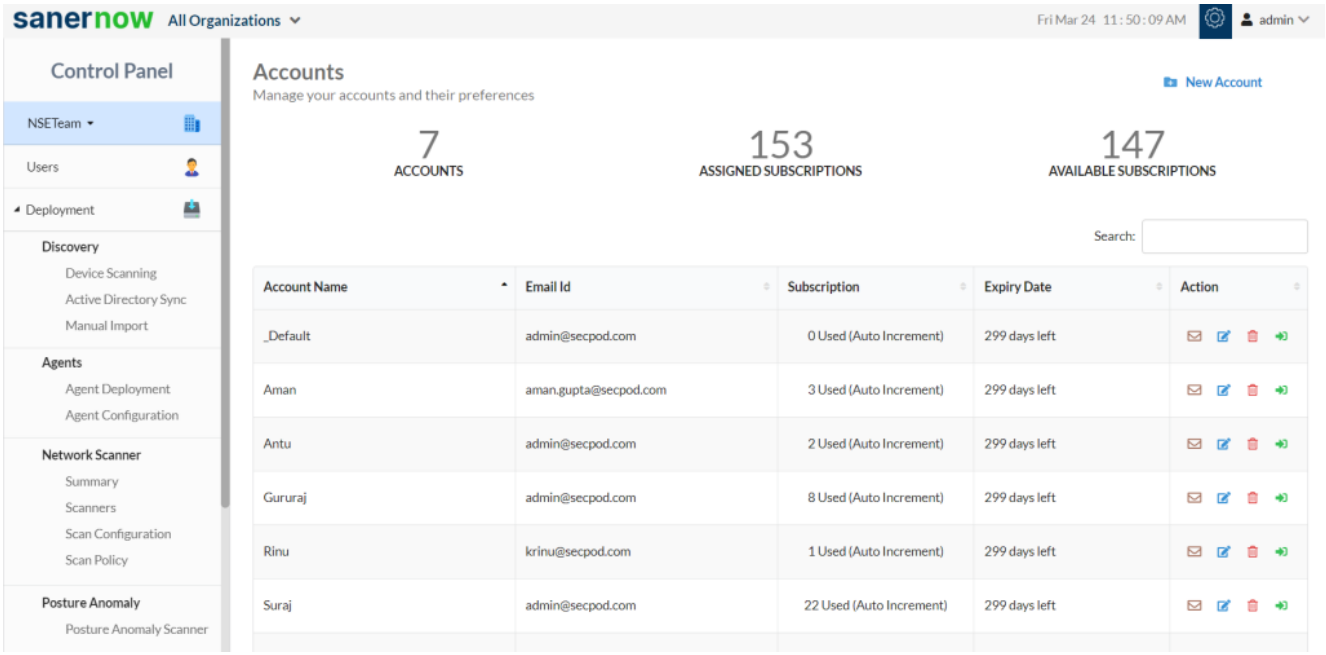
How to enable SSO authentication policy in SanerNow?

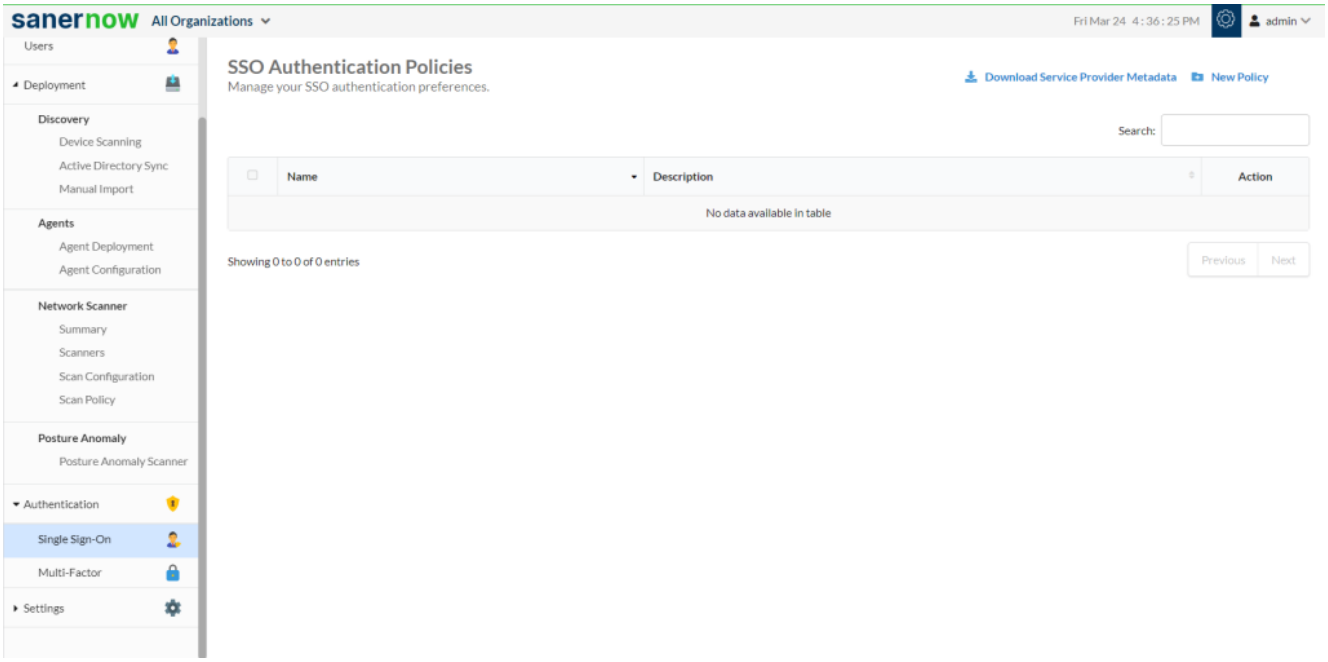
Single sign-on (SSO) is an authentication method that enables users to securely log in to multiple applications and websites with one set of credentials. SanerNow supports SAML v2 based SSO providers. SSO works based upon a trust relationship setup between an application (SanerNow), known as the service provider (SP) and Identity Provider (IDP) such as AWS, Azure, Auth0, Okta, PingID or PingFederate.

1. Go to **Control Panel**



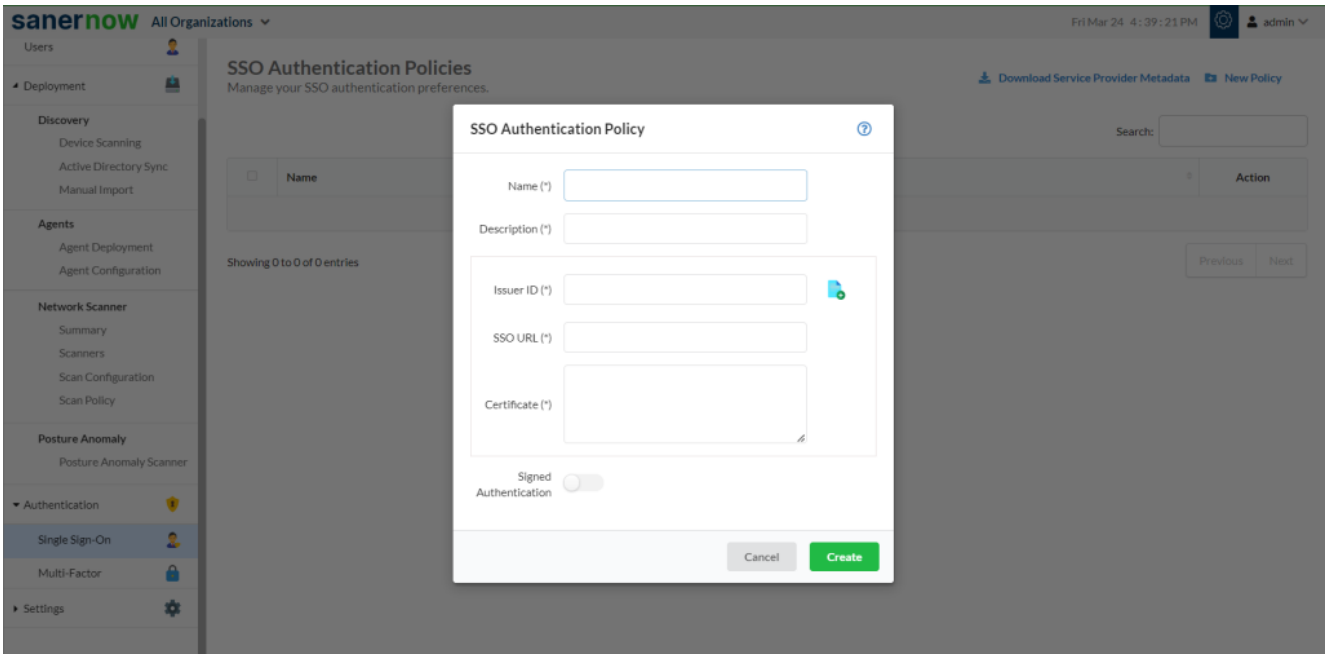
2. In Control Panel, click on **Authentication**

3. Select **Single Sign-On**



4. On the right-hand side, click on **New Policy**

5. Fill up:



- **Name**: Enter the policy name, a unique name to identify the policy.
- **Description**: Enter the description details about the policy.
- **Issuer ID**: Issuer refers to the “Entity Id / Identity Provider Issuer ID” of your identity

provider (also known as IDP), it is a URL that uniquely identifies SAML identity provider. SAML assertions sent to IDP must match this value exactly in the attribute of SAML assertions.

- **SSO URL**: A SSO URL is the IDP URL where the user will be redirected for authentication when they try to sign in from SanerNow directly. It may also be called a "Login URL/Identity Provider Single Sign-On URL" in your IDP.
- **Certificate**: The certificate (X.509 certificate) contains the public key used to verify whether the SAML response really comes from the IDP when the users try to sign in to the service provider (ex: SanerNow).
  The certificate will be in the following format:
  —–BEGIN CERTIFICATE—–
  < Public Key>
  —–END CERTIFICATE——-
- **Signed Authentication**: Enable this option if your IDP provider expects signed authentication requests. Once enabled, SanerNow service provider certificate download option would be displayed. Click on the option to download the certificate. This certificate should be used to enable signed authentication on your IDP.

Note: When configuring SAML SSO in SanerNow, you can either upload the IDP Metadata file directly using "Import IDP Metadata file" option, or copy and paste the data in the respective fields.

Now you know how to enable SSO authentication policy.