

SOLUTION GUIDE

# Integrate Okta with HPE GreenLake

## SINGLE SIGN-ON CONFIGURATION

Version	Date	Modified By	Notes
2022-12	21 Dec 2022	Matt Sutherland	Initial Release
2023-06	07 Jun 2023	Matt Sutherland	Fixed links to web-based documentation

## TABLE OF CONTENTS

Introduction .....	3
Prerequisite .....	3
Setting up Okta .....	3
HPE GreenLake SSO Configuration .....	7
Role Based Authorization .....	12
Fast Sign-in to an HPE GreenLake Application .....	16

## Introduction

This solution guide will provide instructions to integrate HPE GreenLake with Okta for single sign-on.

For best practice configuration within Okta please refer to Okta documentation.

The latest HPE GreenLake Edge-to-Cloud Platform User Guide can be found here:  
[https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en\\_us](https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us)

## Prerequisite

Prerequisite:

- HPE GreenLake Account
- Okta Account
- A unique personalised/company Domain with email

An administrator account must exist in HPE GreenLake with the domain for which you would like to establish single sign-on. Invite a new user if your initial administrator is from a different domain.

Enable user federation across HPE GreenLake services and single sign-on for users with claimed-domain accounts. Users without a claimed-domain account can still sign in using their username and password against the local user database.

## Setting up Okta

1. Login to the Okta dashboard for your organisation
2. Select Applications from the left-hand navigation
3. Select Create App Integration
4. Choose SAML 2.0 as the sign-in method, Select Next
5. Assign an App name and optionally add a meaningful logo

### Create SAML Integration

1 General Settings	2 Configure SAML	3 Feedback
--------------------	------------------	------------

**1 General Settings**

App name

App logo (optional)   

App visibility  Do not display application icon to users

[Cancel](#) [Next](#)

## 6. Configure the SAML General Settings:

1 General Settings      2 Configure SAML      3 Feedback

**A SAML Settings**

**General**

Single sign-on URL <sup>?</sup>   
 Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) <sup>?</sup>

Default RelayState <sup>?</sup>   
If no value is set, a blank RelayState is sent

Name ID format <sup>?</sup>

Application username <sup>?</sup>

Update application username on

[Show Advanced Settings](#)

### What does this form do?

This form generates the XML needed for the app's SAML request.

### Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Single sign-on URL: <https://sso.common.cloud.hpe.com/sp/ACS.saml2>

Audience URI (SP Entity ID): <https://sso.common.cloud.hpe.com>

Name ID format: EmailAddress

## 7. Configure the SAML Attribute Statements

**Attribute Statements (optional)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="NameId"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.email"/>
<input type="text" value="firstName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.firstName"/> <span style="float: right;">✕</span>
<input style="border: 2px solid #007bff;" type="text" value="lastName"/>	<input type="text" value="Unspecified"/>	<input type="text" value="user.lastName"/> <span style="float: right;">✕</span>
<input type="text" value="hpe_css_attribute"/>	<input type="text" value="Unspecified"/>	<input type="text" value="appuser.hpe_css_attribute"/> <span style="float: right;">✕</span>

[Add Another](#)

---

**Group Attribute Statements (optional)**

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>

[Add Another](#)

Name	Value
NameId	user.email
firstName	user.firstName
lastName	user.lastName
hpe_css_attribute	appuser.hpe_css_attribute

8. Select Next
9. Answer the final feedback question for Okta Support and Select Finish
10. After the Application integration workflow has finished Select View SAML setup instructions

### SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

[View SAML setup instructions](#)

11. Copy the text from the Optional IDP metadata field at the bottom and save it into an XML file

12. Here is an example of the resulting SAML Settings:

**SAML Settings** [Edit](#)

**GENERAL**

Single Sign On URL https://sso.common.cloud.hpe.com/sp/ACS.saml2

Recipient URL https://sso.common.cloud.hpe.com/sp/ACS.saml2

Destination URL https://sso.common.cloud.hpe.com/sp/ACS.saml2

Audience Restriction https://sso.common.cloud.hpe.com

Default Relay State

Name ID Format EmailAddress

Response Signed

Assertion Signature Signed

Signature Algorithm RSA\_SHA256

Digest Algorithm SHA256

Assertion Encryption Unencrypted

SAML Single Logout Disabled

SAML Signed Request Disabled

authnContextClassRef PasswordProtectedTransport

Honor Force Authentication Yes

Assertion Inline Hook None (disabled)

SAML Issuer ID http://www.okta.com/\${org.externalKey}

**ATTRIBUTE STATEMENTS**

Name	Name Format	Value
namelid	Unspecified	user.email
firstName	Unspecified	user.firstName
lastName	Unspecified	user.lastName
hpe_css_attribute	Unspecified	appuser.hpe_css_attribute

**GROUP ATTRIBUTE STATEMENTS**

Name	Name Format	Filter
------	-------------	--------

## HPE GreenLake SSO Configuration

1. Login to HPE GreenLake
2. Click Manage from the top navigation
3. Click the Authentication tile



Begin providing access to your users by setting up a SAML connection.

**Set Up SAML Connection**

4. Click Set Up SAML Connection and enter the domain you would like to claim.

Add SSO Connection

### Claim a Domain

Enter a domain to create and manage an SSO connection. There must be at least one verified user belonging to the domain.

Organization Domain Name

Public domain (e.g., Gmail, Outlook, Yahoo, etc.) cannot be used to configure SSO.

**Cancel** **Continue**

**Note:** You must be logged in as a user from the domain you are claiming. HPE GreenLake does not support adding hpe.com, arubanetworks.com and other free public domain names for public cloud deployments, such as gmail.com, yahoo.com or facebook.com for SAML authorization profiles.

## 5. There are four steps in the SSO setup process

Step 1 of 4

### Add Identity Provider Details

Add SSO configuration details for your service provider. Need help getting set up? Visit the [SAML SSO Setup Guide](#).

Select a Configuration Method\*

Metadata File  
 Metadata URL  
 Manual (Enter X.509 Certificate Details)

IdP Metadata File\*

**Upload Metadata File**

Maximum File Size: 1 MB

Entity ID\*

Domain Login URL\*

Domain Logout URL\*

X.509 Signing Certificate\*

**Next →**

## 6. Upload the Metadata XML file created in the Okta setup process

Step 1 of 4

### Add Identity Provider Details

Add SSO configuration details for your service provider. Need help getting set up? Visit the [SAML SSO Setup Guide](#).

Select a Configuration Method\*

Metadata File  
 Metadata URL  
 Manual (Enter X.509 Certificate Details)

IdP Metadata File\*

**hpe-greenlake\_okta.xml** (2.2 KB)

Maximum File Size: 1 MB

Entity ID\*

http://www.okta.com/exkAwIBAgko6nMmt5A0

Domain Login URL\*

https://AwIBAgI/mt5d.okta.com/app/A0AwIBAgI

Domain Logout URL\*

https://not-applicable.com

X.509 Signing Certificate\*

MIIDqDCCApCgAwIBAgIGAYT0xgayMA0

**Next →**

## 7. Select Next

- 8. Configure SAML Settings:  
Email Address: NameId  
HPE GreenLake Attribute: hpe\_css\_attribute  
First Name: firstName  
Last Name: lastName  
Idle Session Timeout: set as required

Step 2 of 4

## Configure Settings

Configure SAML attributes and manage idle session timeout settings.

## Map SAML Attributes

Get the following fields from your identity provider and map them to the relevant fields below. Learn more about the [mapping attributes](#).

### Required Attributes

HPE GreenLake Attribute

Email Address

SAML Attribute Name\*

NameId

HPE GreenLake Attribute

hpe\_css\_attribute

### Optional Attributes

HPE GreenLake Attributes

First Name

SAML Attribute Name

firstName

Last Name

lastName

## Manage Idle Session Timeout

Specify the amount of time a user can be inactive before a session ends.

Idle Session Time(Minutes)

Time is in minutes, Idle time cannot exceed 1,440 minutes(24 hours).

360

Next →

- 9. Select Next

10. Configure a recovery user password. The Recovery User Email is auto generated and cannot be changed. Be sure to write this down along with the Recovery User Password in a safe, secure place. You can alternatively specify a Point of Contact Email address which is used to regain account access if the Recovery User Password is forgotten.

Step 3 of 4

## Create a Recovery User

Create a recovery user to access your account in the event SSO fails. Once SSO is configured users will no longer be able to log in with their email and password.

### Recovery User

Enable Recovery User

Recovery User Email

This email is auto-generated and cannot be changed.

1b9b09d0b11ecb23dda25c6ddbc41@wifi.academy

Recovery User Password\*

.....

Show Password

Point of Contact Email\*

This will be used to regain access to your account if you forget your password.

vip@wifi.academy

Next →

11. Select Next
12. Review the settings and Select Finish
13. Select Download the Metadata file

### SSO Setup Complete

Your SSO domain is ready to go! You can edit details at any time after exiting the wizard.



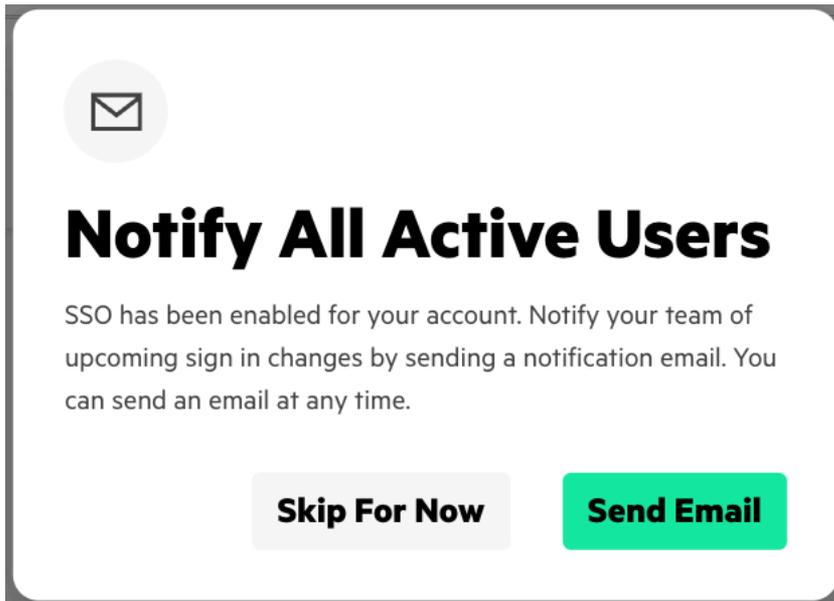
### Download Metadata

Download the metadata file and import into your Identity Provider (IdP).  
You can do this at any time from your connection's detail page.

Download Metadata File

Exit

14. Select Exit
15. If you have existing users configured in HPE GreenLake you can send them an email in the next step, otherwise Select Skip For Now



16. This concludes the configuration of HPE GreenLake configuration. Your domain should now be visible under Authentication

## Authentication

Set an authentication method that meets your security requirements.

### SAML

Add Domain

Enable user federation across HPE GreenLake services and single sign-on for users with claimed-domain accounts. Users without a claimed-domain account can still sign in using their username and password against the local user database.



17. Select the menu icon on your domain and select View SAML Attribute. Data within this popup will be useful for the role-based configuration within Okta. See: [https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en\\_us&page=GUID-237A2D36-D5D3-4514-915F-42B2ACDF825C.html](https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us&page=GUID-237A2D36-D5D3-4514-915F-42B2ACDF825C.html)

## Role Based Authorization

HPE GreenLake supports role-based access control which allows you to define granular access levels to users of HPE GreenLake and the available applications, such as Aruba Central.

The following configuration allows you to configure selectable roles within Okta which define the access available to each user. In the Attribute members field you can create multiple Roles to assign to users.

1. Login to the Okta dashboard for your organisation
2. Select Directory from the left-hand navigation
3. Select Profile Editor
4. Select the Profile representing your HPE-GreenLake User
5. Select + Add Attribute
6. Configure the attribute with the following information

Field	Value
Data type	String
Display name	Role
Variable name	hpe_css_attribute
Description	HPE GreenLake Role
Enum	true
Attribute required	True
User permission	Read Only

7. In the Attribute members you can define multiple roles where the value represents the HPE GreenLake SAML attribute defined at [https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en\\_us&page=GUID-237A2D36-D5D3-4514-915F-42B2ACDF825C.html](https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us&page=GUID-237A2D36-D5D3-4514-915F-42B2ACDF825C.html)

The format is:

```
{version}#{pcid}:{app cid}:{role_name}:{scope_group_names}:{ALL_SCOPES}
```

8. This attribute needs to be edited to contain information found in the SAML Attribute Data for your domain in step 17 of the HPE GreenLake configuration. The following table shows an example of how to map the attribute to the Aruba Central Administrator role:

Attribute Field	Value
Version	version_1
pcid	HPE GreenLake platform Customer ID
app cid	HPE GreenLake platform ID
role_name	HPE GreenLake Role
scope_group_names	Aruba Central Application ID
ALL_SCOPES	Set appropriate scopes (or leave as ALL_SCOPES)

Review the following page for any updates to the SAML syntax:

[https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en\\_us&page=GUID-1F4C67DE-EE99-49D9-B3B4-F63AE5AAB480.html](https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us&page=GUID-1F4C67DE-EE99-49D9-B3B4-F63AE5AAB480.html)

Some examples of the attribute syntax required to define different roles can be found here:

[https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en\\_us&page=GUID-DC6E44BD-890A-4546-B08B-15748D8FFF1D.html](https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us&page=GUID-DC6E44BD-890A-4546-B08B-15748D8FFF1D.html)

9. Here is an example of three roles for Aruba Central with matching HPE GreenLake roles:

**Aruba Central Administrator**

version\_1#8ecxb1d09a0c11edd83dda33c1ddbc01:00000000-0000-0000-0000-000000000000:Account Administrator:ALL\_SCOPES:888ca888-888b-4ce1-92a9-ex8964888098:Aruba Central Administrator:ALL\_SCOPES

**Aruba Central Operator**

version\_1#8ecxb1d09a0c11edd83dda33c1ddbc01:00000000-0000-0000-0000-000000000000:Operator:ALL\_SCOPES: 888ca888-888b-4ce1-92a9-ex8964888098:Aruba Central Operator:ALL\_SCOPES

**Aruba Central Read-Only**

version\_1#8ecxb1d09a0c11edd83dda33c1ddbc01:00000000-0000-0000-0000-000000000000:Operator:ALL\_SCOPES: 888ca888-888b-4ce1-92a9-ex8964888098:Aruba Central View Only:ALL\_SCOPES

10. The Add Attribute form should look like this after you have completed entering the information:

### Add Attribute

\* Local app attributes are only stored on Okta and not created in HPE-GreenLake. Use local attributes if you plan to add the attribute to HPE-GreenLake or only want to store the mapped value in Okta.

! We found some errors. Please review the form and make corrections.

Data type	<input type="text" value="string"/>												
Display name	<input type="text" value="Role"/>												
Variable name	<input type="text" value="hpe_css_attribute"/>												
Description	<input type="text" value="HPE GreenLake Role"/>												
Enum	<input checked="" type="checkbox"/> Define enumerated list of values												
Attribute members	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 60%;">Display name</th> <th style="width: 30%;">Value</th> <th style="width: 10%;"></th> </tr> </thead> <tbody> <tr> <td>Aruba Central Adm</td> <td>version_1#8bcdbe</td> <td style="text-align: center;">✕</td> </tr> <tr> <td>Aruba Central Ope</td> <td>version_1#8bcdbe</td> <td style="text-align: center;">✕</td> </tr> <tr> <td>Aruba Central Rea</td> <td>version_1#8bcdbe</td> <td style="text-align: center;">✕</td> </tr> </tbody> </table> <p style="text-align: center; margin-top: 5px;"><a href="#" style="border: 1px solid #007bff; padding: 2px 5px; color: #007bff;">+ Add Another</a></p>	Display name	Value		Aruba Central Adm	version_1#8bcdbe	✕	Aruba Central Ope	version_1#8bcdbe	✕	Aruba Central Rea	version_1#8bcdbe	✕
Display name	Value												
Aruba Central Adm	version_1#8bcdbe	✕											
Aruba Central Ope	version_1#8bcdbe	✕											
Aruba Central Rea	version_1#8bcdbe	✕											
Attribute length	<input type="text" value="Between"/> <input type="text" value="min"/> and <input type="text" value="max"/>												
Attribute required	<input type="checkbox"/> Yes												
Scope	<input type="checkbox"/> User personal												
User permission	<input type="radio"/> Hide <small>Users cannot view the attribute. Select this option to hide sensitive attributes. For example, salary information</small> <input checked="" type="radio"/> Read Only <small>Users can view the attribute, but attribute properties cannot be modified. Select this option to prevent attribute properties from changing. For example, a title</small> <input type="radio"/> Read-Write <small>Users can view the attribute and edit attribute properties. Select this option to allow users to update attribute properties. For example, a phone number</small>												
<input type="button" value="Save"/> <input type="button" value="Save and Add Another"/> <input type="button" value="Cancel"/>													

## 11. Select Save

Note: The Okta interface enumerates in such a way where the Display Value names are difficult to read.

Further granularity in Okta's profile mapping is possible but is outside the scope of this document. Please refer to Okta documentation.

**Role**

Data type: string

Display name:

Variable name: dev39318555\_gicpwifacademy\_1hpe\_ccs\_attribute

Description:

Enum:  Define enumerated list of values

Attribute members:

DisplayValue	name
<input type="checkbox"/>	version_1#8bcd9b09d0b11ecb23dda25c6d41:00000000-0000-0000-0000-000000000000:Account Administrator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central Administrator:ALL_SCOPES
<input type="checkbox"/>	version_1#8bcd9b09d0b11ecb23dda25c6d41:00000000-0000-0000-0000-000000000000:Operator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central Operator:ALL_SCOPES
<input type="checkbox"/>	version_1#8bcd9b09d0b11ecb23dda25c6d41:00000000-0000-0000-0000-000000000000:Operator:ALL_SCOPES:683da368-66cb-4ee7-90a9-ec1964768092:Aruba Central View Only:ALL_SCOPES

[+ Add Another](#)

Attribute length: Between  and

Attribute required:  Yes

Scope: None

Mutability: READ\_WRITE

[Save Attribute](#) [Cancel](#)

12. To assign one of the new roles to a user, select Directory from the left-hand navigation

13. Select People

14. Select a user for whom you wish to edit the HPE GreenLake Role

15. Select Assign Application

16. Select Assign next to your HPE-GreenLake application

**Assign Applications** ×

---


HPE-GreenLake
[Assign](#)

17. Select the appropriate Role from the user from the drop-down menu

The screenshot shows a dialog box titled "Assign Applications" with a close button (X) in the top right corner. Below the title, there are two input fields. The first is labeled "User Name" and contains the text "r1@wifi.academy". The second is labeled "Role" and has a dropdown menu open. The dropdown menu lists four options: "Aruba Central Admi...", "Aruba Central Administrator", "Aruba Central Operator", and "Aruba Central Read-Only". To the right of the dropdown menu, there are two buttons: "Save" and "Cancel".

18. Select Save and Go Back

19. Select Done

20. The user should now be able to login via the HPE GreenLake SSO sign-in workflow

The screenshot shows the Okta sign-in page. At the top, it says "Connecting to Hewlett Packard Enterprise" with the HPE logo. Below that, it says "Sign in with your WiFi Academy account to access HPE-GreenLake". The Okta logo is prominently displayed in the center. Below the logo, there is a "Sign In" section. It contains a "Username" field with the text "r1@wifi.academy", a "Password" field with masked characters and a visibility toggle, a "Keep me signed in" checkbox, and a blue "Sign in" button. At the bottom of the sign-in section, there are links for "Forgot password?" and "Help".

## Fast Sign-in to an HPE GreenLake Application

It may be convenient to have rapid access to an application within HPE GreenLake, such as Aruba Central. It is possible to configure faster access to a particular application by setting the Default Relay State in the Okta SAML settings and then using the Okta App Embed Link.

With this configuration you will be able to browse to the Okta Embed Link, sign-in and then be forwarded straight to Aruba Central.

1. Login to the Okta dashboard for your organisation
2. Select Applications from the left-hand navigation then select Applications once again from the expanded menu
3. Select the HPE-GreenLake application from the list
4. Select General
5. Select Edit in the SAML Settings info panel
6. Select Next at Step 1
7. Edit the Default RelayState field to include the portal URL for your Aruba Central region. find the domain name here (include https:// in front of the domain name):  
[https://www.arubanetworks.com/techdocs/central/latest/content/nms/device-mgmt/communication\\_ports.htm](https://www.arubanetworks.com/techdocs/central/latest/content/nms/device-mgmt/communication_ports.htm)

**A SAML Settings**

**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 ?

8. Select Next
9. Select Finish on the Okta Feedback step if applicable
10. Select General again and scroll to the bottom of the page
11. Copy the App Embed Link
12. Users should be able to login to the Okta portal using this Embed Link and be forwarded directly to Aruba Central after login if they have been assigned access.

