Configure Okta Remote Authentication for Silver Peak Unity Orchestrator

Silver Peak Unity Orchestrator supports remote authentication via the OAuth 2.0 framework. This document provides information about how to register Orchestrator with Okta and configure Orchestrator to enable authentication via Okta.

Add an Orchestrator App in Okta

1. Sign in to your Okta organization as a user with administrative privileges.
2. From the dashboard, click **Applications** on the header menu, then click **Add Application**.
3. Select **Web** as the platform, then click **Next**.
4. Enter a name for your application (for example, Silver Peak Unity Orchestrator).
5. For the login redirect URI, specify the Orchestrator endpoint to which the user will be redirected after successful authentication:
   https://<*Orch_domain_or_IP_address*>/gms/rest/authentication/oauth/redirect
6. Under allowed grant types, select **Refresh Token**.

   NOTE: The **Authorization Code** option is already selected, and you cannot clear it.

7. Click **Done**.

   NOTE: Copy the Client ID and Client Secret for use later when setting up the OAuth server in Orchestrator.

8. Use the Assignments tab to assign users to the Orchestrator app.

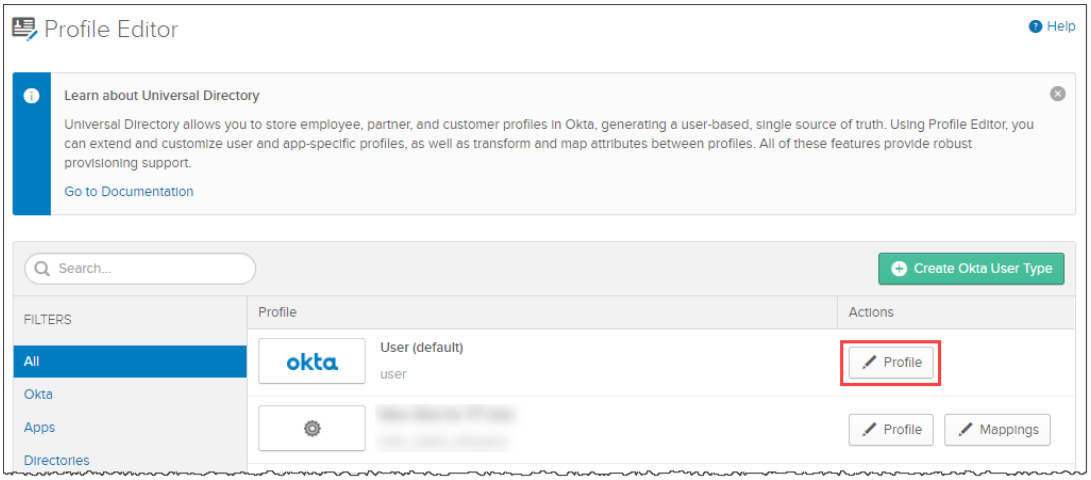
Add Profile Attributes in Okta

An Okta OAuth server supports Role Based Access Control (RBAC) and appliance access groups (AAG), which are sent as claims to Orchestrator. Later in this document, you will add two claims to the Okta authorization server. The RBAC or AAG value is applied to a user profile attribute in Okta and sent to Orchestrator as a claim.

In this section, we will create two new profile attributes called RBAC and AppGroup.

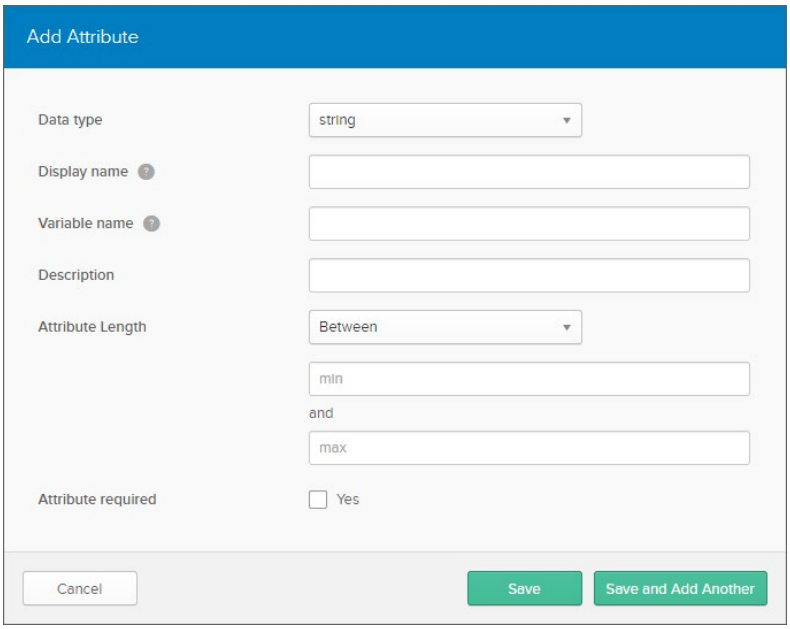
1. From the Okta dashboard, move your cursor over **Users** on the header menu, then click **Profile Editor**.

   The Profile Editor appears.



2. Click the edit profile button next to the default Okta user profile.
3. At the top of the attributes table, click **Add Attribute**.

   The Add Attribute dialog appears.



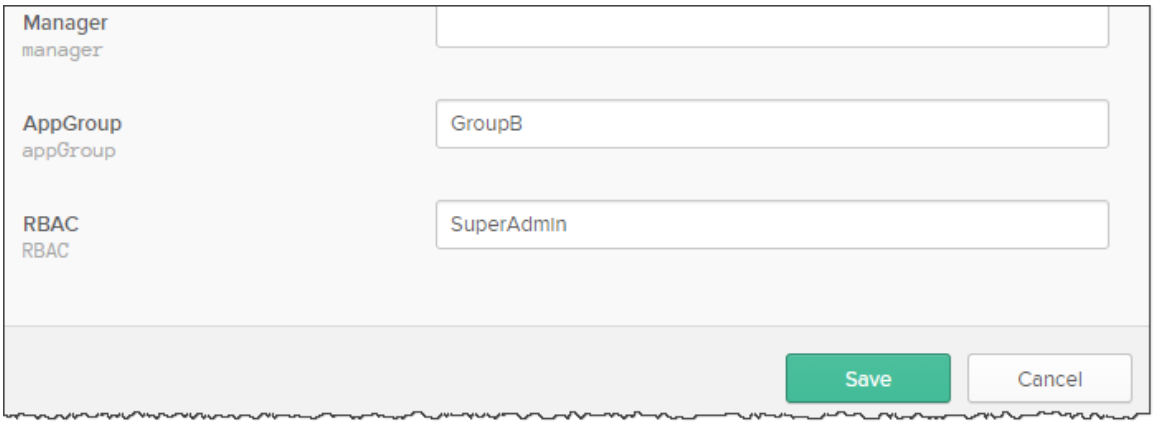
4. Enter the following details to create the RBAC attribute:

Field	Value
Data type	string
Display name	RBAC
Variable name	RBAC
Description	Add an optional description for the attribute.
Attribute length	Set to **Between 0** and **255**.
Attribute required	Do not select this option.

5. Click **Save and Add Another**.
6. Enter the following details to create the AppGroup attribute:

Field	Value
Data type	string
Display name	AppGroup
Variable name	AppGroup
Description	Add an optional description for the attribute.
Attribute length	Set to **Between 0** and **255**.
Attribute required	Do not select this option.

7. Click **Save**.
8. For each Okta user who has access to Orchestrator, you can add the RBAC roles and appliance access group values to the new custom attributes.

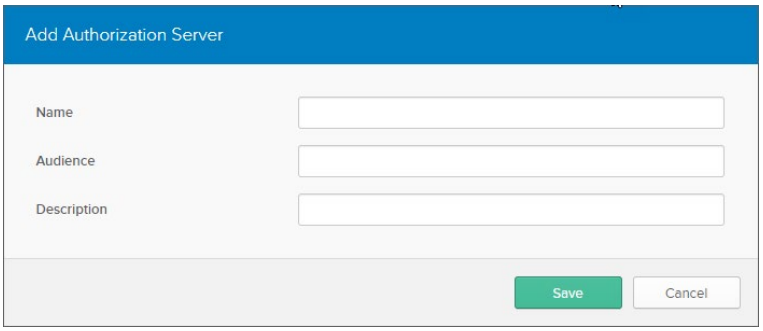


Configure an Authorization Server in Okta

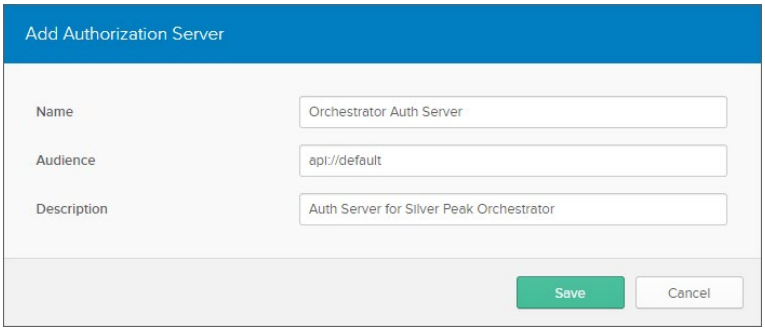
An authorization server is used to apply access policies, and each server has a unique issuer URI and its own signing key for tokens to keep a proper boundary between security domains.

1. Click **API** on the header menu, then click **Authorization Servers**.
2. Click **Add Authorization Server**.

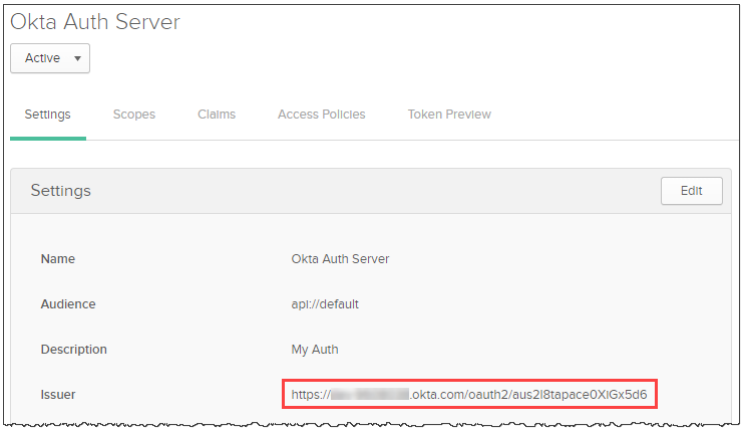
   The Add Authorization Server dialog appears.



3. Enter a name for the server.
4. For the audience, enter the following: **api://default**
5. Use the description field if you want to add more detail.



6. Click **Save** and copy the Issuer URI for use when configuring Orchestrator.

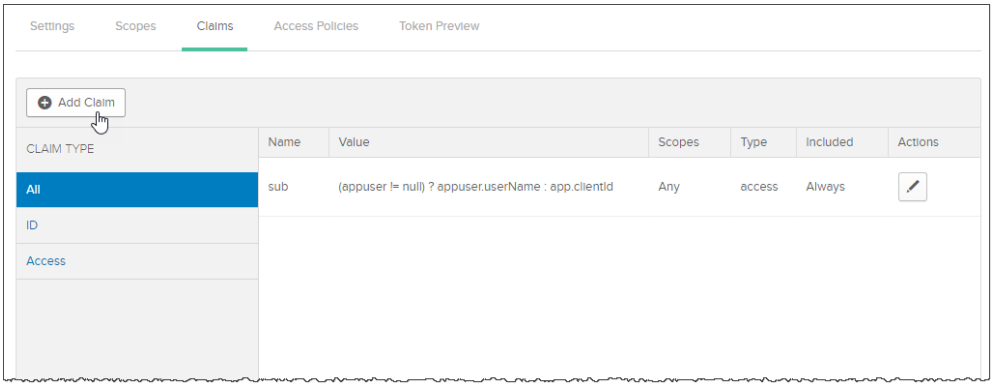


7. Proceed to the next section to add claims to the new authorization server. These claims will be used to associate RBAC roles and appliance access groups with users.

Add Claims for RBAC Roles and Appliance Access Groups in Okta

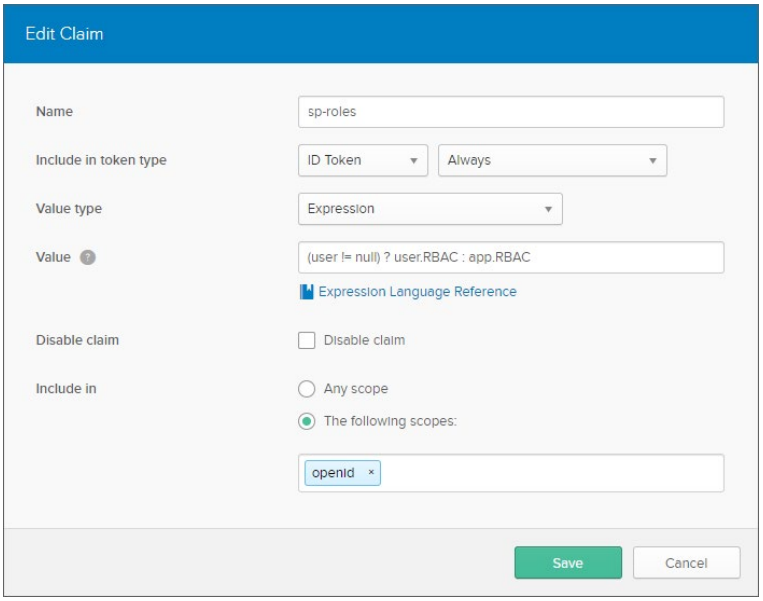
Claims are simply additional statements about the user, such as name, role, or email address.

1. In the list of authorization servers, click the name of the server you just created.
2. Click the **Claims** menu.



3. Click **Add Claim** and enter the following details to add the RBAC claim:

Field	**Value**
Name	sp-roles
Include in token type	ID token / Always
Value type	Expression
Value	(user != null) ? user.RBAC : app.RBAC
Disable claim	Do not select this option.
Include in	Select **The following scopes** and enter/select the **openid** scope.

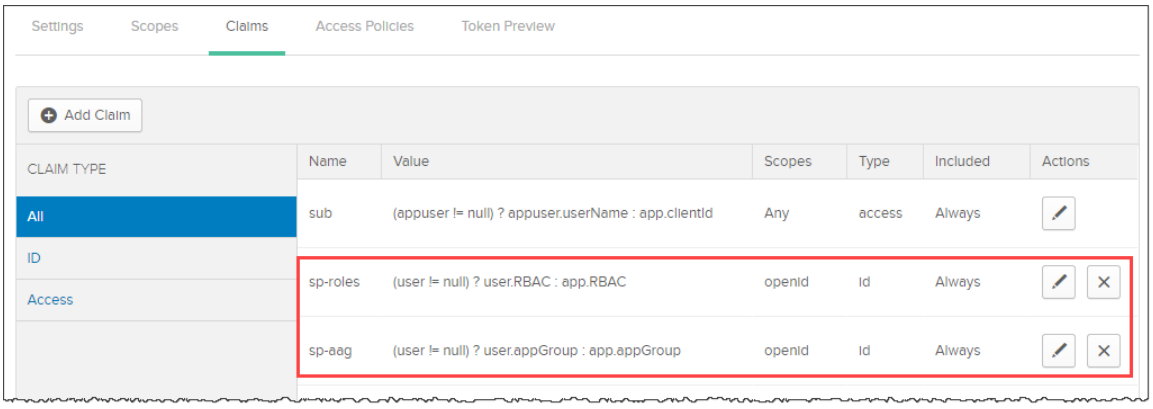


4. Click **Save**.

5. Click **Add Claim** again and enter the following details to add the appliance access group claim:

Field	**Value**
Name	sp-aag
Include in token type	ID token / Always
Value type	Expression
Value	(user != null) ? user.appGroup : app.appGroup
Disable claim	Do not select this option.
Include in	Select **The following scopes** and enter/select the **openid** scope.

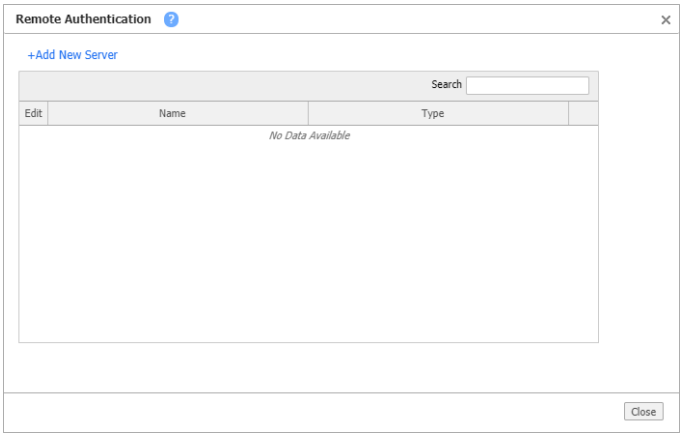
When finished, you should have two new claims as shown below:



Configure Remote Authentication in Orchestrator

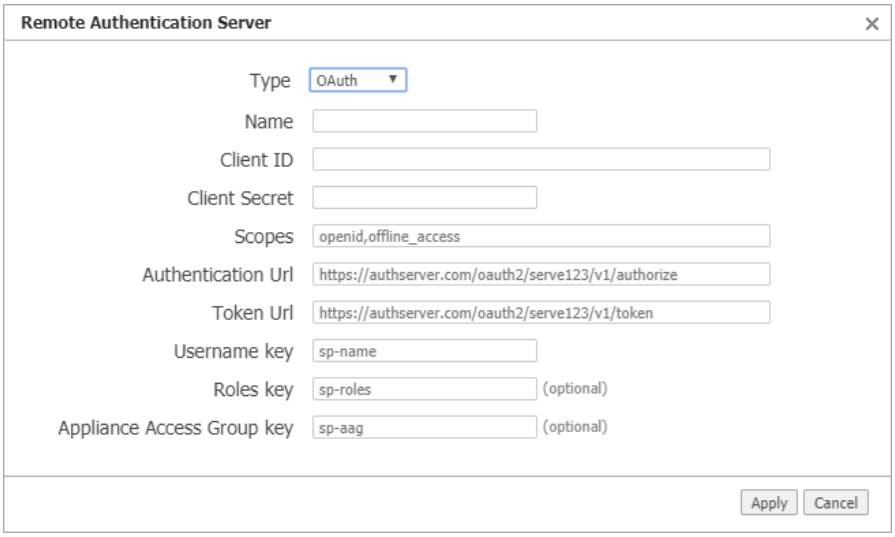
1. Log in to Orchestrator as an administrative (read-write) user.
2. Click *Orchestrator* > *Orchestrator Server* > *Users & Authentication* > *Authentication*.

   The Remote Authentication dialog appears.



3. Click **+Add New Server**.

   The Remote Authentication Server dialog appears.



4. Fill in the available fields for the new server, as follows:

Field	Value
Type	**OAuth**
Name	Enter a name to identify the server. This name will be displayed in a button on the Orchestrator login page as an alternative method of authentication.
Client ID	Paste the client ID for the Orchestrator application that you created in Okta.
Client Secret	Paste the client secret for the Orchestrator application that you created in Okta.
Scopes	**openid, email**
Authentication URL	This is the Issuer URL (from the authorization server details) with the authentication request path appended. For example: https://company.okta.com/oauth2/aus28aaeXG56/v1/authorize
Token URL	This is the Issuer URL (from the authorization server details) with the token path appended. For example: https://company.okta.com/oauth2/aus28aaeXG56/v1/token
Username key	This is the OAuth attribute to be sent as the username. Use **email** if username is an email address. If any other key is used, ensure that it is mapped to the correct scope in Okta.
Roles key	**sp-roles**
Appliance Access Group key	**sp-aag**
Default role	If you are using Orchestrator v9, you can select a default RBAC role if one is not assigned using the roles key.

5. Click **Apply**, and then click **Close** in the Remote Authentication dialog.

   Your Orchestrator login screen should now have a button to log in with Okta.

Revision History

Jan 12, 2021 Rev A: Initial document revision.