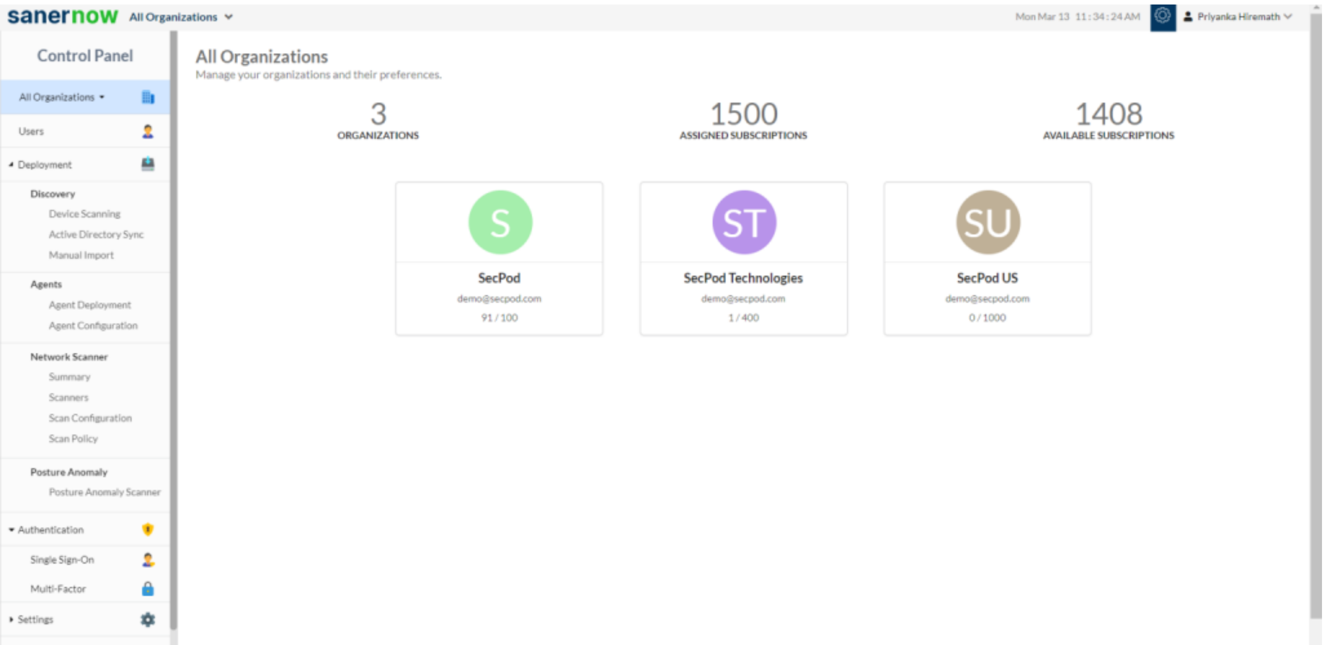
How to create MFA policy for Okta?

To configure the Okta MFA policy in SanerNow, you need Authentication Path, Client ID and Private Key from your organization's Okta account. Currently, SanerNow supports various authentication methods:

- SMS
- Email
- TOTP
- Okta push notification in mobile
- Authenticator app from Okta.

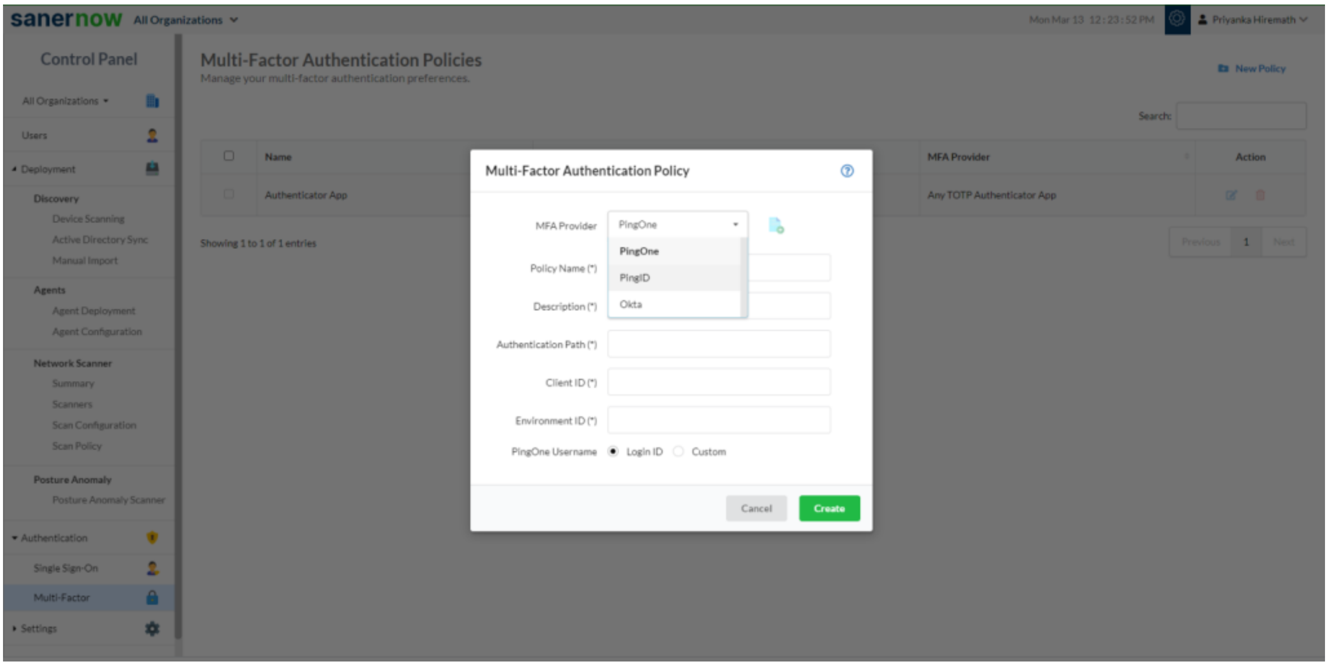
1. Go to **Control Panel** on the right.



2. From **Authentication** dropdown, select **Multi-factor**.

3. Click on **New Policy**.

4. Select **Okta** from the drop-down.



Multi-Factor Authentication Policy

MFA Provider: PingOne

Policy Name (*)

Description (*)

Authentication Path (*)

Client ID (*)

Environment ID (*)

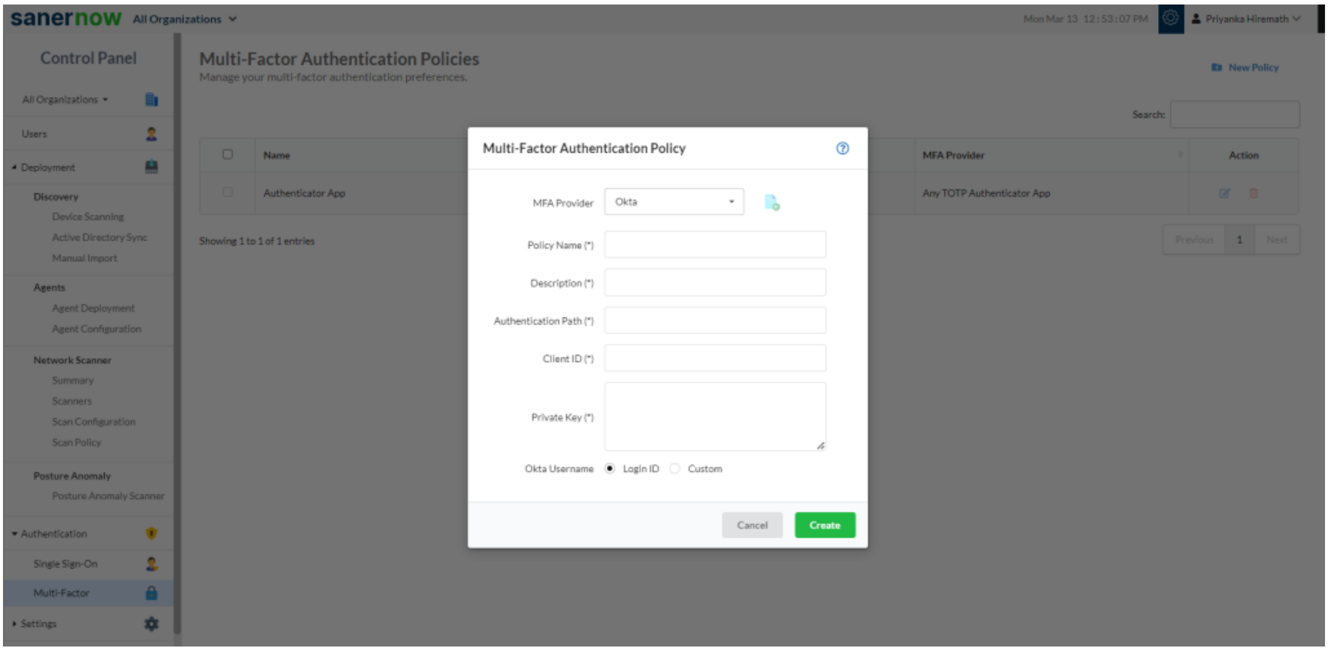
PingOne Username ● Login ID ○ Custom

Cancel Create

6. Policy Name: Enter the Policy Name. This should be a unique name to identify the policy within an organization.

Note: Refer this document to fetch the details of mandatory fields from the Okta account:

How to fetch the details of the mandatory fields from the Okta account? – SecPod – Documentation



Multi-Factor Authentication Policy

MFA Provider: Okta

Policy Name (*)

Description (*)

Authentication Path (*)

Client ID (*)

Private Key (*)

Okta Username ● Login ID ○ Custom

Cancel Create

7. Enter the Description about the policy.

8. Enter the Authentication Path from the organization’s Okta account.

9. Enter the Client ID from the organization’s Okta account.

10. Enter the Private Key from the organization’s Okta account.

11. Enter the Token information from your Okta enterprise account.

12. Select **Login ID** or **Custom** This option is selected depending on the SanerNow and Okta username mapping.

- Login ID: Select this option if your Okta username and SanerNow login ID are identical. By default, this option is selected.
- Custom: Select this option if your Okta username and SanerNow login ID are different.

Note: Users need to enter the valid inputs in each field, if invalid inputs are entered it throws an error message as Invalid ***Multi-Factor Authentication Input****.*