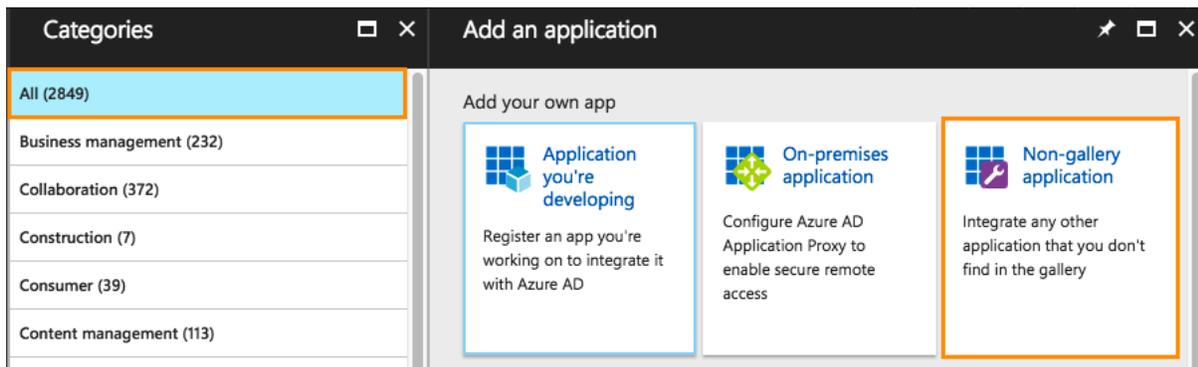
In the Azure Active Directory navigation blade, select **Enterprise applications**.



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 ⓘ

✓

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 redirected to the Quick start blade for the app. Select **Configure single sign-on** from the list.



Configure single sign-on (required)
Configure your instance of Aruba Boston Onboard Demo 2 to use Azure AD as its identity provider.

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

Mode

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**.



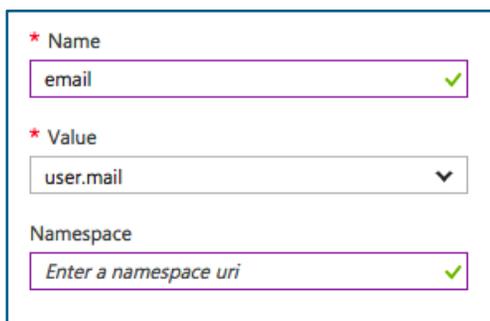
User Attributes
Edit the user information sent in the SAML token when user sign in to Aruba Boston - Onboard Demo - SAML.

User Identifier

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.



* Name

* Value

Namespace

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

NAME	VALUE	NAMESPACE
givenname	user.givenname	...
surname	user.surname	...
email	user.mail	...
name	user.userprincipalname	...
Department	user.department	...
Title	user.jobtitle	...

[Add attribute](#)

Add Attribute

* Name
 ✓

* Value
 ▼

Namespace

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	31BFCB545657FA6DD5DBAF1D94138CD9E2F1B5F9	Certificate (Base64) Certificate (Raw) Metadata XML

[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/wsfederation?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

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.

The screenshot shows the 'Aruba Boston - Onboard Demo - SAML - Properties' configuration page. The left-hand menu is visible, with 'Properties' highlighted. The main content area shows the following configuration details:

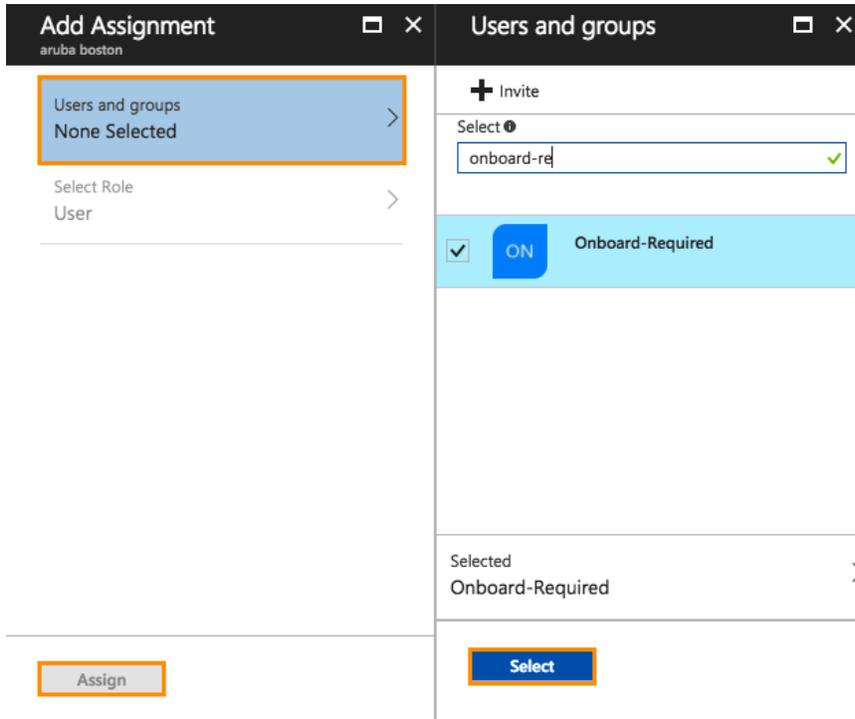
- Buttons: **Save** (highlighted), **Discard**
- Enabled for users to sign-in?: Yes No
- Name: Aruba Boston - Onboard Demo - SAML
- Publisher: Aruba Boston
- Homepage URL: (empty)
- Logo: (Aruba logo)
- User access URL: <https://myapps.microsoft.com/signin/Aruba%2...>
- Application ID: b1ba3bf1-566b-4158-9bd1-8e79d800d25a
- 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.

The screenshot shows the 'Aruba Boston - Onboard Demo - SAML - Users and groups' configuration page. The left-hand menu is visible, with 'Users and groups' highlighted. The main content area shows the following configuration details:

- Buttons: **Add user** (highlighted), **Edit**, **Remove**
- Search: 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**.



ClearPass Policy Manager Configuration

IdP Certificate

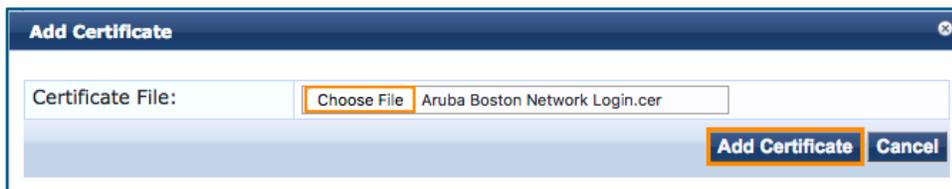
The first step in Policy Manager is to upload the identity provider certificate provided in the Azure portal.

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

SAML SP Configuration	SAML IdP Configuration
Identity Provider (IdP) URL: <input type="text" value="https://login.microsoftonline.com/406a990a-06b2-4a9e-"/>	

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"/> Enabled 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**.

Identity Provider (IdP) Certificate	
Select Certificate:	<input type="text" value="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

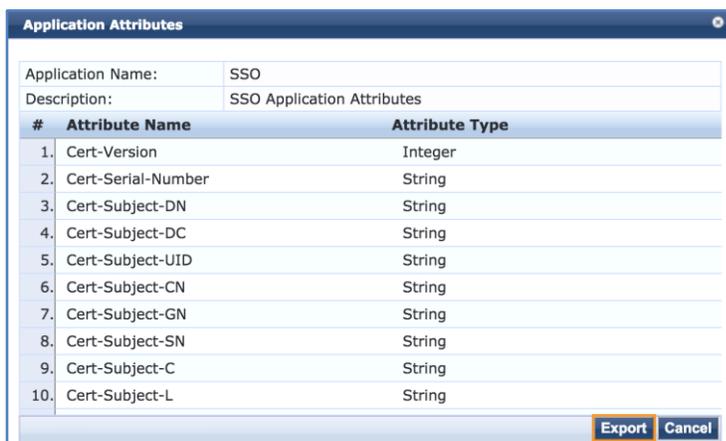
Click **Save** at the bottom.

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**.

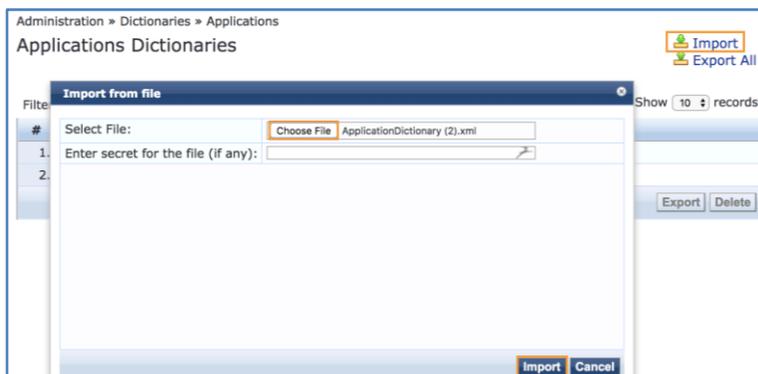


Open the exported XML file in a text editor.

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

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

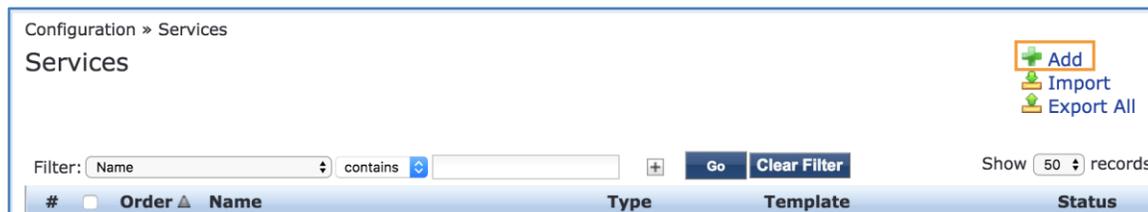
Once all of the desired attributes have been added, save the file and import it back into ClearPass.



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	

Service	Roles	Enforcement	Summary	
Type:	Aruba Application Authorization			
Name:	ONBOARD_PRE-AUTHZ_SAML			
Description:	Authorization Service for Applications			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
	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 a configuration interface with tabs for Service, Authorization, Roles, Enforcement, and Summary. The Enforcement tab is active. It contains a checkbox for "Use Cached Results" and another for "Use cached Roles and Posture attributes from previous sessions". Below this, there is a dropdown menu for "Enforcement Policy" currently set to "[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" configuration page with tabs for Enforcement, Rules, and Summary. The Enforcement tab is active. It contains a form with the following fields: "Name" (ONBOARD_PRE-AUTHZ_SAML), "Description" (empty), "Enforcement Type" (Application selected), and "Default Profile" ([Deny Application Access Profile]). There are also "View Details" and "Modify" buttons, and a partially visible "Add new" button.

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" configuration page. It has a "Conditions" section with a table for defining conditions. The table has columns for Type, Name, Operator, and Value. The first condition is: Type: TIPS, Name: Role, Operator: EQUALS, Value: [User Authenticated]. Below the conditions is an "Enforcement Profiles" section with a list of profile names, including "[Allow Application Access Profile]", and buttons for "Move Up", "Move Down", and "Remove". There is also a "--Select to Add--" dropdown and "Save" and "Cancel" buttons at the bottom.

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]

[Back to Services](#)

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

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 Select the method used to authorize devices.
Use SSO:	<input checked="" type="checkbox"/> Single Sign-On – Enable SSO for device provisioning If enabled then users will be required to authenticate via SSO
* Configuration Profile:	Wireless_Aruba-Boston Select the configuration profile that will be provisioned to devices.
* Maximum Devices:	0 The maximum number of devices that a user may provision. Use 0 for unlimited.

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

NAD Whitelist

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

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

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

Sample Request

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

Request Details

Summary
Input
Output

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

Policies Used -

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

◀ Showing 1 of 1-10 records ▶▶

Change Status
Show Configuration
Export
Show Logs
Close

Request Details

Summary
Input
Output

Computed Attributes

Application:Name	Onboard
Application:SSO:Company	Galactice Empire
Application:SSO:Department	Management
Application:SSO:http://schemas.microsoft.com/claims/authnmethodsreferences	http://schemas.microsoft.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 Status
Show Configuration
Export
Show Logs
Close

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

The screenshot shows a 'Request Details' window with a dark blue header and a light blue background. It features three tabs: 'Summary' (selected), 'Input', and 'Output'. The 'Summary' tab contains a table with the following data:

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)

Below this table is a section titled 'Policies Used -' with a dark blue header. It contains another table:

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

At the bottom of the window, there is a navigation bar with a left arrow, the text 'Showing 6 of 1-10 records', a right arrow, and five buttons: 'Change Status', 'Show Configuration', 'Export', 'Show Logs', and 'Close'.

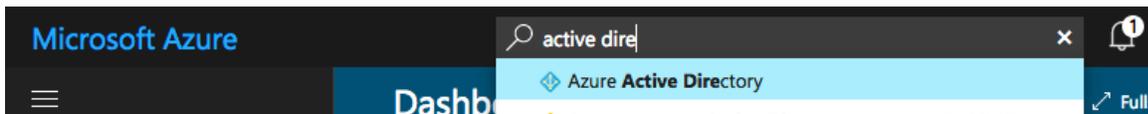
OAuth 2.0

Azure Active Directory Configuration

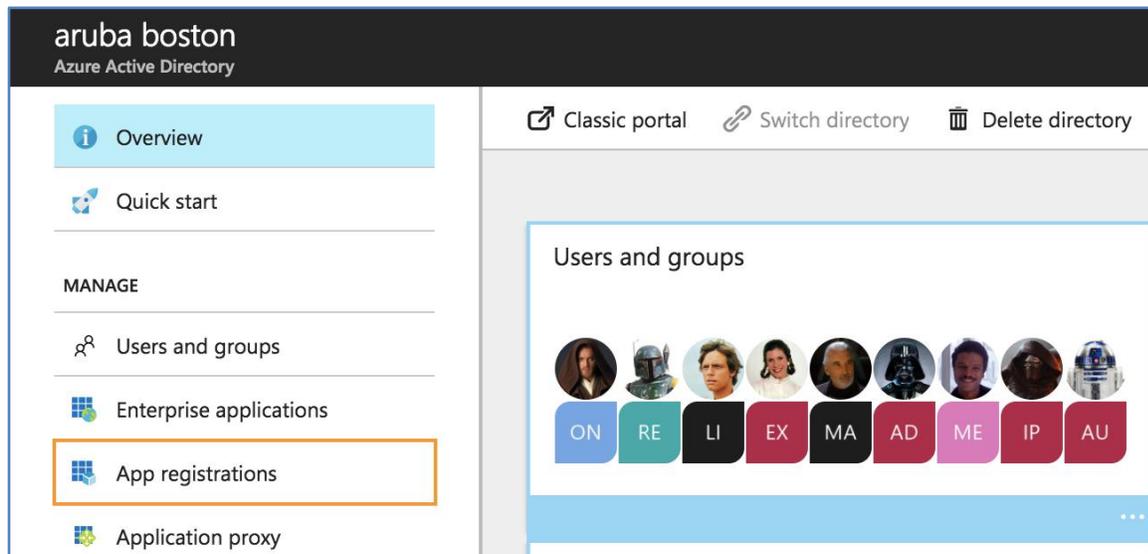
Application Setup

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

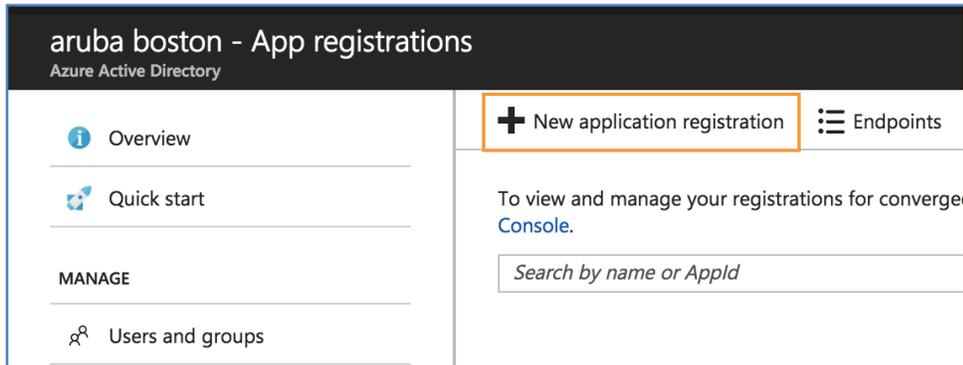
Using the search bar at the top, search for and select **Azure Active Directory**.



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



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

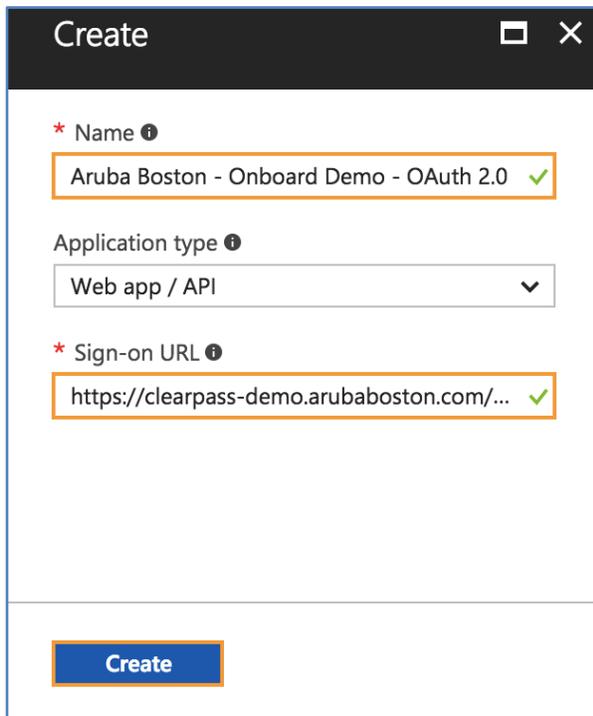


Give the app a friendly name (this will be displayed to users the first time they authenticate).

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

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

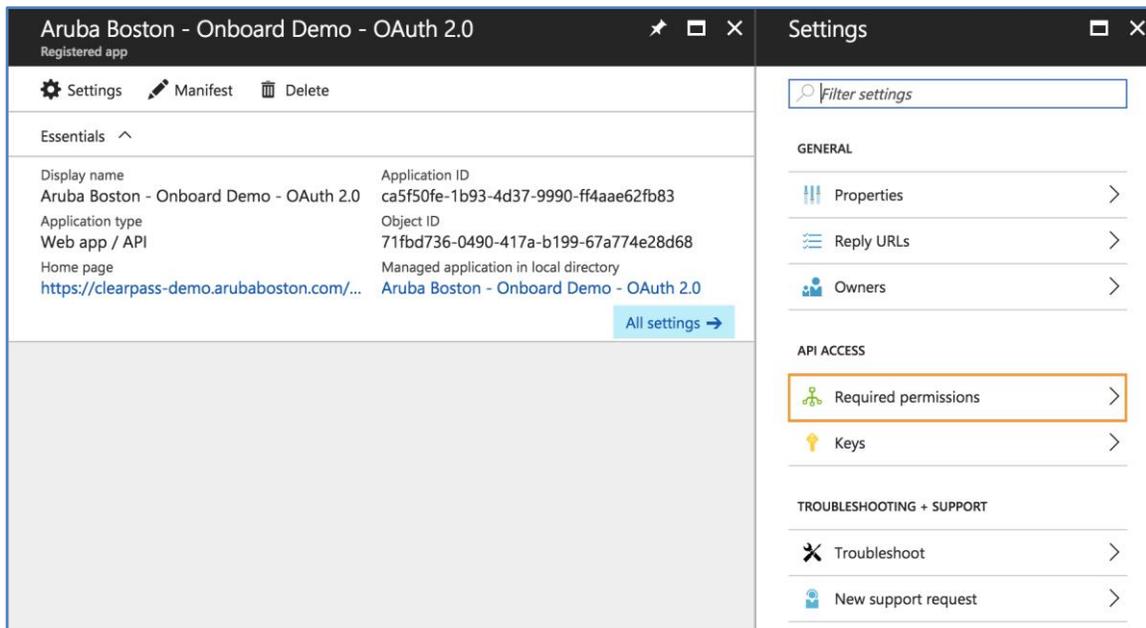
Click **Create** when done.



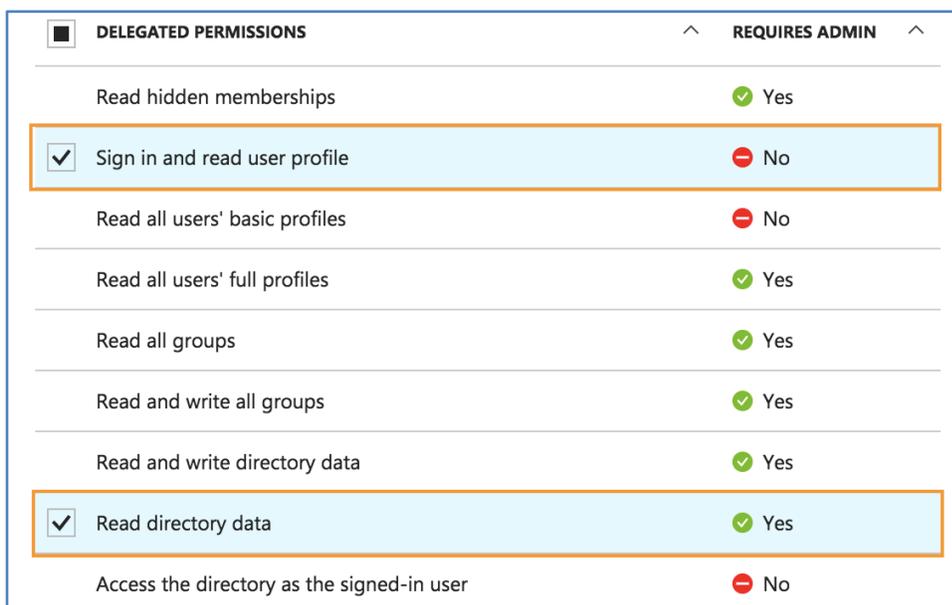
The page will redirect back to the application list. A refresh may be required if the newly created app does not appear.

Click the newly created app to access the configuration.

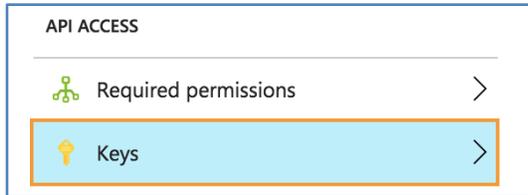
In the Settings blade under API access, click **Required permissions** and then choose **Windows Azure Active Directory**.



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



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



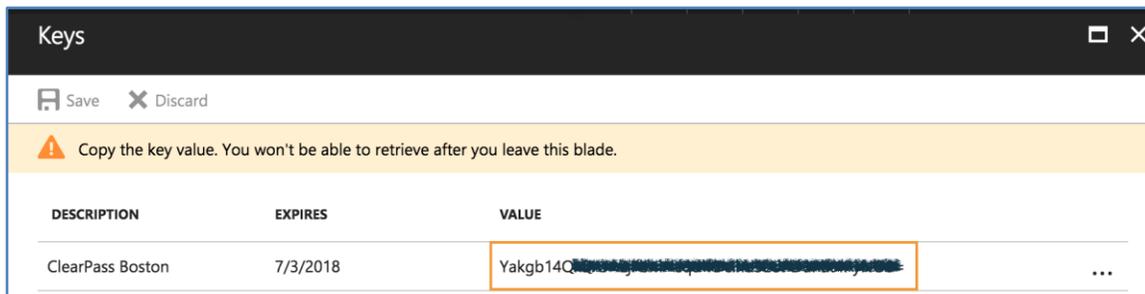
For **Key description**, give the API key a nickname.

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

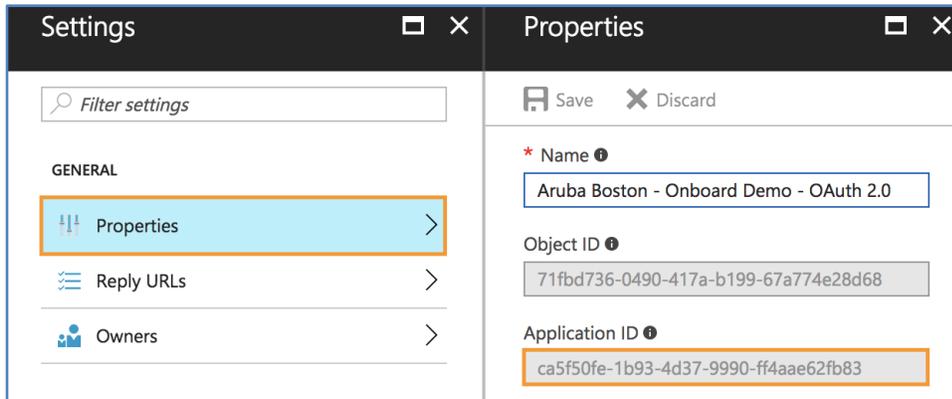
Click **Save** at the top and the key will be generated.



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



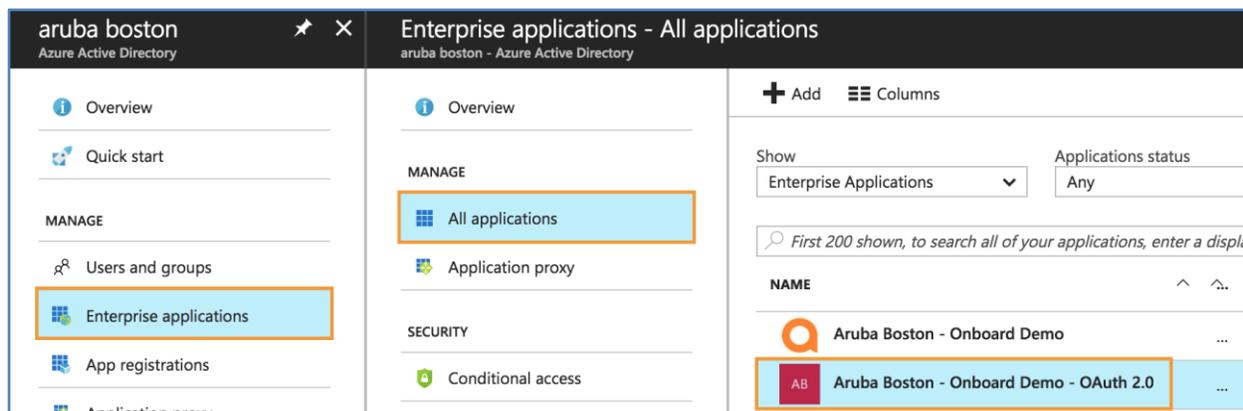
Close the **Keys** pane and then click **Properties**. Copy the **Application ID** and store it. This will be required to configure ClearPass along with the key from the previous step.



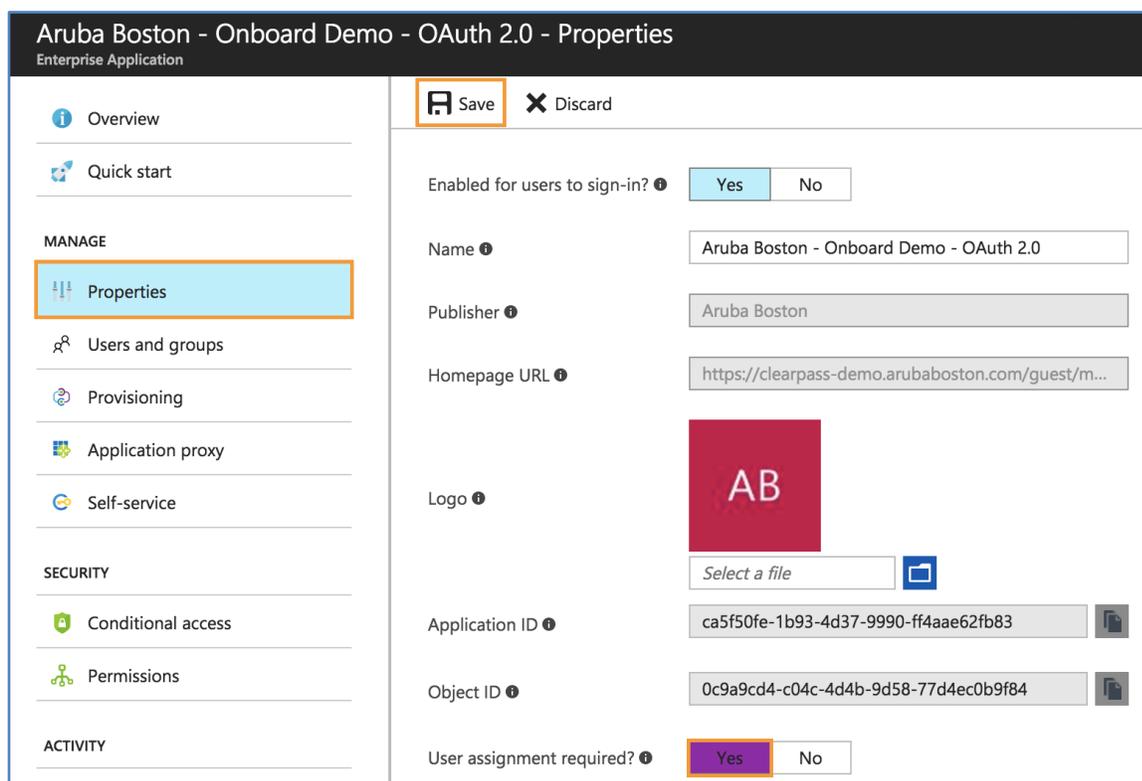
Restricting Access

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

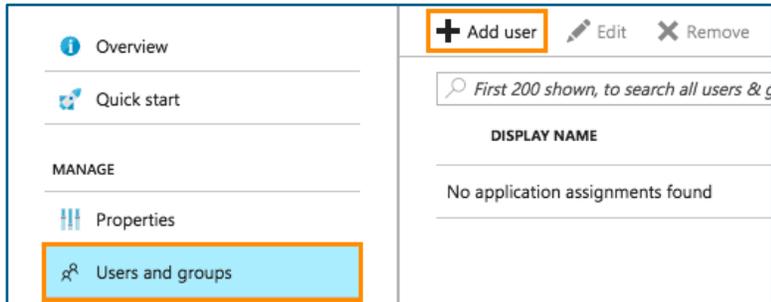
If there is a need to restrict access by group or user at the Azure Active Directory level, navigate back to the top-level Azure Active Directory blade, click **Enterprise applications**, **All applications** and then select the app created in the previous steps.



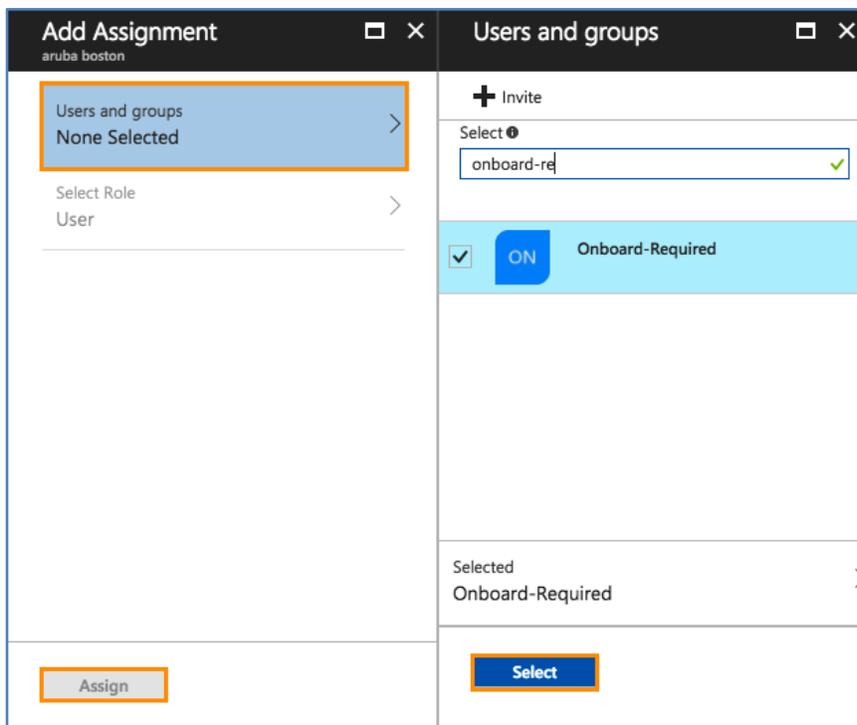
Click **Properties** and then change **User assignment required** to **Yes**, then click **Save** at the top.



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



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



ClearPass Policy Manager Configuration

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

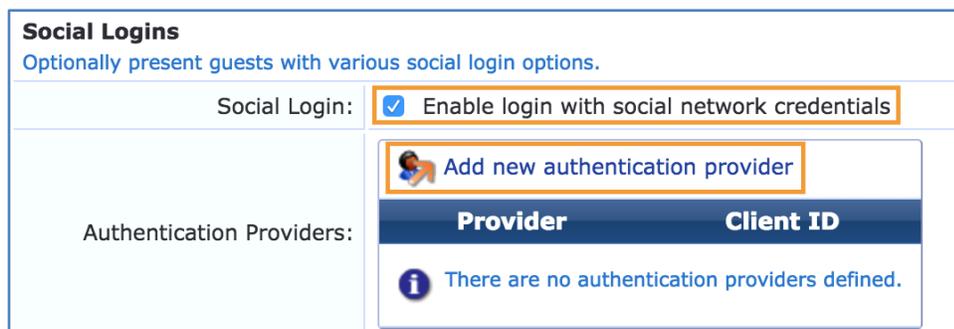
ClearPass Onboard Configuration

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



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

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



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

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

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

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

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

Properties	
* Provider:	Microsoft Azure
Enabled:	<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
Policy:		
Policy Name:	AZURE-AD_OAUTH2	
Description:		
Default Role:	[Other]	
Mapping Rules:		
Rules Evaluation Algorithm: Evaluate all		
Conditions	Role Name	
1. (Endpoint:social_groups CONTAINS Students)	USER_STUDENT	
2. (Endpoint:social_groups CONTAINS Staff)	USER_STAFF	
3. (Endpoint:social_groups CONTAINS Faculty)	USER_FACULTY	
4. (Endpoint:social_groups CONTAINS Certificate-Required)	USER_CERT-REQ	
5. (Endpoint:social_groups CONTAINS Device-Registration)	USER_DEVICE-REG	

NAD Whitelist

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

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

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

Google Cloud Identity and G Suite

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

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

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

Feature	SAML	OAuth 2.0
Requires end-user consent dialog		
Requires override for Google "Unreviewed Apps"		
Group membership	 <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	groups
title	group emails
department	given name
costcenter	family_name
	picture
	gender
	locale
	hd
	kind
	etag
	primaryEmail
	isAdmin
	isDelegatedAdmin
	lastLoginTime
	creationTime
	agreedToTerms
	suspended
	changePasswordAtNextLogin
	ipWhitelisted
	emails
	organizations:primary
	organizations:customType
	organizations:department
	nonEditableAliases
	customerId
	orgUnitPath
	isMailboxSetup
	isEnrolledIn2Sv
	isEnforcedIn2Sv
	includeInGlobalAddressList

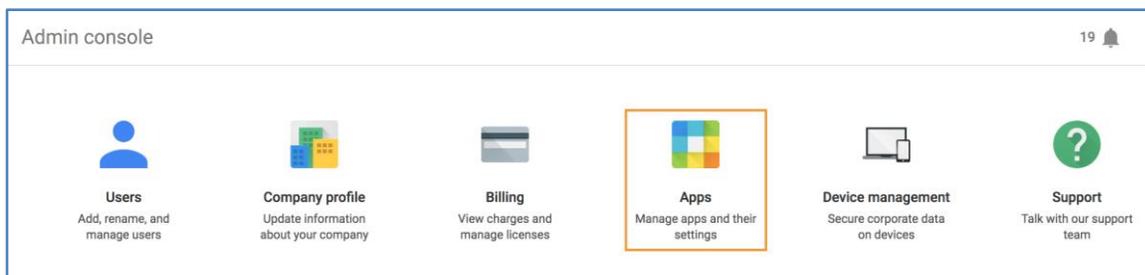
Google Secure LDAP Connector

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

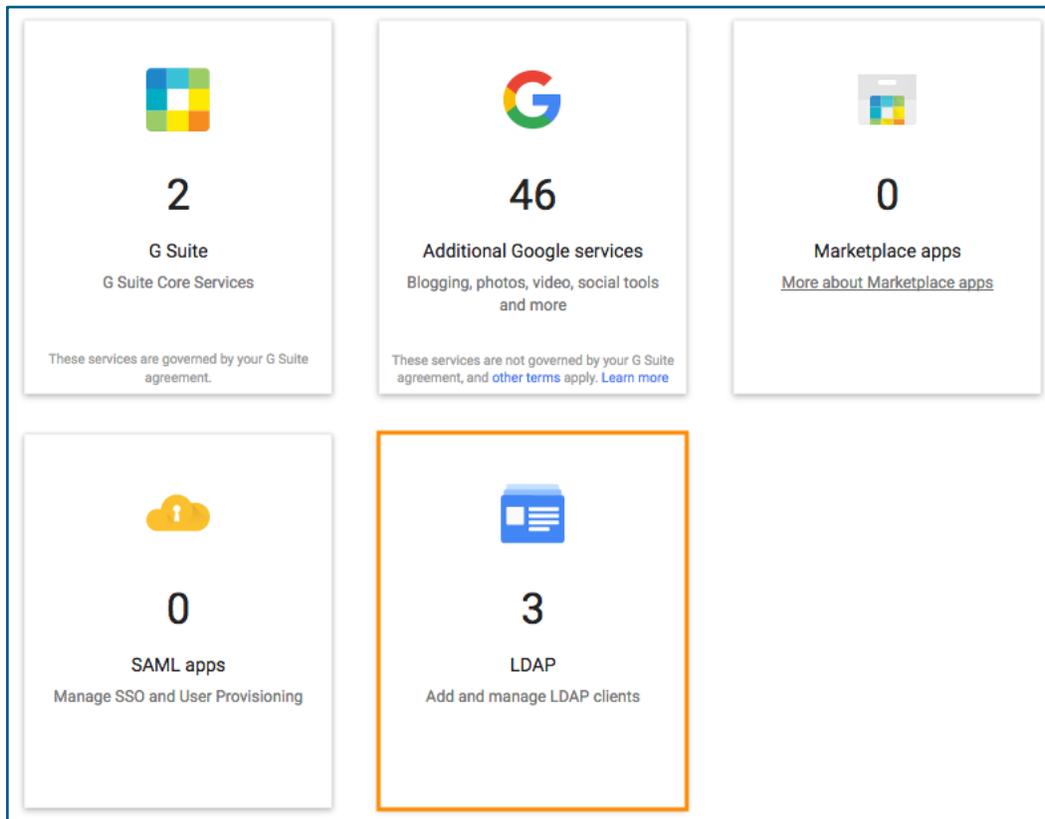
This connector uses the ClearPass Extensions framework. The Google Secure LDAP service is available to Cloud Premium, G Suite Enterprise, and all G Suite for Education organizations.

Google Admin Console Configuration

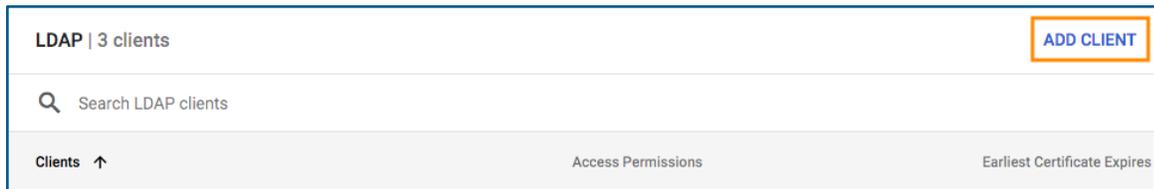
Log into the Google Admin portal at admin.google.com with an account with admin privileges for the organization. At the main admin landing page, click the **Apps** icon.



Choose **LDAP** from the list.

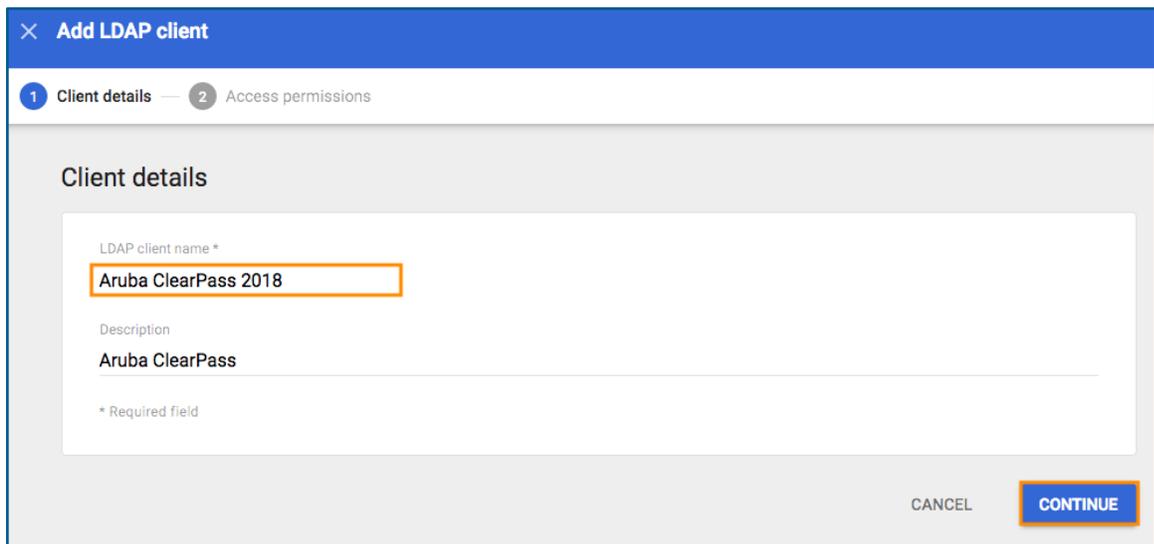


Click **ADD CLIENT**.



The screenshot shows a web interface for managing LDAP clients. At the top left, it says "LDAP | 3 clients". On the top right, there is a blue button labeled "ADD CLIENT". Below this is a search bar with a magnifying glass icon and the text "Search LDAP clients". At the bottom, there are 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 modal window titled "Add LDAP client" with a close button (X) in the top left. Below the title is a progress indicator with two steps: "1 Client details" (active) and "2 Access permissions". The main content area is titled "Client details" and contains a form with two fields: "LDAP client name *" with the value "Aruba ClearPass 2018" and "Description" with the value "Aruba ClearPass". A note at the bottom left of the form says "* Required field". At the bottom right of the modal, there are two buttons: "CANCEL" and "CONTINUE".

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

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

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:

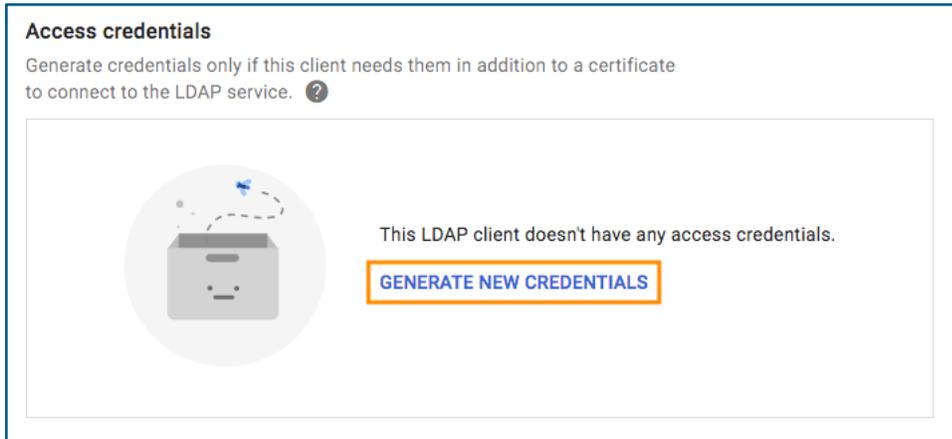
Verify user credentials	Read user information	Read group information
Entire domain	Entire domain	Has access

Authentication

Certificates
1 certificate is associated with this LDAP client

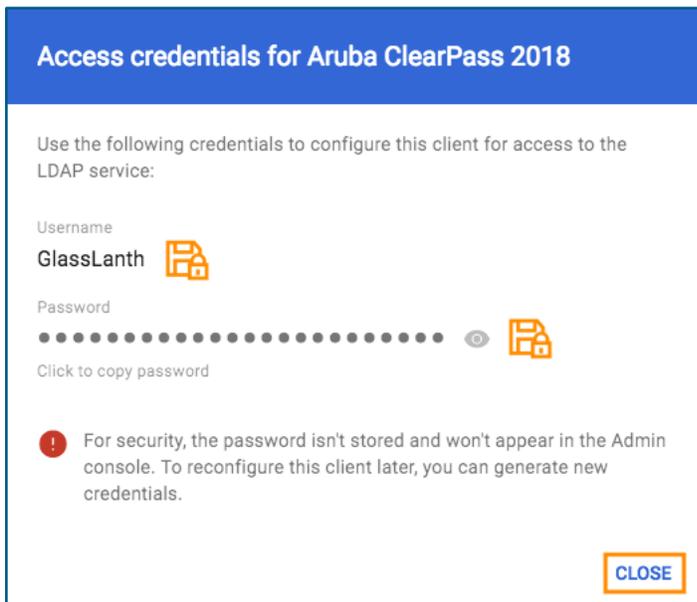
Access credentials
0 access credentials are associated with this LDAP client

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



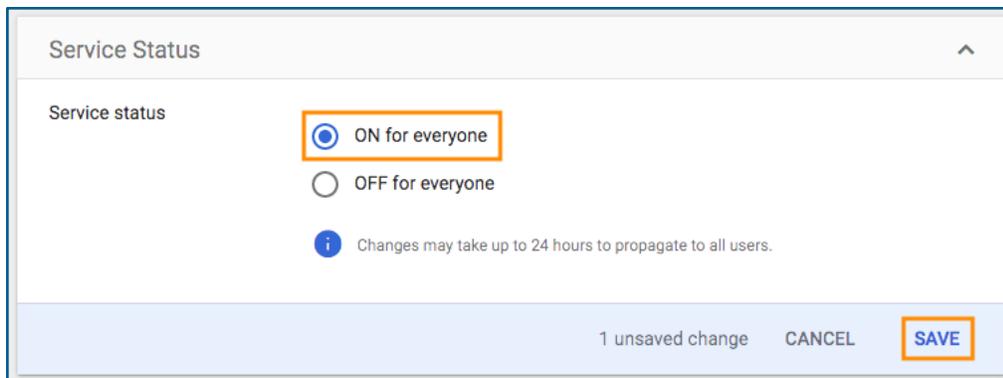
Securely store a copy of the generated credentials. They will be required to configure ClearPass.

Click **Close** when finished.



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

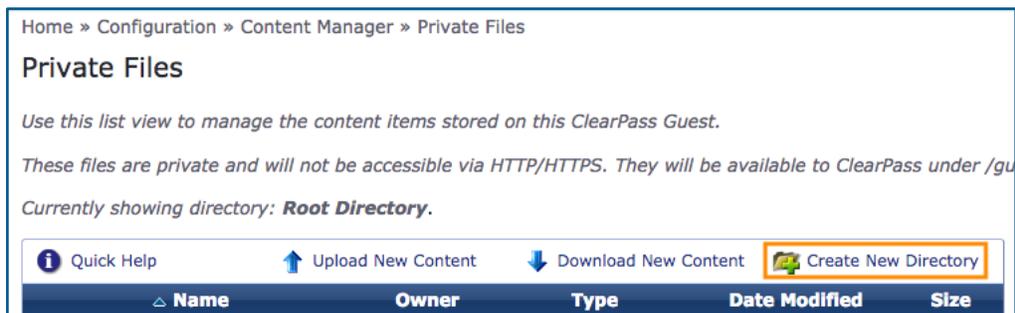
Lastly, click the **Service status** widget and choose **ON for everyone** and click **SAVE**.



The screenshot shows a dialog box titled "Service Status" with a close button in the top right corner. Inside the dialog, the "Service status" section has two radio button options: "ON for everyone" (which is selected and highlighted with an orange box) and "OFF for everyone". Below these options is an information icon and the text "Changes may take up to 24 hours to propagate to all users." At the bottom of the dialog, there is a status bar that says "1 unsaved change" and two buttons: "CANCEL" and "SAVE" (highlighted with an orange box).

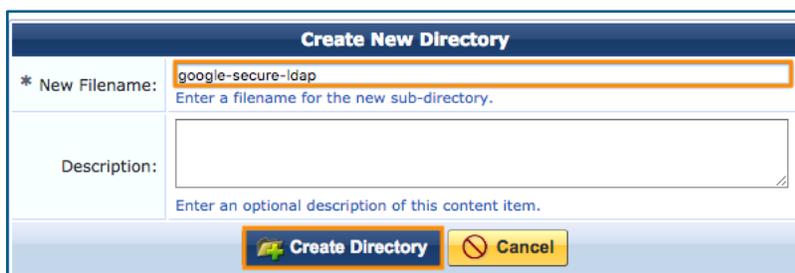
ClearPass Extension Configuration

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



The screenshot 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." and "These files are private and will not be accessible via HTTP/HTTPS. They will be available to ClearPass under /gu". It also states "Currently showing directory: **Root Directory**". At the bottom, there is a navigation bar with buttons for "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 screenshot shows a dialog box titled "Create New Directory". It has two main input fields: "* New Filename:" with the value "google-secure-ldap" (highlighted with an orange box) and a description field. Below the filename field is the text "Enter a filename for the new sub-directory." Below the description field is the text "Enter an optional description of this content item." At the bottom of the dialog, there are two buttons: "Create Directory" (highlighted with an orange box) and "Cancel".

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](#).

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

Install Extension			
* Search:	280008e1-64aa-4899-a547-19840bbabad0		
Results:	Name	Version	State
	Google Secure LDAP Connector Google Secure LDAP Connector	1.0.0	Not installed
Install			
Search			

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.

Install Extension	
Extension:	Google Secure LDAP Connector Google Secure LDAP Connector
Extension Settings	
Start:	<input checked="" type="checkbox"/> Start the extension after installation
IP Address:	<input type="text" value="172.17.0.90"/> Enter IPV4 address to allocate to this extension, from the network 172.17.0.1/16. Leave blank to automatically assign an IP address.
Content Items Required	
* certificate:	<input type="text" value="0101 google-secure-ldap/Google_2021_11_04_74127.crt"/> Select the Google LDAP Certificate (generated at admin.google.com).
* privateKey:	<input type="text" value="0101 google-secure-ldap/Google_2021_11_04_74127.key"/> Select the Google LDAP Private Key (generated at admin.google.com).
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:	<input type="text" value="Google LDAP"/>
Description:	<input type="text"/>
Type:	<input type="text" value="Generic LDAP"/>
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:	<input type="text" value="172.17.0.90"/>
Connection Security:	<input type="text" value="None"/>
Port:	<input type="text" value="1636"/>
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection
Bind DN:	<input type="text" value="CN=GlassLanth"/>
Bind Password:	<input type="password" value="....."/>
Base DN:	<input type="text" value="dc=clearpass,dc=boston"/> Search Base Dn
Search Scope:	<input type="text" value="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.	<input type="text" value="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 <i>ENDS_WITH</i> ou=Staff,ou=Users,dc=clearpass,dc=boston)	USER_STAFF	
2. (Authorization:Google LDAP:UserDN <i>ENDS_WITH</i> ou=Faculty,ou=Users,dc=clearpass,dc=boston)	USER_FACULTY	
3. (Authorization:Google LDAP:Groups <i>EQUALS</i> employees)	USER_EMPLOYEE	
4. (Authorization:Google LDAP:Groups <i>EQUALS</i> it-admins)	USER_IT	

Sample request:

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

Summary	Input	Output
Username:	josh@clearpass.boston	
End-Host Identifier:	8B-5A-F9-3A-70-C4	
Access Device IP/Port:	100.81.2.10:0 (aruba-fmc-1 / Aruba)	
RADIUS Request		
Authorization Attributes		
Authorization:Google LDAP:Groups	employees	
Authorization:Google LDAP:UserDN	uid=josh,ou=Staff,ou=Users,dc=clearpass,dc=boston	

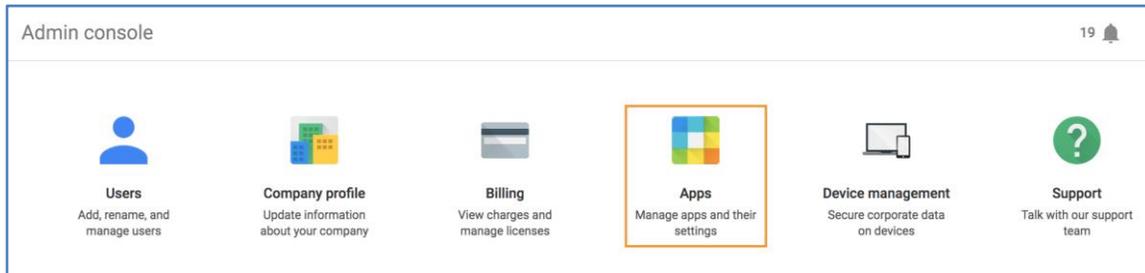
SAML

Google Admin Configuration

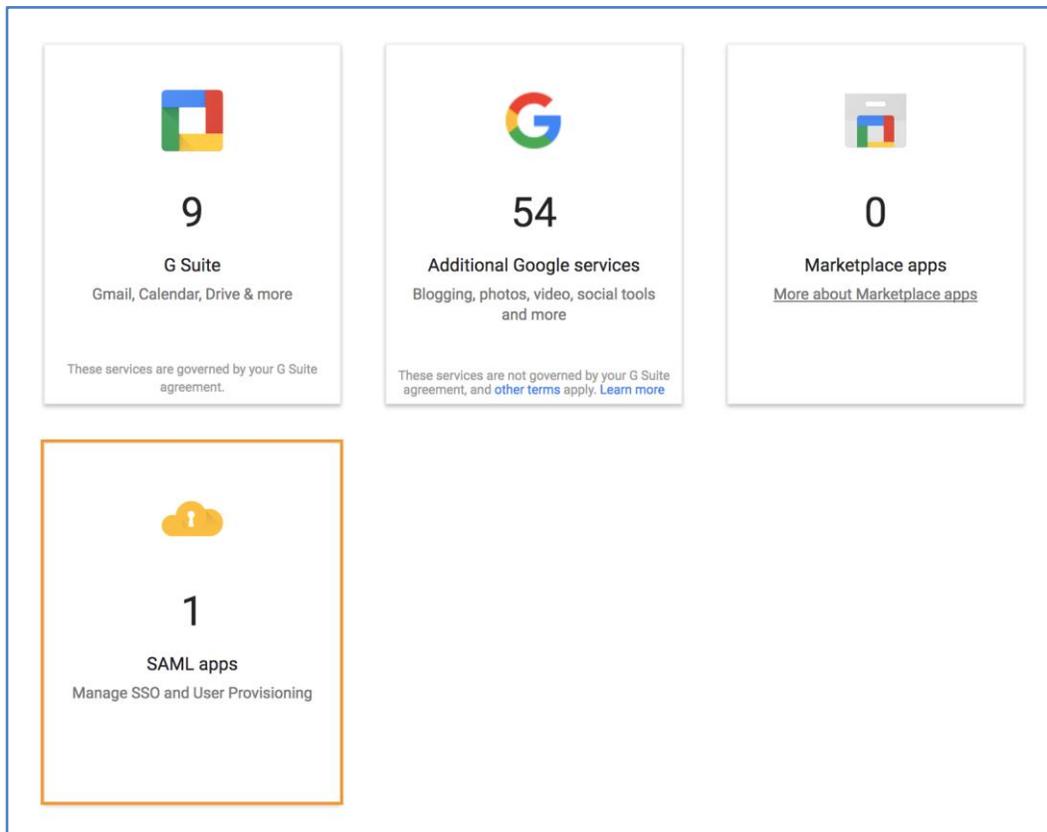
Application Setup

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

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

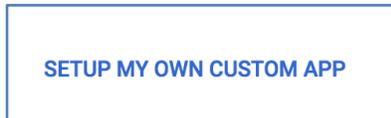


Choose **SAML apps** from the list.



Click the  button towards the bottom right.

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



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

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 options:

- Application Name ***: A text input field containing "Aruba Boston - Onboard Demo". Below it, the app-id is "aruba_boston_-_onboard_demo".
- Description**: A text input field containing "ClearPass Onboard login".
- Upload logo**: A "CHOOSE FILE" button. Below it, a file named "aruba-a_500x500.jpg" is listed with a size of "64.9 KB".

At the bottom of the window, there are three buttons: "PREVIOUS", "CANCEL", and "NEXT". The "NEXT" button is highlighted with an orange border.

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

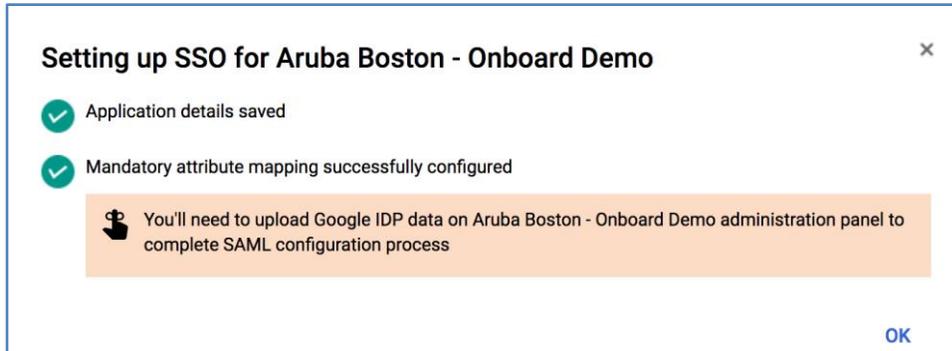
Provide mappings between service provider attributes to available user profile fields.

Title Employee Details Job Title

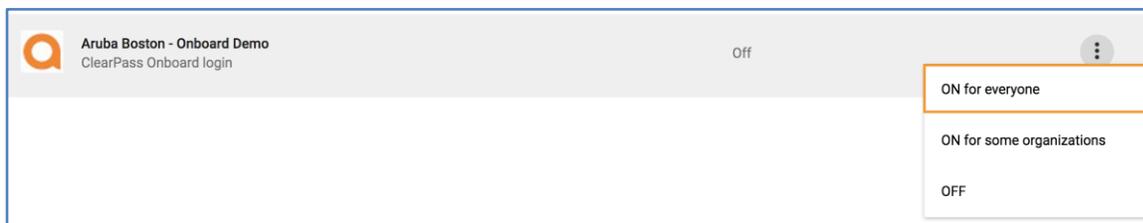
Department Employee Details Department

PREVIOUS CANCEL FINISH

Click **OK** on the summary screen.

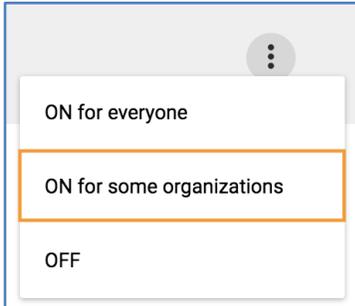


By default, the application will be turned off. In the SAML App list, click the triple dot menu for the app, and click **ON for everyone**. To restrict access to certain groups, see the next section.



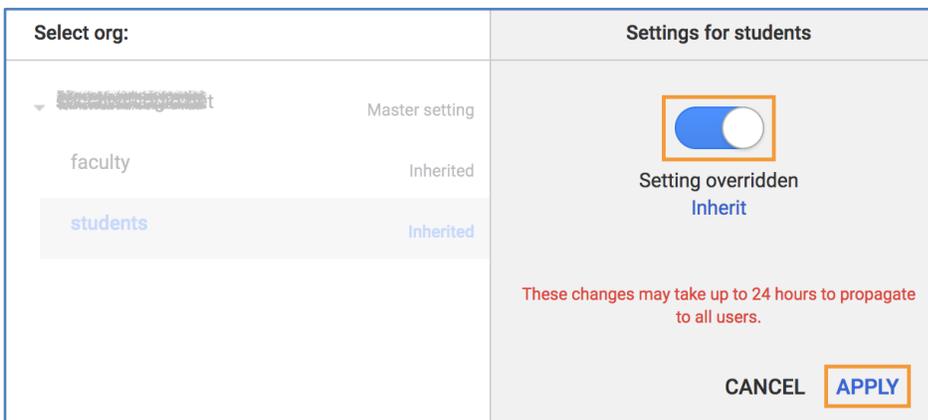
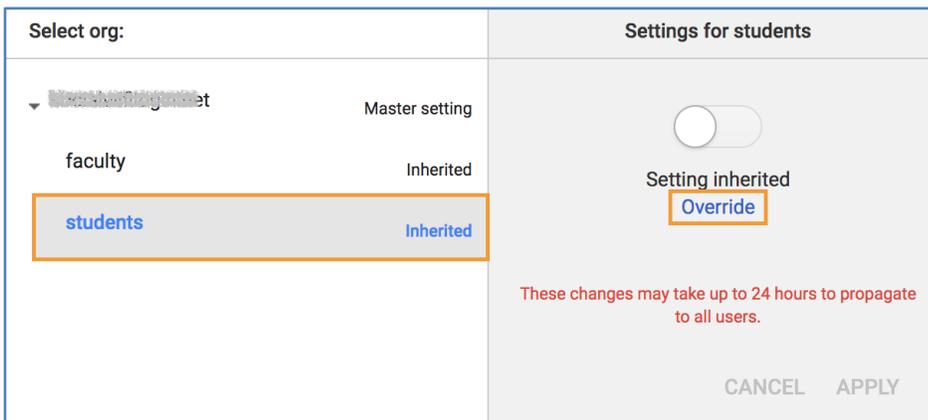
Restricting Access

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

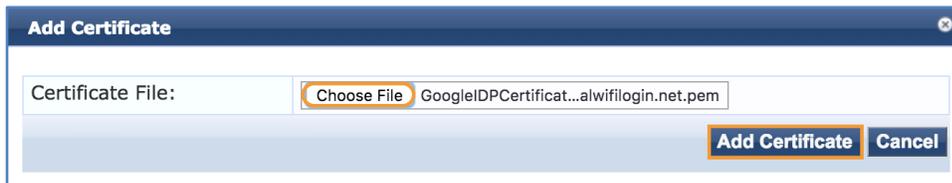
The first step in Policy Manager is to upload the identity provider certificate provided in the G Suite admin console.

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:	https://accounts.google.com/o/saml2/idp?idpid=C02qd8

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"/> Enabled 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=Googli
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
Note: IdP certificate must be enabled in Certificate Trust List first, if not listed above.	

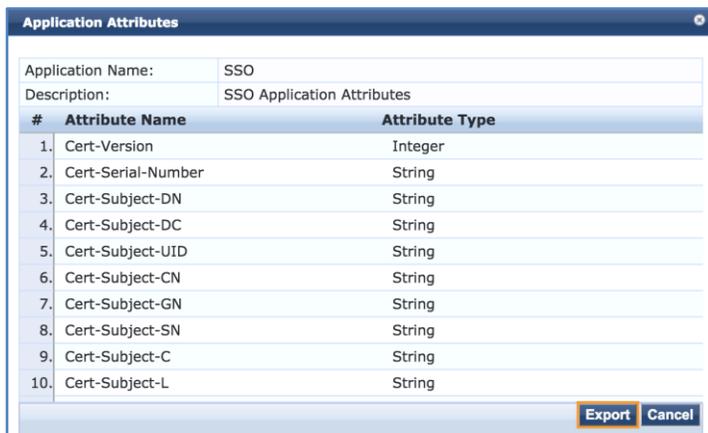
Click **Save** at the bottom.

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. 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**.



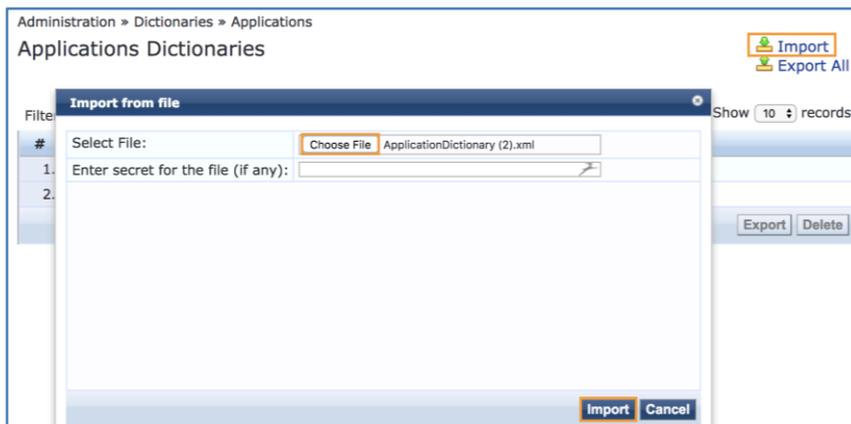
#	Attribute Name	Attribute Type
1.	Cert-Version	Integer
2.	Cert-Serial-Number	String
3.	Cert-Subject-DN	String
4.	Cert-Subject-DC	String
5.	Cert-Subject-UID	String
6.	Cert-Subject-CN	String
7.	Cert-Subject-GN	String
8.	Cert-Subject-SN	String
9.	Cert-Subject-C	String
10.	Cert-Subject-L	String

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.

```
<AppDictionaryAttributes 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	

Service	Roles	Enforcement	Summary	
Type:	Aruba Application Authorization			
Name:	ONBOARD_PRE-AUTHZ_SAML			
Description:	Authorization Service for Applications			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
	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 a configuration interface with tabs for Service, Authorization, Roles, Enforcement, and Summary. The Enforcement tab is active. It contains a checkbox for 'Use Cached Results' and another for 'Use cached Roles and Posture attributes from previous sessions'. Below this, there is a dropdown menu for 'Enforcement Policy' currently set to '[Guest Operator Logins]', a 'Modify' button, and a button labeled 'Add new Enforcement Policy' which is highlighted with an orange box.

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

The screenshot shows the 'Enforcement Policies' configuration page with tabs for Enforcement, Rules, and Summary. The Enforcement tab is active. It contains a form with the following fields: 'Name' (ONBOARD_PRE-AUTHZ_SAML), 'Description' (empty), 'Enforcement Type' (Application selected), and 'Default Profile' ([Deny Application Access Profile]). There are 'View Details' and 'Modify' buttons, and a partially visible 'Add new' button.

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' configuration page. It has two main sections: 'Conditions' and 'Enforcement Profiles'. The 'Conditions' section shows a table with one condition: Type: TIPS, Name: Role, Operator: EQUALS, Value: [User Authenticated]. The 'Enforcement Profiles' section shows a list of profile names with '[Allow Application Access Profile]' selected. There are 'Move Up', 'Move Down', and 'Remove' buttons. At the bottom, there 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
Policy:		
Policy Name:	G-SUITE_SAML	
Description:		
Default Role:	[Other]	
Mapping Rules:		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Role Name	
1. (Application:SSO:Department EQUALS Students)	USER_STUDENT	
2. (Application:SSO:Department EQUALS Staff)	USER_STAFF	
3. (Application:SSO:Department EQUALS Faculty)	USER_FACULTY	

Summary	Enforcement	Rules
Enforcement:		
Name:	ONBOARD_PRE-AUTHZ_SAML-GSUITE	
Description:		
Enforcement Type:	Application	
Default Profile:	[Deny Application Access Profile]	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Role EQUALS USER_STUDENT)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M, ONBOARD_MAX-DEVICES_3	
2. (Tips:Role MATCHES_ANY USER_STAFF USER_FACULTY)	[Allow Application Access Profile], ONBOARD_MAX-DEVICES_5	

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

Summary	Service	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> 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 Google accounts login page and other embedded resources, certain domain names need to be whitelisted.

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

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

Sample Request

Request Details ✕

Summary

Input

Output

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

Policies Used -

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

◀ Showing 1 of 1-32 records ▶▶
Change Status
Show Configuration
Export
Show Logs
Close

Request Details ✕

Summary

Input

Output

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

Computed Attributes ⊖

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

◀ Showing 1 of 1-32 records ▶▶
Change Status
Show Configuration
Export
Show Logs
Close

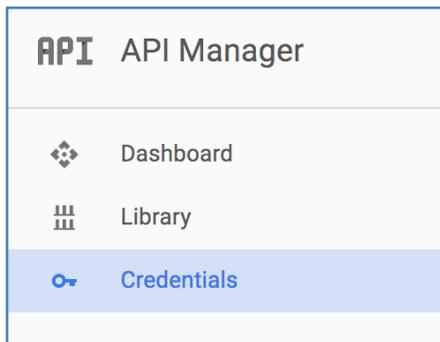
OAuth 2.0

Google Admin Console Configuration

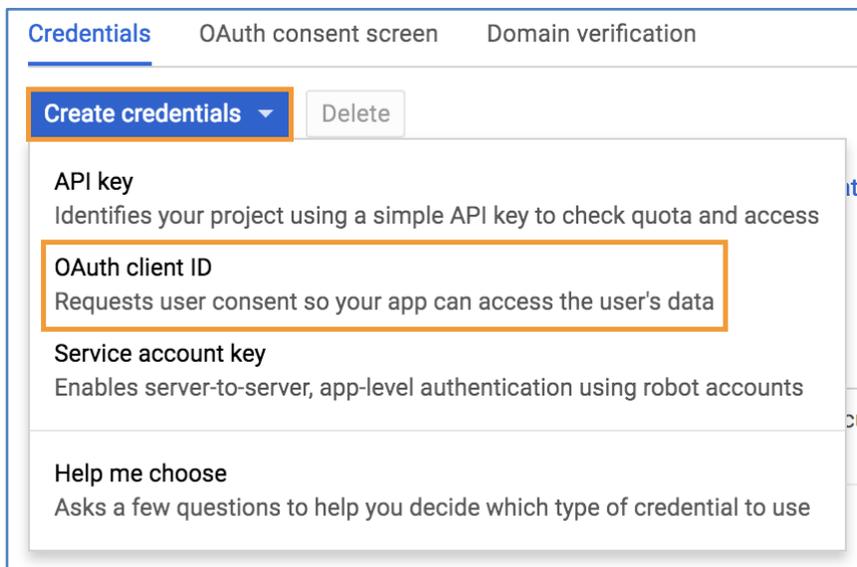
Application Setup

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

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



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



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

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

The screenshot shows a configuration form with two sections. The first section is titled "Application type" and contains five radio button options: "Web application" (which is selected), "Android Learn more", "Chrome App Learn more", "iOS Learn more", "PlayStation 4", and "Other". The second section is titled "Name" and contains a text input field with the value "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.

The screenshot shows the "Restrictions" configuration page. It has a sub-header "Enter JavaScript origins, redirect URIs, or both". There are two main sections: "Authorized JavaScript origins" and "Authorized redirect URIs". The "Authorized JavaScript origins" section has a text input field containing "http://www.example.com". The "Authorized redirect URIs" section has a list of two entries: "https://clearpass-demo.arubaboston.com/onboard/wireless_g_suite_oauth2.php" and "https://clearpass-demo.arubaboston.com/guest/social_provider_edit.php". Each entry has a "Replace" button and a close "X" button. Below the list is a text input field containing "http://www.example.com/oauth2callback". At the bottom left, there are "Save" and "Cancel" buttons.

Google Developer Verification Override

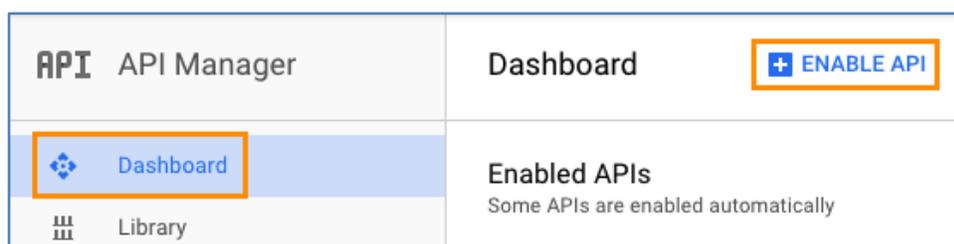
Google now requires that all OAuth web apps be verified. Because this is a custom configuration for each Cloud Identity or G Suite tenant, this web app must be enabled as an “Unreviewed” app.

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

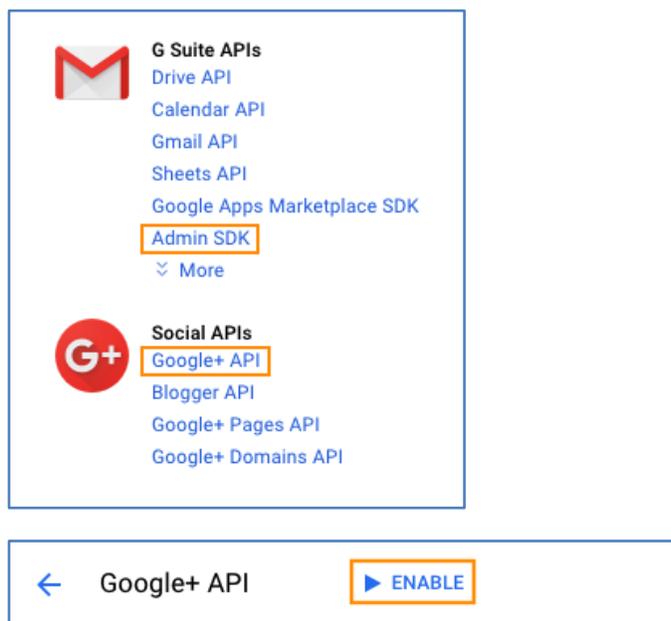
Enable APIs

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

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



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



ClearPass Policy Manager Configuration

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

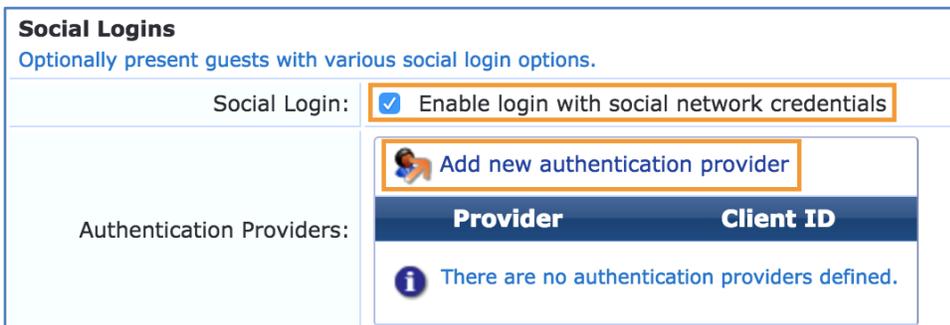
ClearPass Onboard Configuration

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



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

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



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

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

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

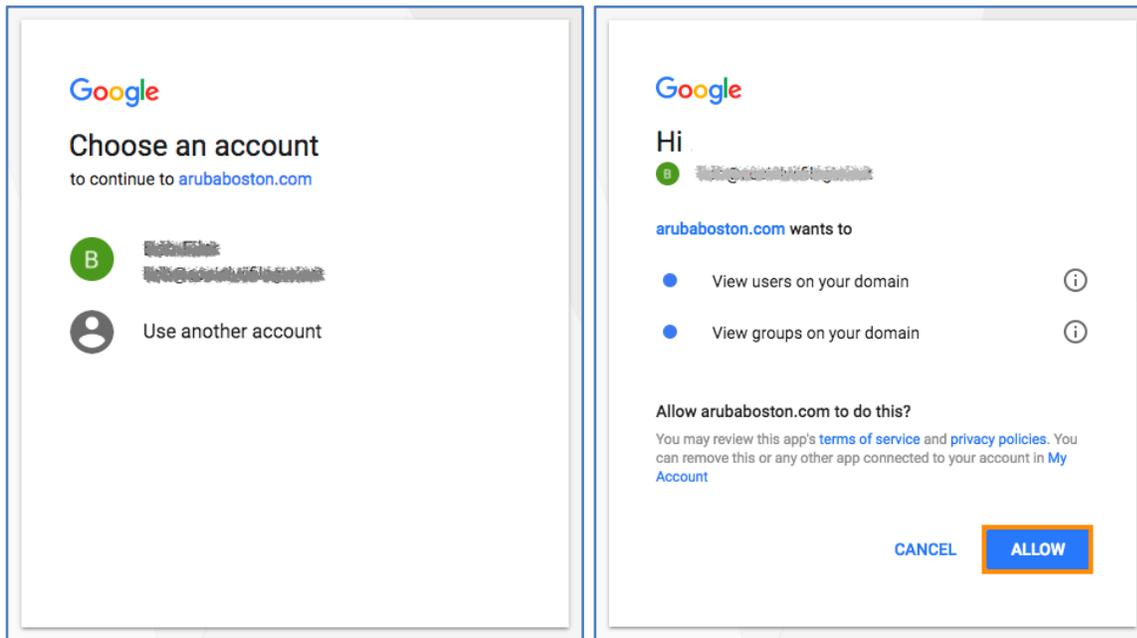
For **Endpoint Attributes**, select **Create Endpoint converting any arrays to JSON**.

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"/> Retrieve the group memberships for the guest's account
* 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.



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"/>
 	

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

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.	(Endpoint:social_orgUnitPath ENDS_WITH /students) OR (Endpoint:social_groups CONTAINS students)	USER_STUDENT
2.	(Endpoint:social_orgUnitPath ENDS_WITH /staff) OR (Endpoint:social_groups CONTAINS Staff)	USER_STAFF
3.	(Endpoint:social_orgUnitPath ENDS_WITH /staff/faculty) OR (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

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	

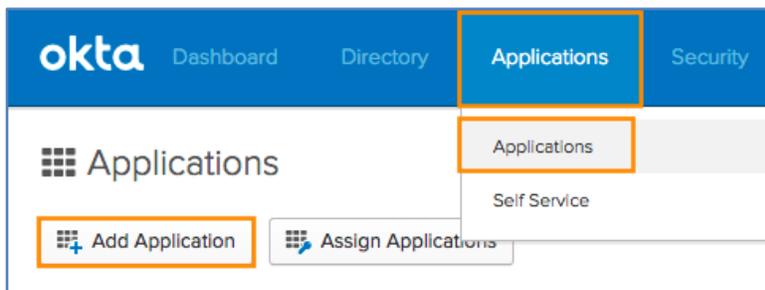
SAML

Okta Configuration

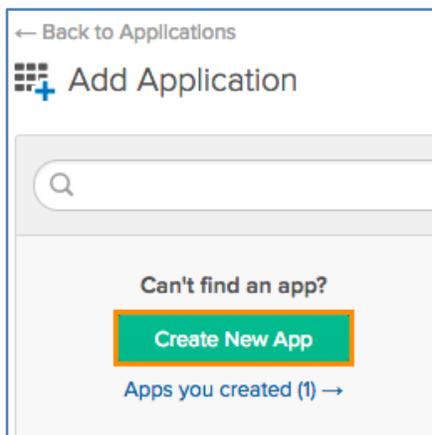
Application Setup

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**.

Create a New Application Integration

Sign on method

Secure Web Authentication (SWA)
Users credentials to sign in. This integration works with most apps.

SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

Create Cancel

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**.

1 General Settings

App name: Aruba Boston - Onboard Demo

App logo (optional): aruba

okta_aruba-horiz.png Browse..

Upload Logo

App visibility:

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel Next

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

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

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

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

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	
<input type="text" value="Title"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.title"/> ▼	×
<input type="text" value="Department"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.department"/> ▼	×
<input type="text" value="Company"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.company"/> ▼	×
<input type="text" value="givenname"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.firstName"/> ▼	×
<input type="text" value="surname"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.lastName"/> ▼	×
<input type="text" value="email"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.email "/> ▼	×

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	
<input type="text" value="groups"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="Regex"/> ▼ <input type="text" value=".*"/>	×

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

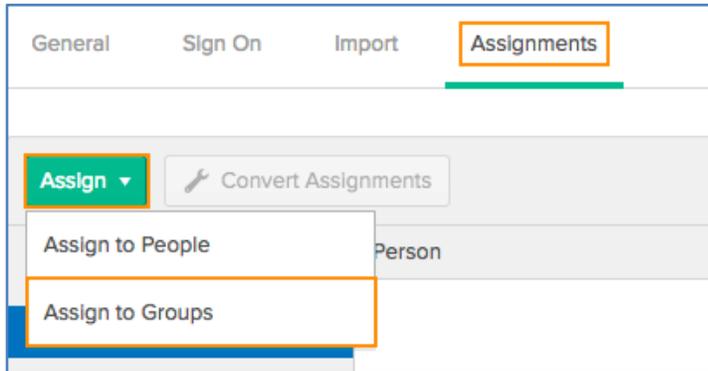
Any tips or additional comments?

Placeholder text

Previous Finish

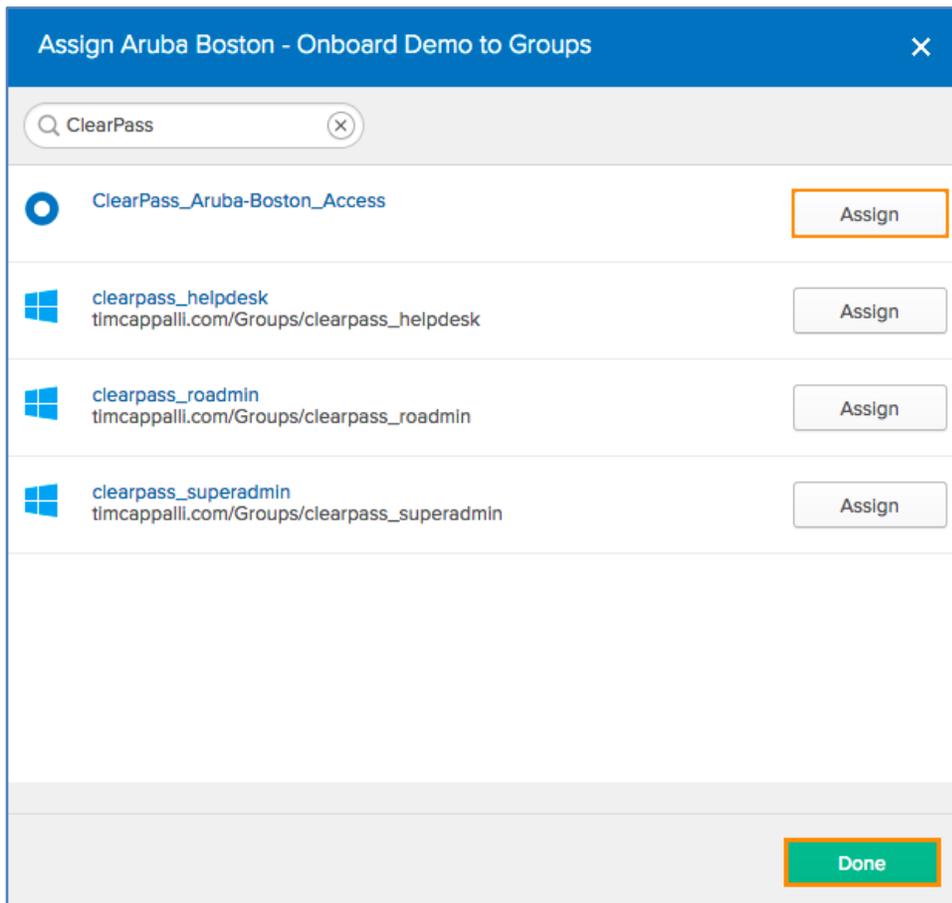
User Assignment

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



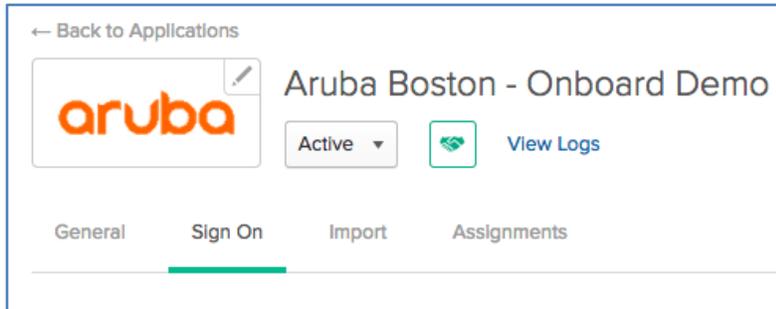
Search for the group(s) and then click **Assign**. Click **Done** when finished.

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

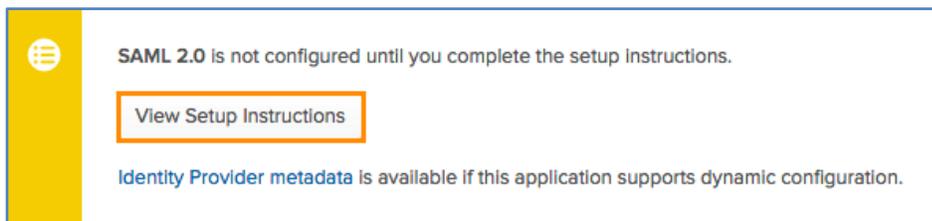


SAML Metadata

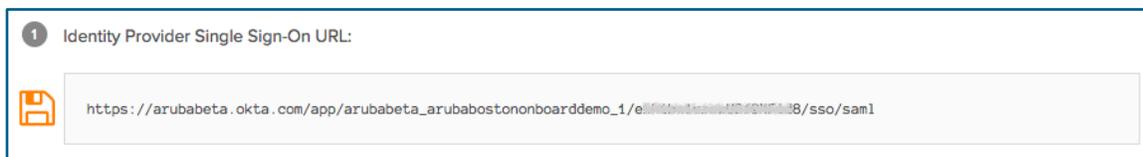
Now move over to the **Sign On** tab.



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)**.

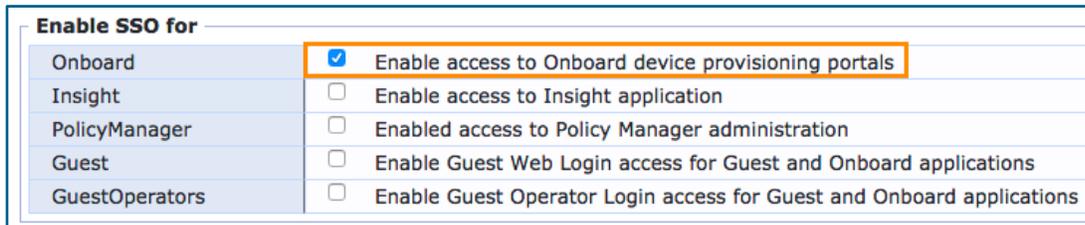
For **Identity Provider (IdP) URL**, enter in the **Login URL/SignOn URL** that was saved earlier from the Okta metadata page. The URL should look something like this:

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



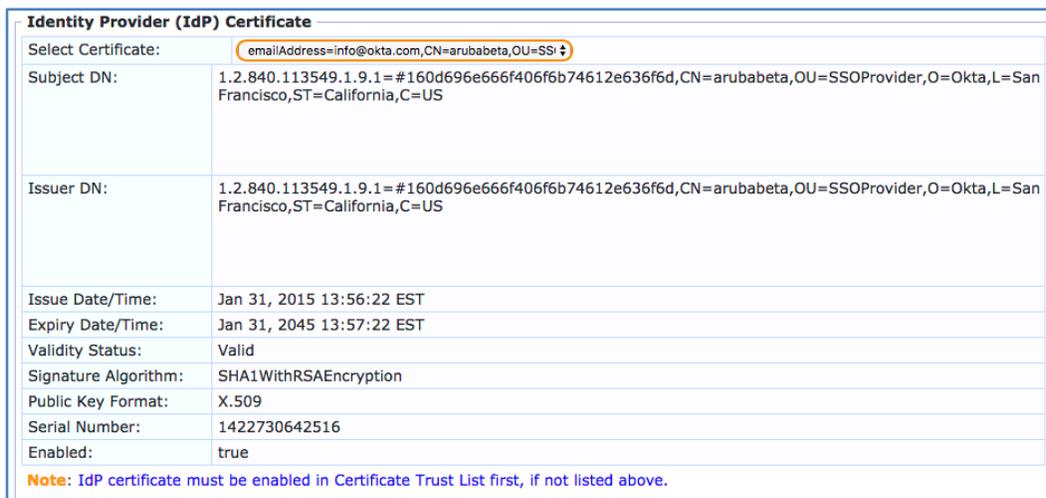
The screenshot shows the 'SAML IdP Configuration' tab selected. The 'Identity Provider (IdP) URL' field is highlighted with an orange border and contains the URL: `https://arubabeta.okta.com/app/arubabeta_arubabostonc`.

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



The screenshot shows the 'Enable SSO for' section. The 'Onboard' row is selected, and the checkbox for 'Enable access to Onboard device provisioning portals' is checked and highlighted with an orange border. Other options include 'Insight', 'PolicyManager', 'Guest', and 'GuestOperators', all with unchecked checkboxes.

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



The screenshot shows the 'Identity Provider (IdP) Certificate' section. The 'Select Certificate:' dropdown is highlighted with an orange border and shows the selected certificate: `emailAddress=info@okta.com,CN=arubabeta,OU=SS`. Below this, various certificate details are listed, including Subject DN, Issuer DN, Issue Date/Time, Expiry Date/Time, Validity Status, Signature Algorithm, Public Key Format, Serial Number, and Enabled status. A note at the bottom states: 'Note: IdP certificate must be enabled in Certificate Trust List first, if not listed above.'

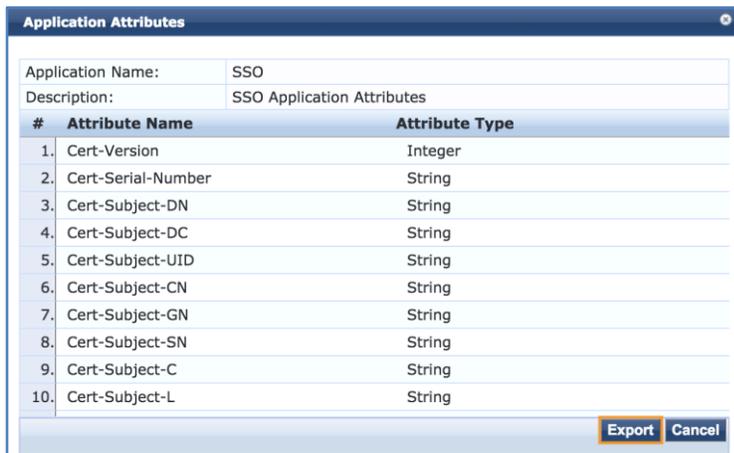
Click **Save** at the bottom.

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**.

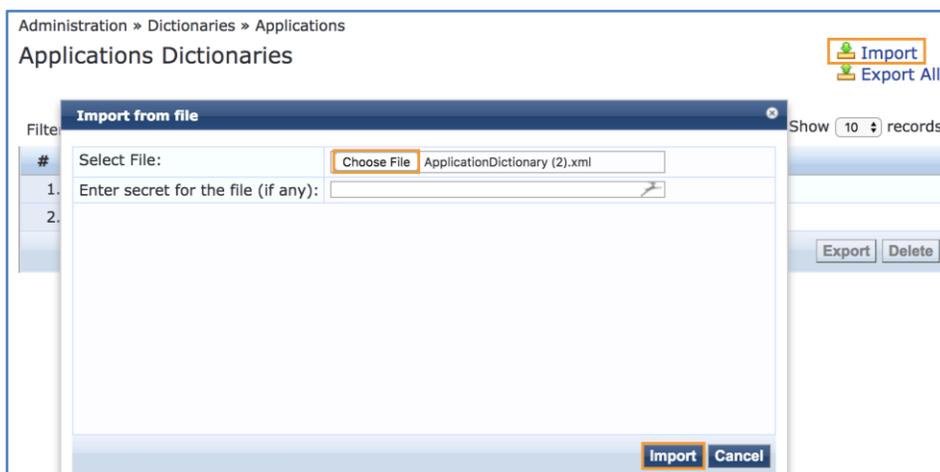


#	Attribute Name	Attribute Type
1.	Cert-Version	Integer
2.	Cert-Serial-Number	String
3.	Cert-Subject-DN	String
4.	Cert-Subject-DC	String
5.	Cert-Subject-UID	String
6.	Cert-Subject-CN	String
7.	Cert-Subject-GN	String
8.	Cert-Subject-SN	String
9.	Cert-Subject-C	String
10.	Cert-Subject-L	String

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.

```
<AppDictionaryAttributes 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: 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	

Service	Roles	Enforcement	Summary	
Type:	Aruba Application Authorization			
Name:	ONBOARD_PRE-AUTHZ_SAML			
Description:	Authorization Service for Applications			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
	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 a configuration interface with tabs for Service, Authorization, Roles, Enforcement, and Summary. The Enforcement tab is active. It contains a checkbox for "Use Cached Results" and another for "Use cached Roles and Posture attributes from previous sessions". Below this is a dropdown menu for "Enforcement Policy" currently set to "[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" configuration form with tabs for Enforcement, Rules, and Summary. The Enforcement tab is active. The "Name" field is set to "ONBOARD_PRE-AUTHZ_SAML". The "Description" field is empty. The "Enforcement Type" is set to "Application" (selected with a radio button). The "Default Profile" is set to "[Deny Application Access Profile]". There are "View Details" and "Modify" buttons, and a partially visible "Add new" button.

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" configuration form. The "Conditions" section is titled "Match ALL of the following conditions:" and contains a table with the following data:

Type	Name	Operator	Value
1. TIPS	Role	EQUALS	[User Authenticated]
2. Click to add...			

The "Enforcement Profiles" section shows a list of profile names with "[Allow Application Access Profile]" selected. There are "Move Up", "Move Down", and "Remove" buttons. A "--Select to Add--" dropdown is also visible. "Save" and "Cancel" buttons are at the bottom right.

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

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

Summary	Policy	Mapping Rules
Policy:		
Policy Name:	OKTA	
Description:		
Default Role:	[Other]	
Mapping Rules:		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Role Name	
1. (Application:SSO:groups CONTAINS Staff)	USER_STAFF	
2. (Application:SSO:groups CONTAINS Nurses)	USER_NURSE-FT	
3. 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
Enforcement:		
Name:	ONBOARD_PRE-AUTHZ_SAML-OKTA	
Description:		
Enforcement Type:	Application	
Default Profile:	[Deny Application Access Profile]	
Rules:		
Rules Evaluation Algorithm:	First applicable	
Conditions	Actions	
1. (Tips:Role EQUALS USER_CONTRACTOR)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_1M, ONBOARD_MAX-DEVICES_1	
2. (Tips:Role EQUALS USER_DOC-ROAM)	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_1M, ONBOARD_MAX-DEVICES_3	
3. (Tips:Role MATCHES_ANY USER_DOC-FT USER_NURSE-FT USER_STAFF)	[Allow Application Access Profile], ONBOARD_MAX-DEVICES_5	
4. (Tips:Role EQUALS [User Authenticated])	[Allow Application Access Profile], ONBOARD_SESSION-TIMEOUT_3M, ONBOARD_MAX-DEVICES_3	

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

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

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

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

NAD Whitelist

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

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

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

Sample Request

Request Details

Summary Input Output

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

Policies Used -

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

Showing 1 of 1-26 records

Change Status Show Configuration Export Show Logs Close

Request Details

Summary Input Output

Computed Attributes

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

Showing 1 of 1-26 records

Change Status Show Configuration Export Show Logs Close

Additional Resources

Technologies

[RFC 6749: The OAuth 2.0 Authorization Framework](#)

[RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage](#)

[SAML 2.0 OASIS Standard](#)

ClearPass

[ClearPass Policy Manager 6.7 User Guide](#)

[ClearPass Onboard 6.7 User Guide](#)

[TechNote: SAML Configuration Guide v1.5](#)

[TechNote: ClearPass REST APIs](#)

Microsoft Azure Active Directory

[Azure Active Directory Documentation Landing](#)

[Azure Active Directory + SAML](#)

[Azure Active Directory + OpenID Connect](#)

Google Cloud Identity

[G Suite Administrator Help Center](#)

[Google Secure LDAP service](#)

Okta

[Beginner's Guide to SAML](#)

[Single Sign-On](#)

[Adaptive MFA](#)

[Firewall Whitelisting](#)

aruba

a Hewlett Packard
Enterprise company

www.arubanetworks.com

3333 Scott Blvd

Santa Clara, CA 95054

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

Fax 408.227.4550

© 2018 Hewlett Packard Enterprise Development LP. All Rights Reserved.