

Ping Integration

OVERVIEW

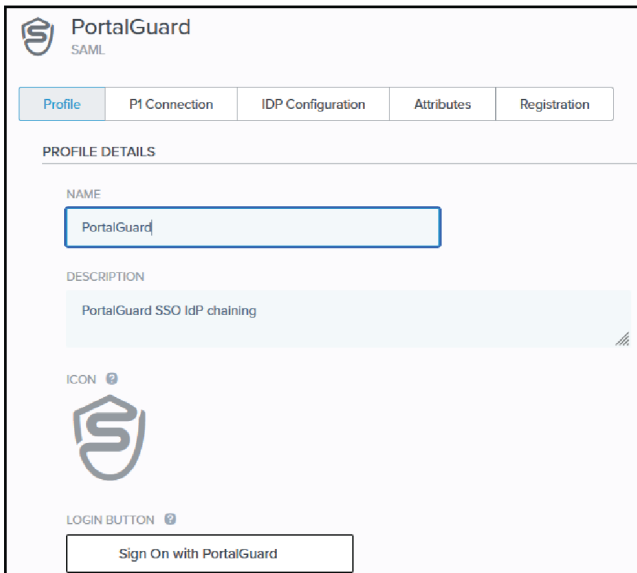
1. Download PortalGuard metadata
2. Configure connection in the Ping One Console
3. Download Ping metadata
4. Configure connection in the PortalGuard Admin Panel
5. Ping Authentication Policy
6. Test

1. Download PortalGuard Metadata

- Download the PortalGuard SAML metadata by using the following URL format: [https://\[instance\]](https://[instance])
 - Replace [instance] with the name of your PortalGuard instance.
- Open the downloaded metadata.xml file to view the contents.

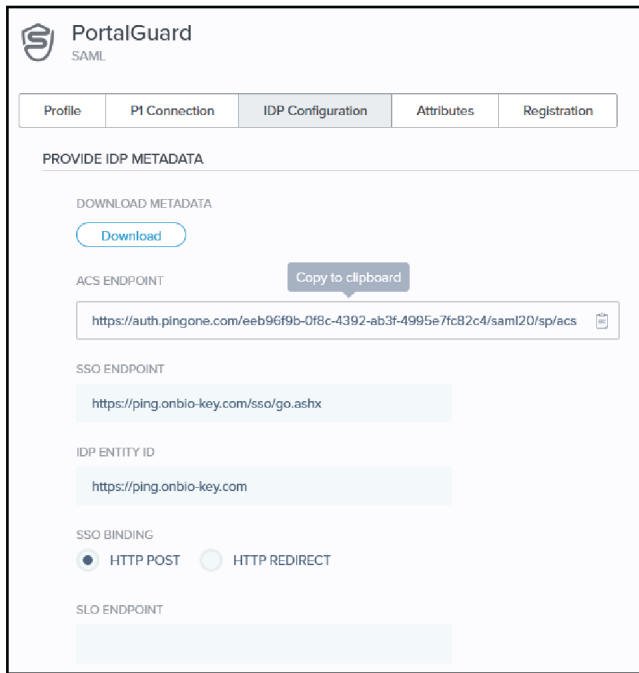
2. Configure connection in the Ping One Console

- Once authenticated to the Ping One console, navigate to Connections -> External IDPs.
- Click “+ Add Provider” to setup the connection to PortalGuard.



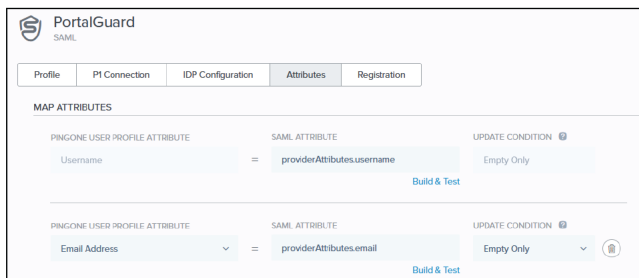
1. Profile

- a. Name – “PortalGuard”
- b. Description – Optional



2. IDP Configuration

- SSO Endpoint – SingleSignOnService HTTP-POST Binding from the PortalGuard Metadata
- IDP Entity ID – EntityID from PortalGuard Metadata
- SSO Binding – HTTP POST
- SLO Endpoint – empty



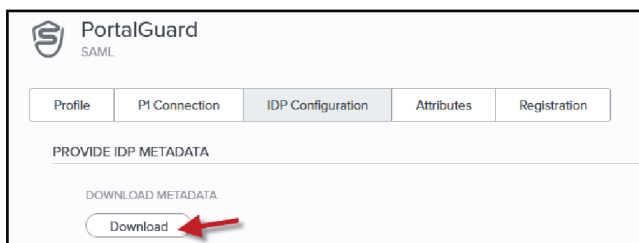
3. Attributes

- User Profile Attribute – Username
 - SAML Attribute = providerAttributes.username
- User Profile Attribute – Email Address
 - SAML Attribute = providerAttributes.email
- Add any additional claims, which will also need to be added in PortalGuard



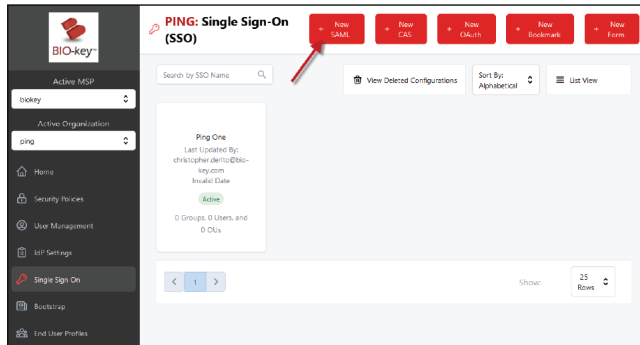
Once the configuration is finished and saved, enable the configuration by flipping the toggle switch for it in the external IdP list.

3. Download Ping metadata



- Edit the PortalGuard External IDP connection you just configured, and navigate to the IDP Configuration tab.
- Here click Download under Download Metadata.
- Open the downloaded metadata file.

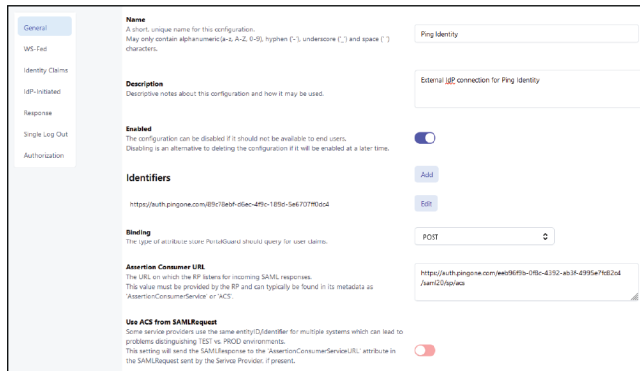
4. Configure connection in the PortalGuard Admin Panel



- Navigate to the BIO-key IDaaS Admin Panel, select Single Sign On, and Create new SAML in the top right corner.
- Configure the PortalGuard Application as follows for each tab:

1. General

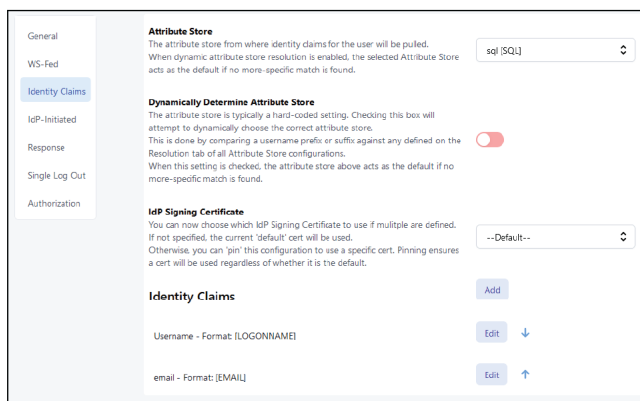
- Name – “Ping Identity”
- Description – “External IdP connection for Ping Identity”
- Enabled – True
- Identifiers – EntityID from Ping metadata
- Binding - POST
- Assertion Consumer URL – AssertionConsumerService “Location” from Ping Metadata
- Use ACS from SAML Request

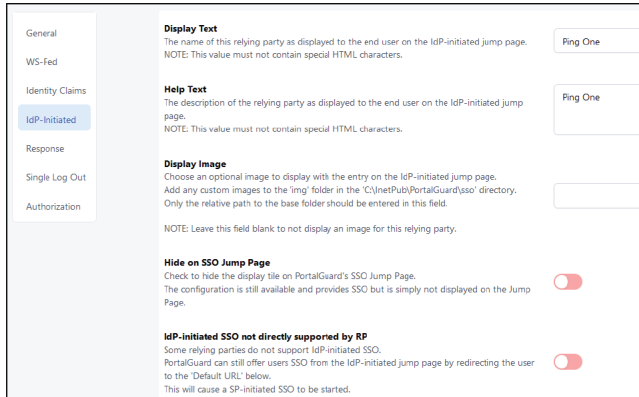


2. Identity Claims

For each claim, set the Name and Schema Type field the same. The Value Type will always be “Formatted String”. Select the add Placeholder button to choose a predefined placeholder to reference the desired field in the Composite Value Format field.

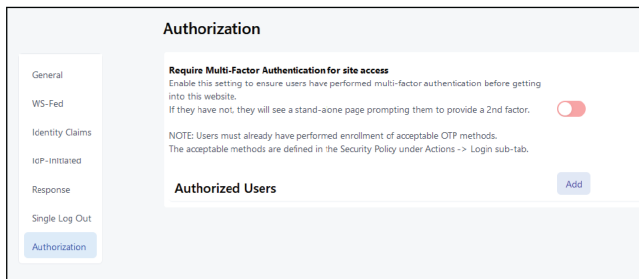
- Name/Schema Type: Username
 - Composite Value Format: [LOGONNAME]
- Name/Schema Type: Email
 - Composite Value Format: [EMAIL]





3. IdP-Initiated

- Display Text – “Ping One”
- Help Text – “Ping One”
- Display Image – Leave blank for no image, alternatively, you can work with PortalGuard support to upload a custom image for this tile.

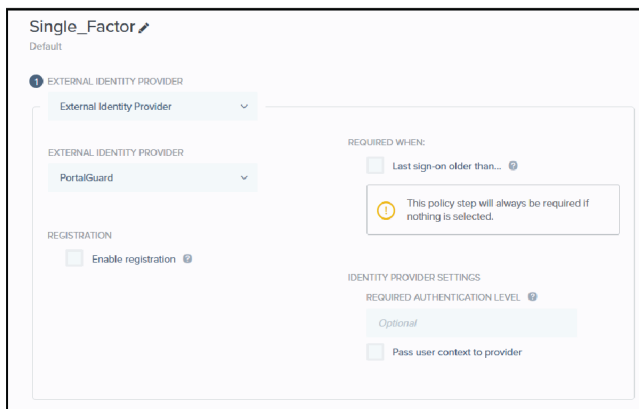


4. Authorization

- Optionally, you can require MFA be used for this specific application, as well as specify individual users, groups, or OU's that are able to access this application.

Once you have configured the application within the PortalGuard Admin panel, click 'Save' in the top right corner and then Apply the changes by clicking on the banner at the top of the page.

5. Ping Authentication Policy



- Edit the existing policy for single_factor. PortalGuard will be handling authentication and MFA.
 - Choose 'External Identity Provider' in the first dropdown
 - External identity Provider – PortalGuard
- Save these settings.

6. Test

Try to login to the Ping site. You will be directed to PortalGuard to enter your username and password and complete MFA as it is configured in PortalGuard. Once finished, you will be redirected back to Ping.