Configuring Provisioning for Okta

This guide provides the steps required to configure provisioning for Okta and includes the following sections:

Features

The following provisioning features are supported:

- **Push new users**
  New users created through Okta are also created in OpsRamp.
- **Push user deactivation**
  Deactivating the user or disabling the user's access to the application through Okta deactivates the user in OpsRamp.
- **Push profile updates**
  Updates made to the user's profile through Okta are pushed to OpsRamp.
- **Group Push**
  Groups and their members created through Okta are pushed to OpsRamp.

Requirements

Before you configure provisioning, see Okta Basic Configuration.

OpsRamp configuration

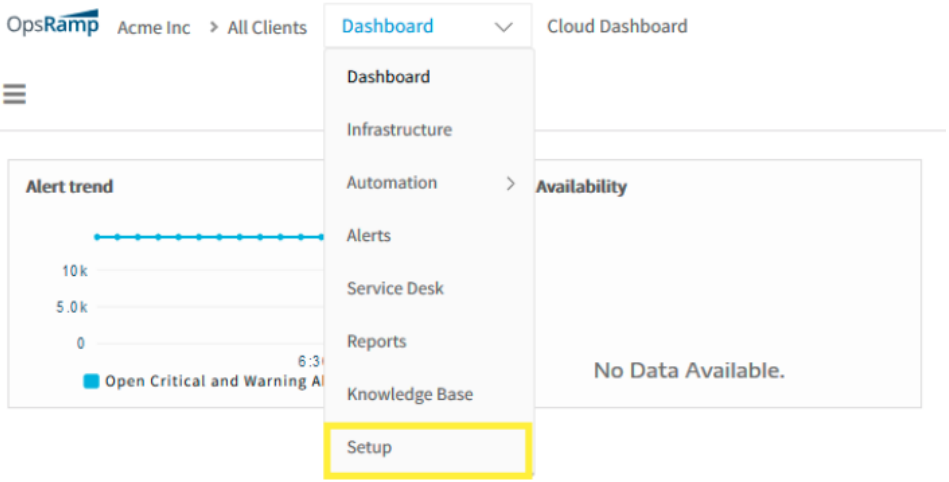
Configuration involves:

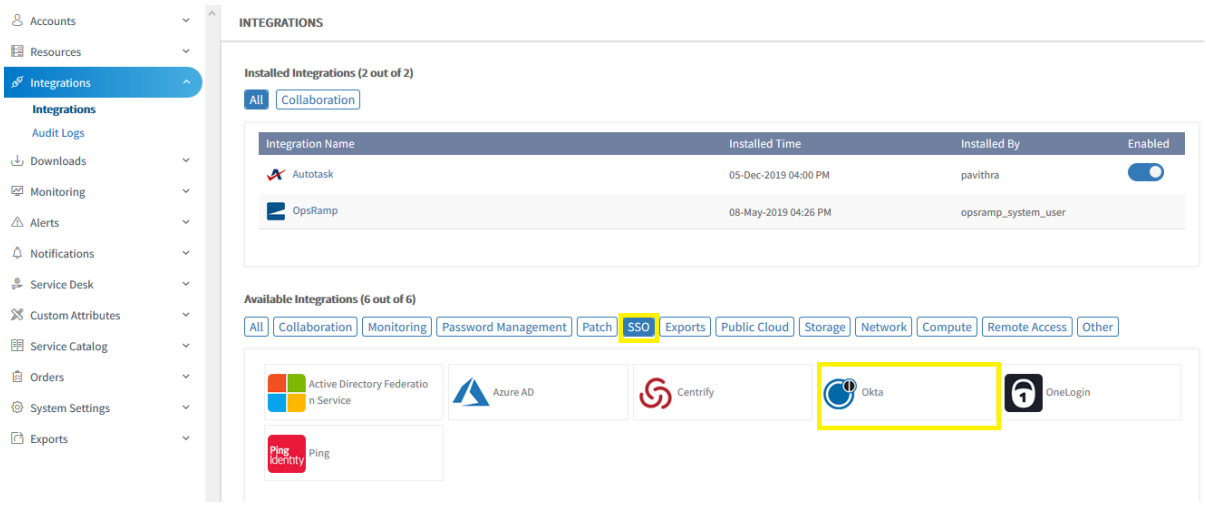
1. Installing the Okta integration. Note: During installation, a URL and token are generated. The URL and token are used for Okta configuration.
2. Configuring the integration.

Step 1: Install the integration

To install:

1. From **All Clients**, select a client.
2. Go to **Setup > Integrations > Integrations**.
3. From **Available Integrations**, select **SSO > Okta**.
4. Click **Install**.

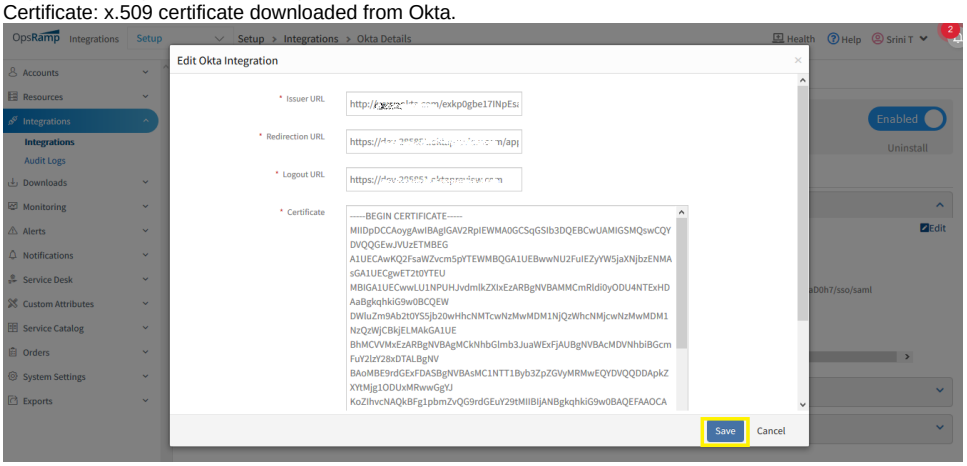




Step 2: Configure the integration

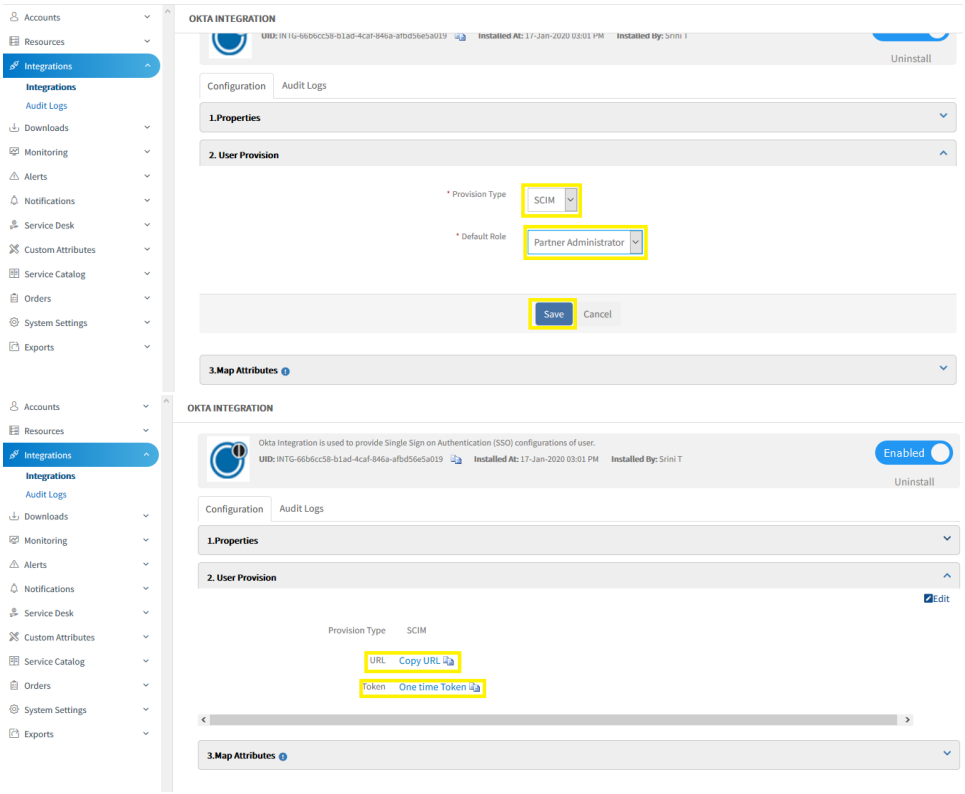
To configure Okta integration:

1. Provide the following and click **Install**:
    - Issuer URL: Identity Provider Issuer URL
    - Redirection URL: Identity Provider Single Sign-On URL
    - Logout URL: Sign-out URL as required
    - Certificate: x.509 certificate downloaded from Okta.

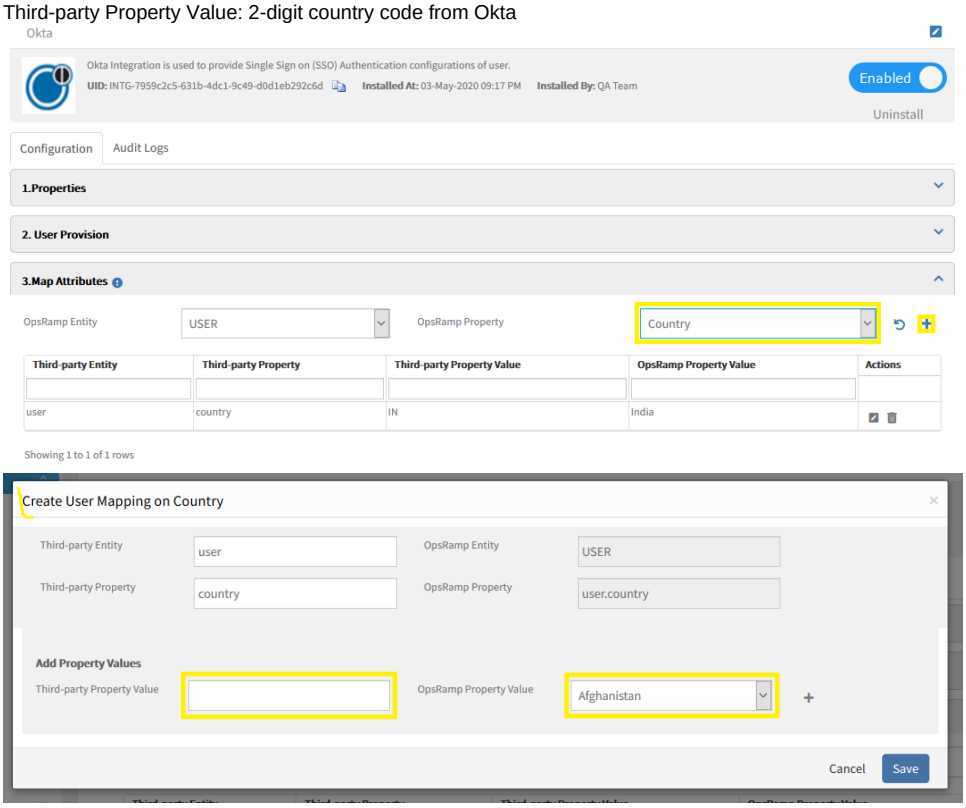


2. From **Configuration tab > User Provision section**, provide the following and click **Save**:
    - Provision Type: Select SCIM.
    - Default Role: Select the desired role.

- Note: The default role represents the role assigned for SCIM. The URL and token are displayed. The URL represents the SCIM 2.0 base URL and the token represents the OAuth bearer token. Both are required for Okta configuration.

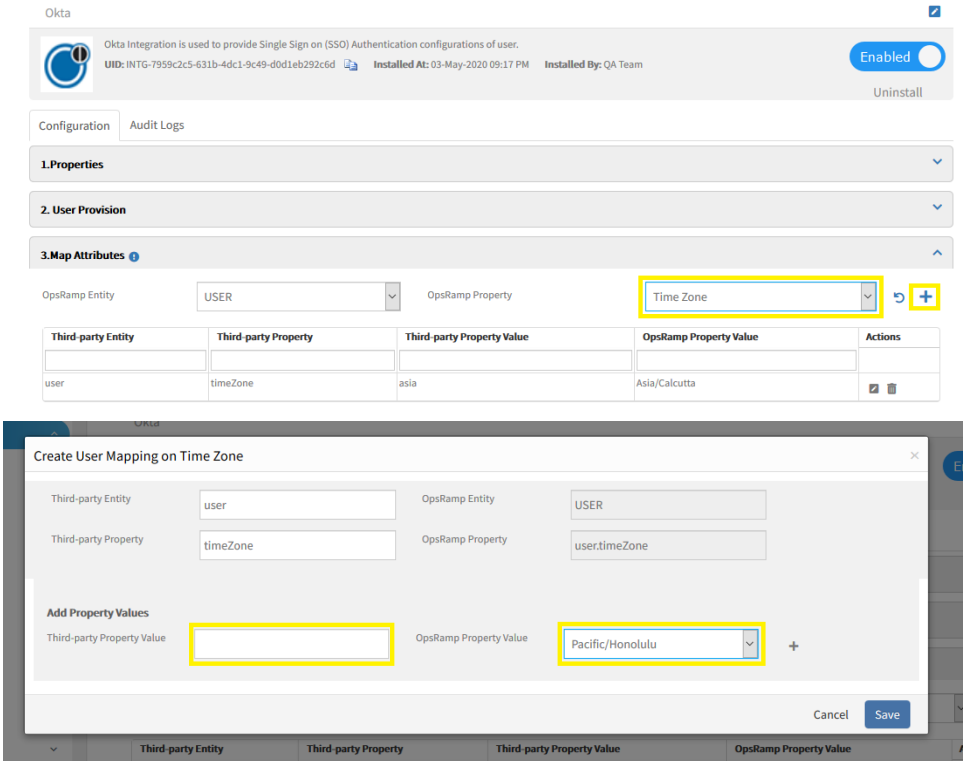


3. From the **Map Attributes** section, add the mapping to the country property and provide the following:
   - Third-party Entity: user
   - Third-party Property: country
   - Third-party Property Value: 2-digit country code from Okta



4. From the **Map Attributes** section, add the mapping to timeZone property and provide the following:
   - Third-party Entity: user
   - Third-party Property : country

- Third-party Property Value : timeZone value from OKTA.

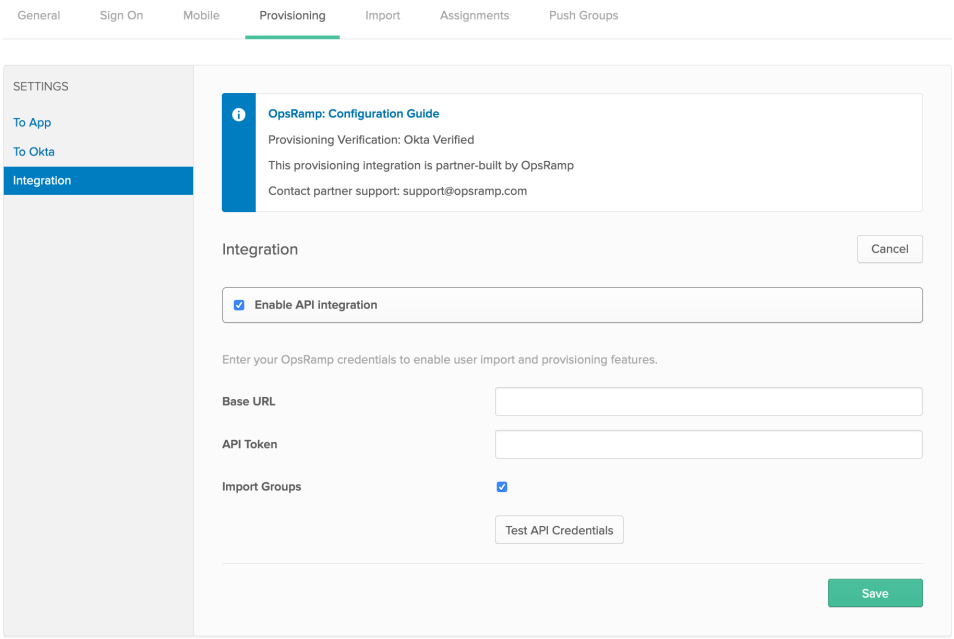


5. Click **Save**.

Okta configuration

To configure the provisioning settings:

1. Check the **Enable API Integration** box.
2. Enter your OpsRamp API Credentials:
    - SCIM 2.0 Base Url: Enter BaseUrl (this is the API URL which is displayed after enabling SCIM in OpsRamp).
    - OAuth Bearer Token: Enter the access token from OpsRamp.
3. Click **Test API Credentials** to validate the credentials.



4. Select **To App** in the left panel and then select the **Provisioning Features** that you want to enable.
5. Assign people and groups to the app (if needed) and finish the application setup.

Limitations

- Synchronization between Okta and OpsRamp is unidirectional. Changes in Okta reflects in Opsramp but not vice-versa.
- Fields with Empty values in Okta are not updated when pushed to OpsRamp.
- The Okta `userName` attribute, whose equivalent is `loginname` in OpsRamp, is not updated.
- When a user is terminated but the session is not terminated in OpsRamp, the user must log out from OpsRamp to end the session.
- Push Now is not functional. Push Now serves to *force* a push if the state of Okta and the target application are not in sync.
- Time Zone for the user group is not updated.

User provisioning test cases

The following list displays the status of test cases for Okta user provisioning.

	Test Cases	**Result**
1	After synchronization with Okta, try to login to the custom branding URL.	Passed
2	Assign a user in Okta where the mapping attributes were not mapped in OpsRamp. Validate that the same user was created in OpsRamp and assigned the default role.	Passed
3	Update different field values for a user in Okta. Check whether the user's updated values display in OpsRamp.	Passed
4	Unassign a user in Okta. Check whether the user is deactivated in OpsRamp.	Passed
5	Change the default role in OpsRamp and assign the user in Okta without specifying the mapping attributes. Update the assigned user in Okta and unassign the user in Okta. Validate whether the role changes display in OpsRamp.	Passed
6	Create mapping attributes for `firstname`, `lastname`, and `email` but do not create mapping attributes for `role`. Verify the assign, update, and unassign cases with both the default role and changed role. In this case, the default role is assigned.	Passed
7	Create mapping attributes for for `firstname`, `lastname`, `email`, and `role`. Verify the assign, update, and unassign cases. Check whether the same role displays.	Passed
8	Change the value for the `role` mapping attribute. Verify the assign, update, and unassign cases. Check whether the same role is passes the test cases and check whether the same role displays.	Passed
9	Create and assign a User Group in Okta to our SCIM app. Validate that the same user group is created in OpsRamp.	Passed
10	Update the name of the user group in Okta. Check whether it is displays in OpsRamp.	Passed
11	Unassign the user group from the SCIM app in Okta. Check whether the user group is deleted in OpsRamp.	Passed
12	Assign a user which is already in the Okta device group in the SCIM app. Then check whether the assigned user is created and added to the device group in OpsRamp.	Passed
13	Assign a user which is not in the Okta device group in the SCIM app. Then verify that the user is created in OpsRamp but not added to the user group in OpsRamp.	Passed
14	Unassign the user from the SCIM app. Verify that the user is deactivated and removed from the assigned user group in OpsRamp.	Passed
15	Map a role to an assigned user where the user group has one default role. Verity at the user level of the role view that it shows both the roles but at the user group level and it shows only the user group role.	Passed
16	In all the above user group scenarios, a default role of user provision is assigned. Map a user group with a mapping attribute of `role`. Verify that for the mentioned device group in `role`, the mentioned role, not the default role, displays.	Passed
17	Create a mapping for a User Group and assign that group in Okta to the app. Verify that the app is created in OpsRamp with the same role.	Passed
18	Assign two different groups each with a user and then exchange the users of both groups. Check to see whether the same displays in OpsRamp.	Passed