BeyondTrust

Remote Support
Ping Identity PingOne Integration

TC:3/4/2024

Table of Contents

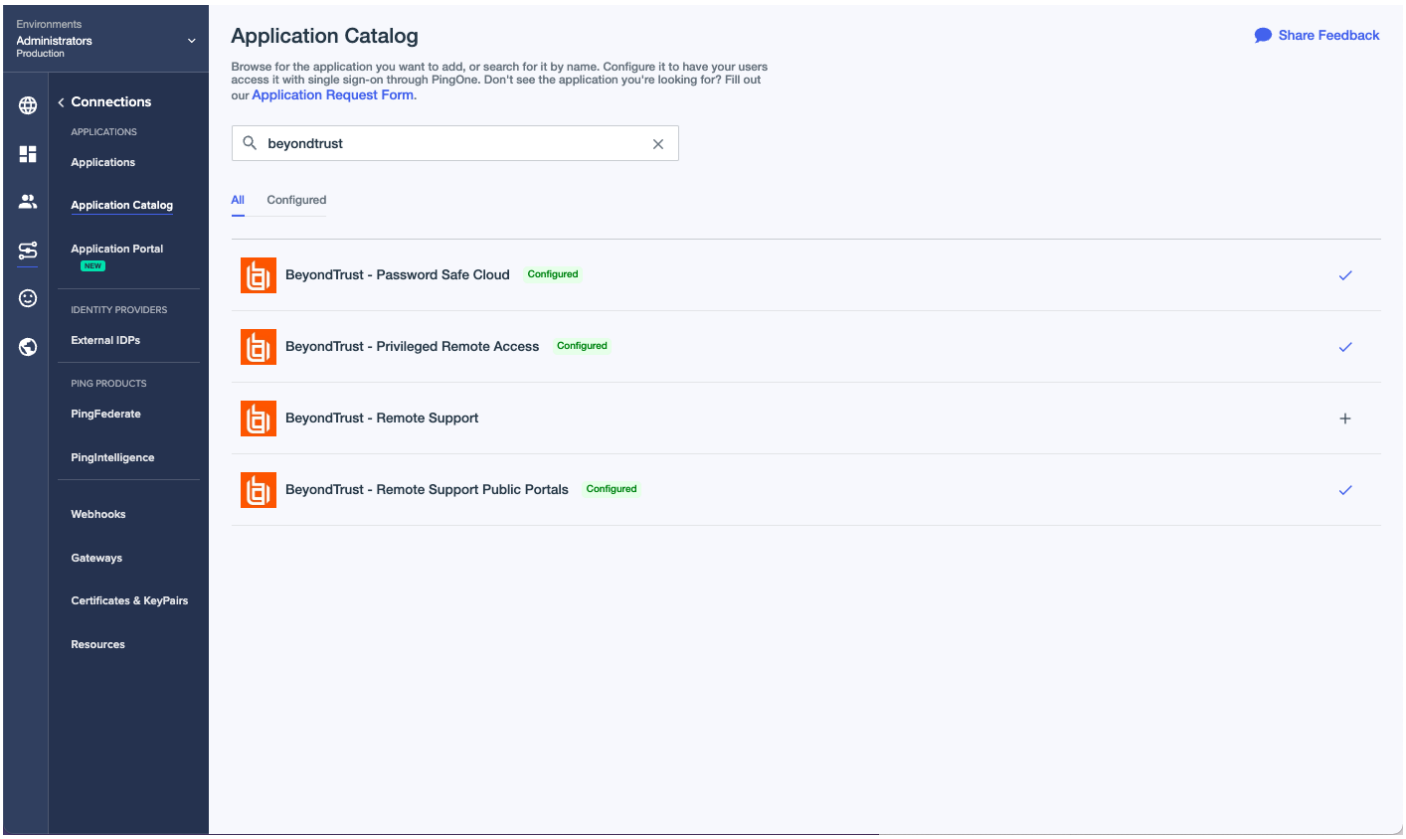
Configure SAML 2.0 for Remote Support using Ping Identity PingOne

Ping Identity offers a PingOne SSO solution that integrates with BeyondTrust Remote Support. It can be set up for Representatives, Public Portals, or both. This guide shows how to configure PingOne and Remote Support integrations.

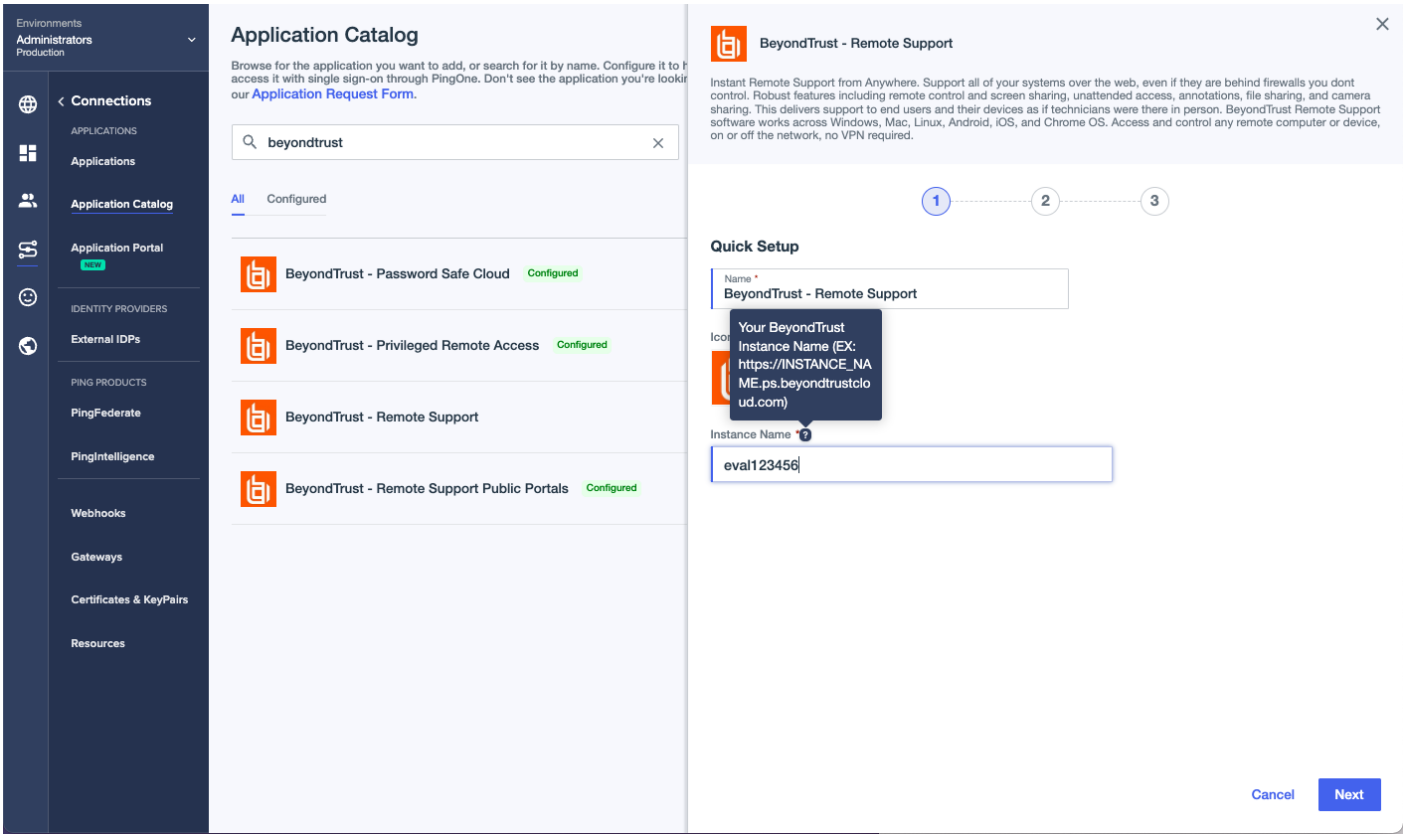
Configure PingOne for Remote Support Representatives

Configuring the PingOne integration with BeyondTrust Remote Support for Representatives requires steps in both applications. Start in PingOne, and follow these steps:

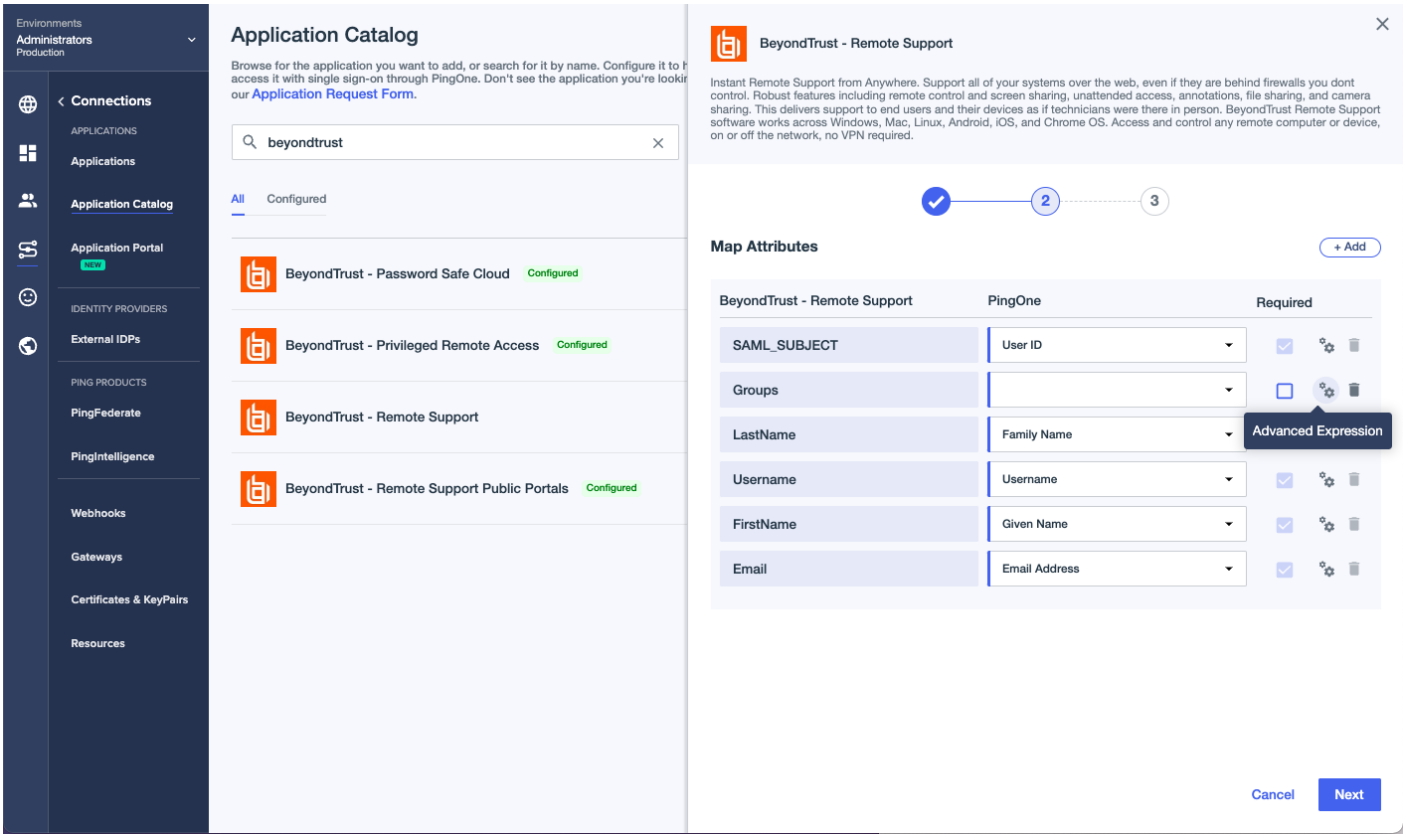
1. Log in to PingOne.
2. Navigate to the **Application Catalog**.
3. Search for *BeyondTrust*. The search results show the various BeyondTrust applications and their configuration status.



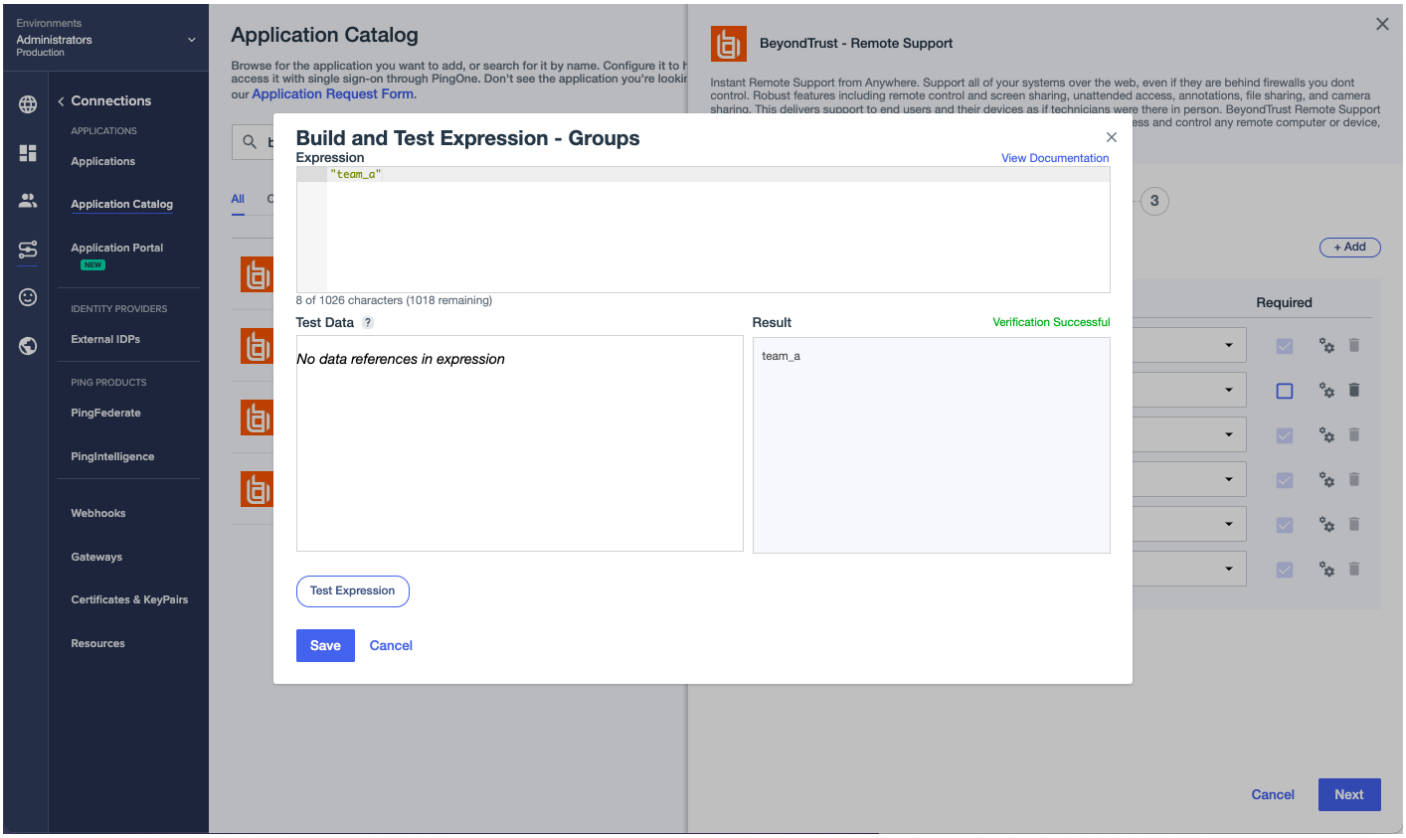
4. Click the **+** icon at the end of the row for **BeyondTrust - Remote Support.**
5. Enter your instance name.



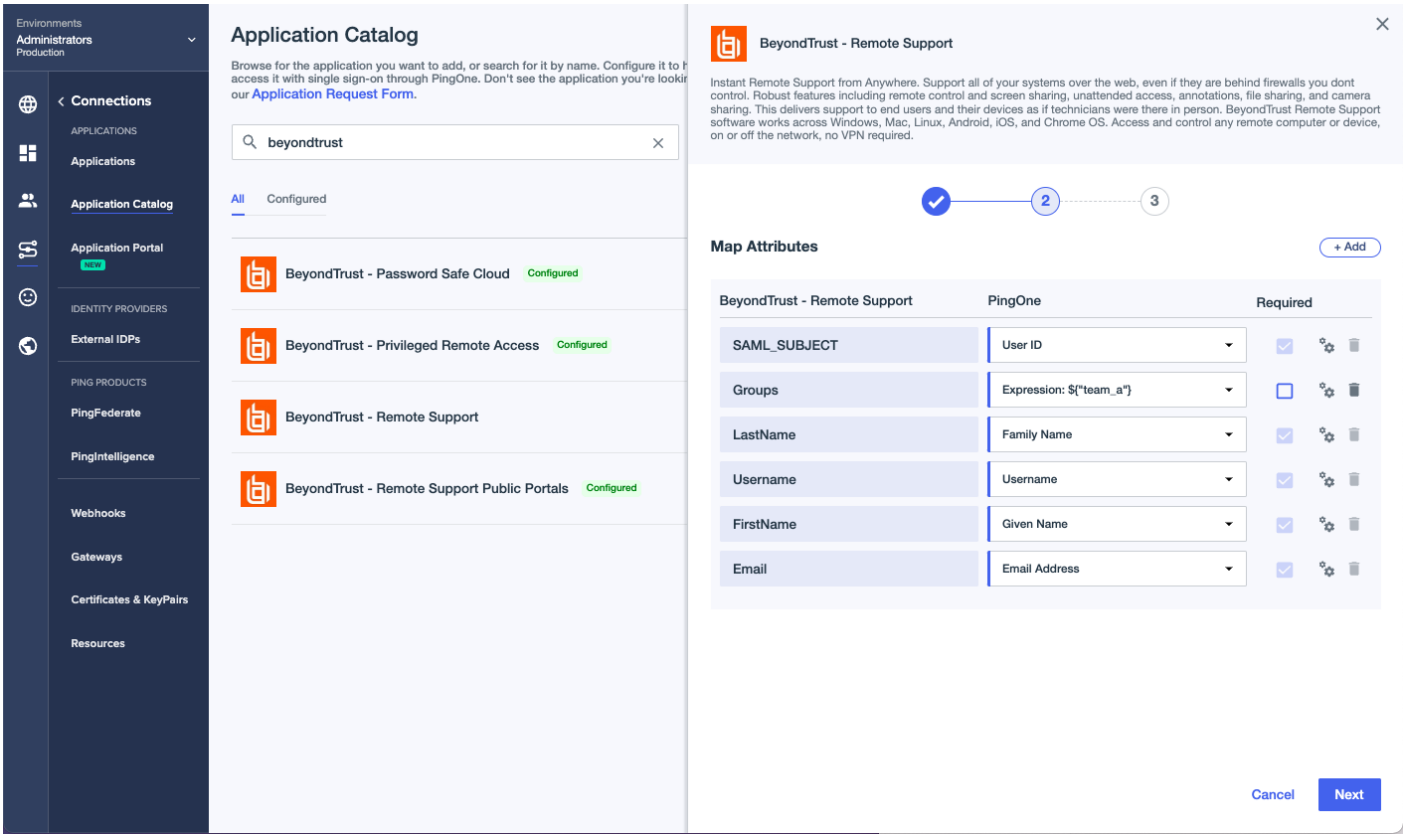
6. Click **Next**.



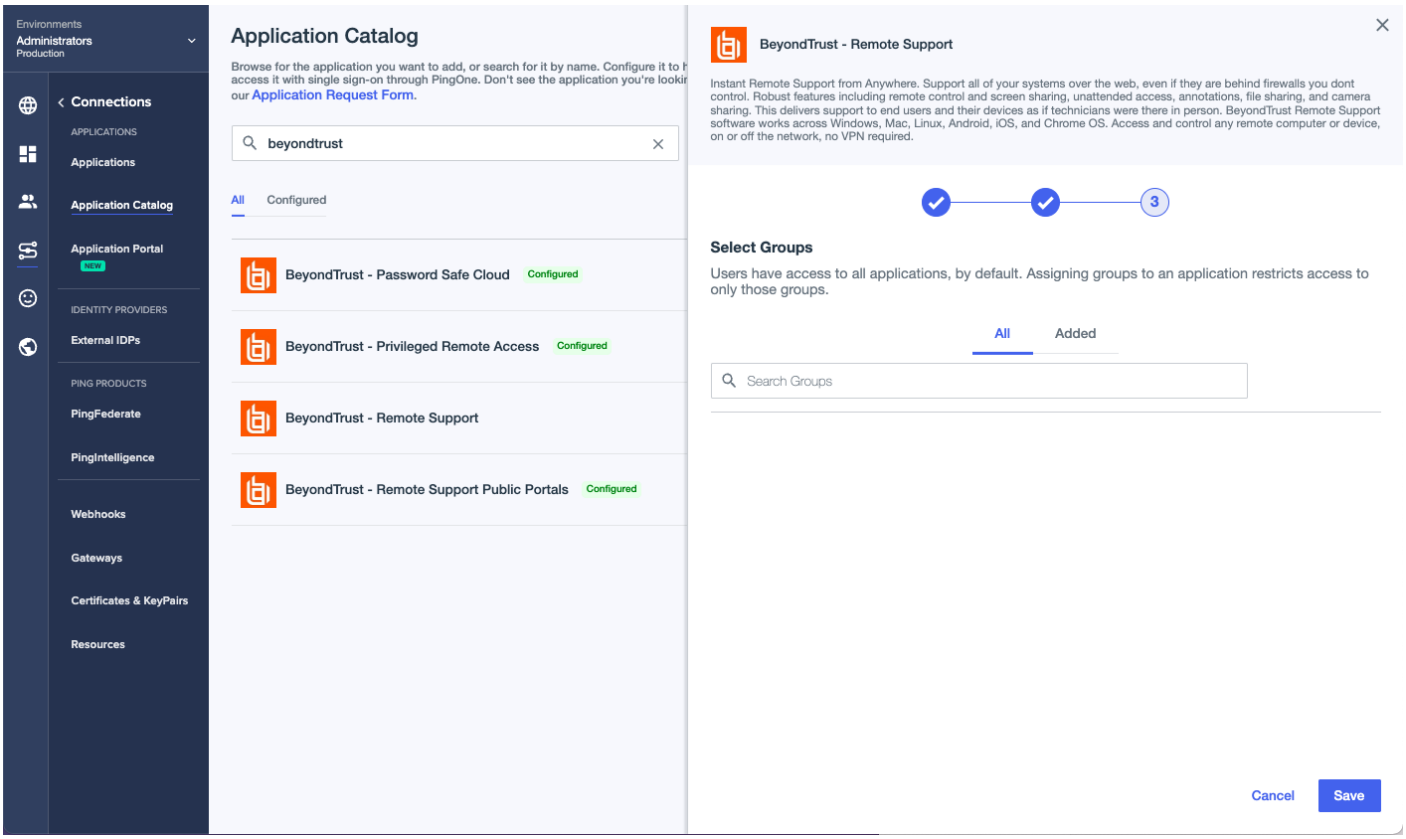
7. On the Map Attributes page, complete the configuration for the Groups attribute. Remote Support requires one or more string values with multiple values separated by a configurable delimiter. It is possible to map a PingOne User Attribute or another method, but that is beyond the scope of this guide. We must configure an advanced expression for the groups attribute. Assign a static value, surrounded by double quotes, that corresponds to an existing group in Remote Support. In this example, *team_a* is used.
8. The Map Attributes page should look like the image below.



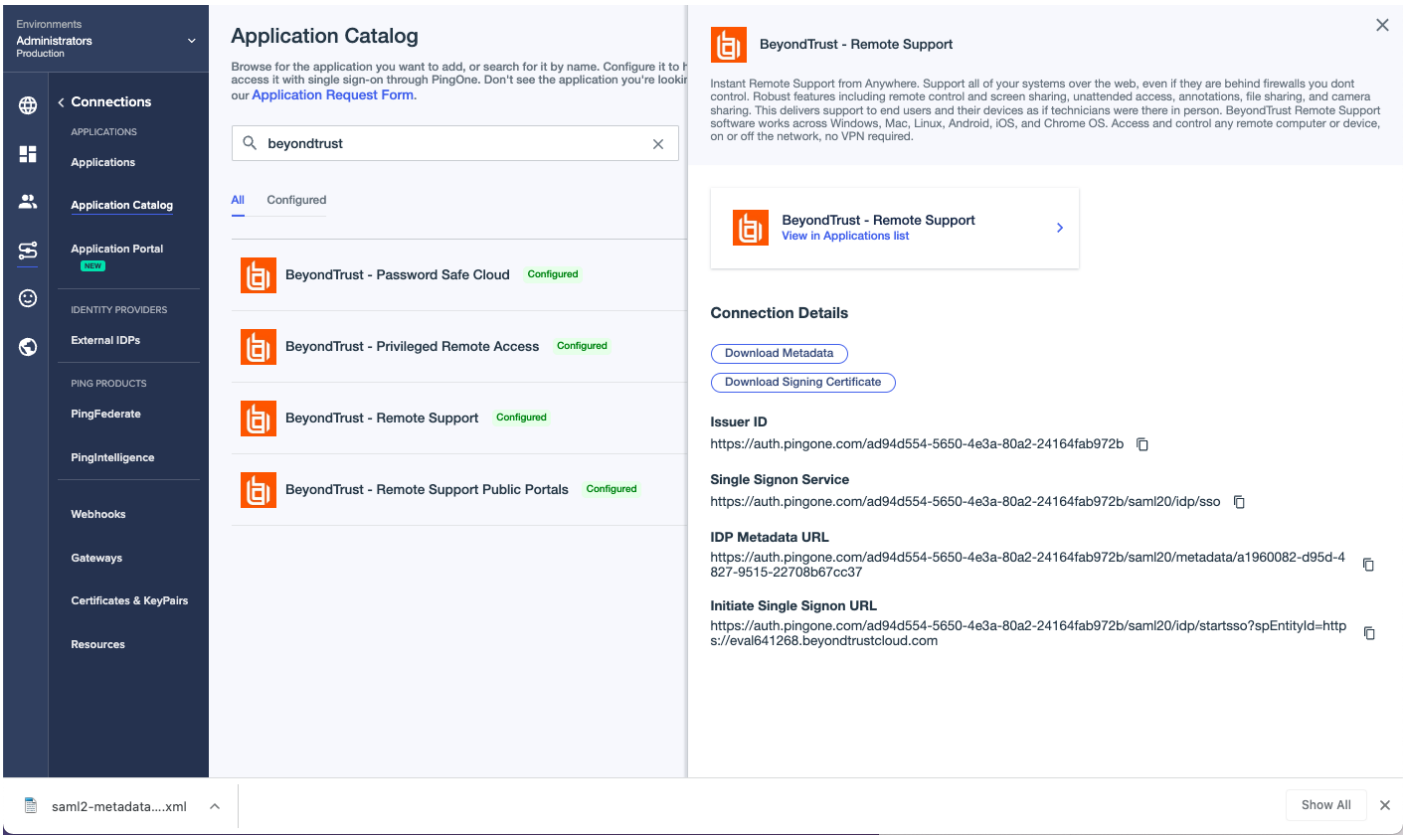
9. Click **Save**, then **Next**.



10. Access Control Groups in PingOne can be used to limit access to the Application. Leave the page empty for now and click **Save**.



11. On the Connection Details page, click **Download Metadata**.

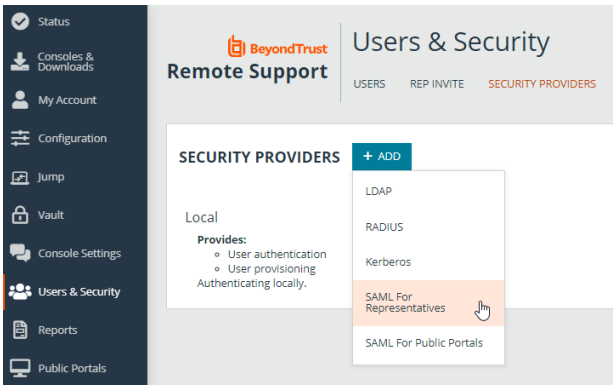


12. Continue the configuration in BeyondTrust Remote Support.

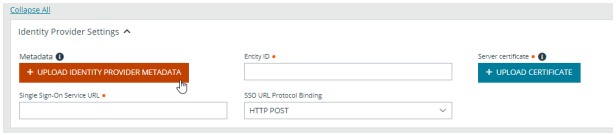
Configure Remote Support Representatives for PingOne

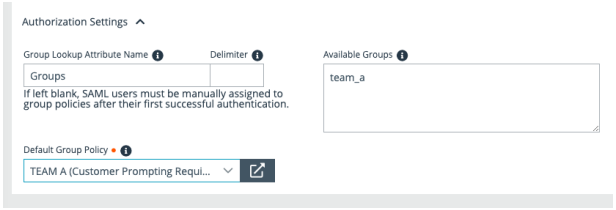
Follow these steps to create a new SAML Provider for Ping Identity PingOne.

1. Log in to BeyondTrust Remote Support.
2. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
3. Click **Add** and select **SAML for Representatives**.
4. Enter a name to identify this provider, such as *SAML For Representatives*.

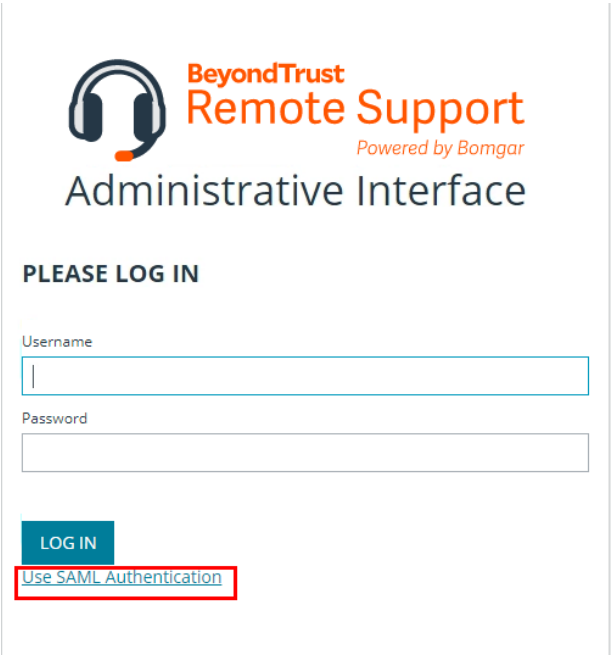


5. Under **Identity Provider Settings**, click **UPLOAD IDENTITY PROVIDER METADATA**.
6. Browse to the metadata file downloaded from PingOne and select it.
7. The **Single Sign-On Service URL** and the **Entity ID** are populated by the metadata file. Leave the **SSO URL Protocol Binding** as *HTTP POST*.
8. Select the Available Groups and Default Group Policy.
9. Click **SAVE** at the top of the screen.

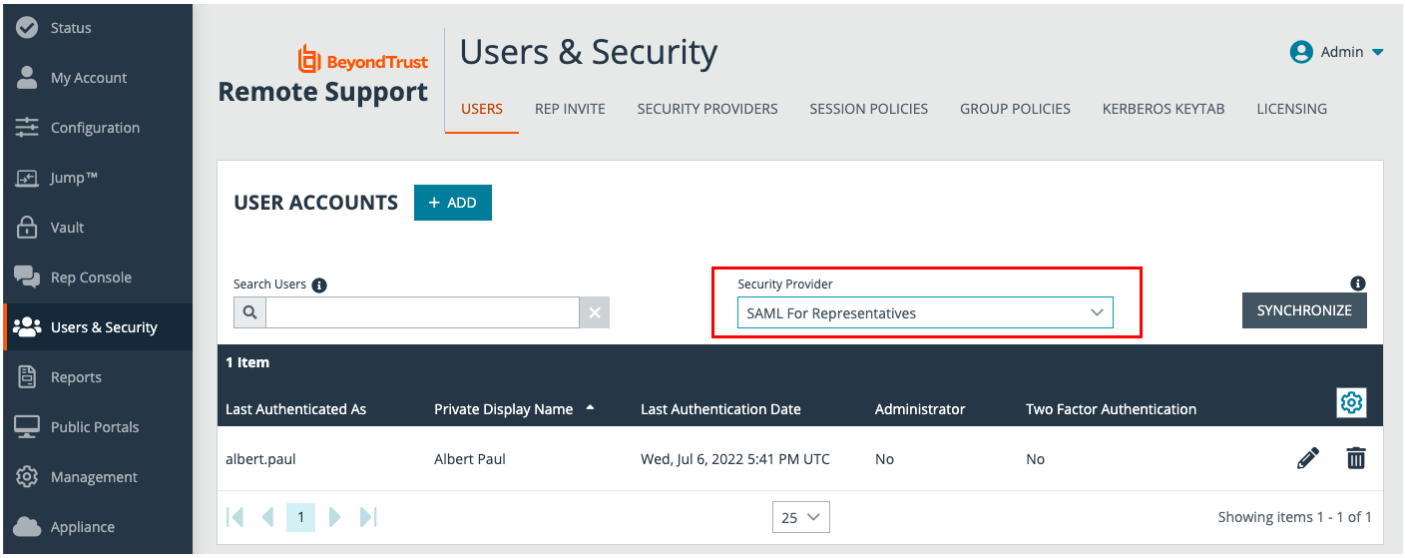




PingOne supports Identity Provider (IdP) initiated Single Sign-On, via a direct link or the Apps portal for Users. Remote Support supports Service Provider (SP) initiated Single Sign-On. On the login page, click **Use SAML Authentication** for SP initiated SSO.



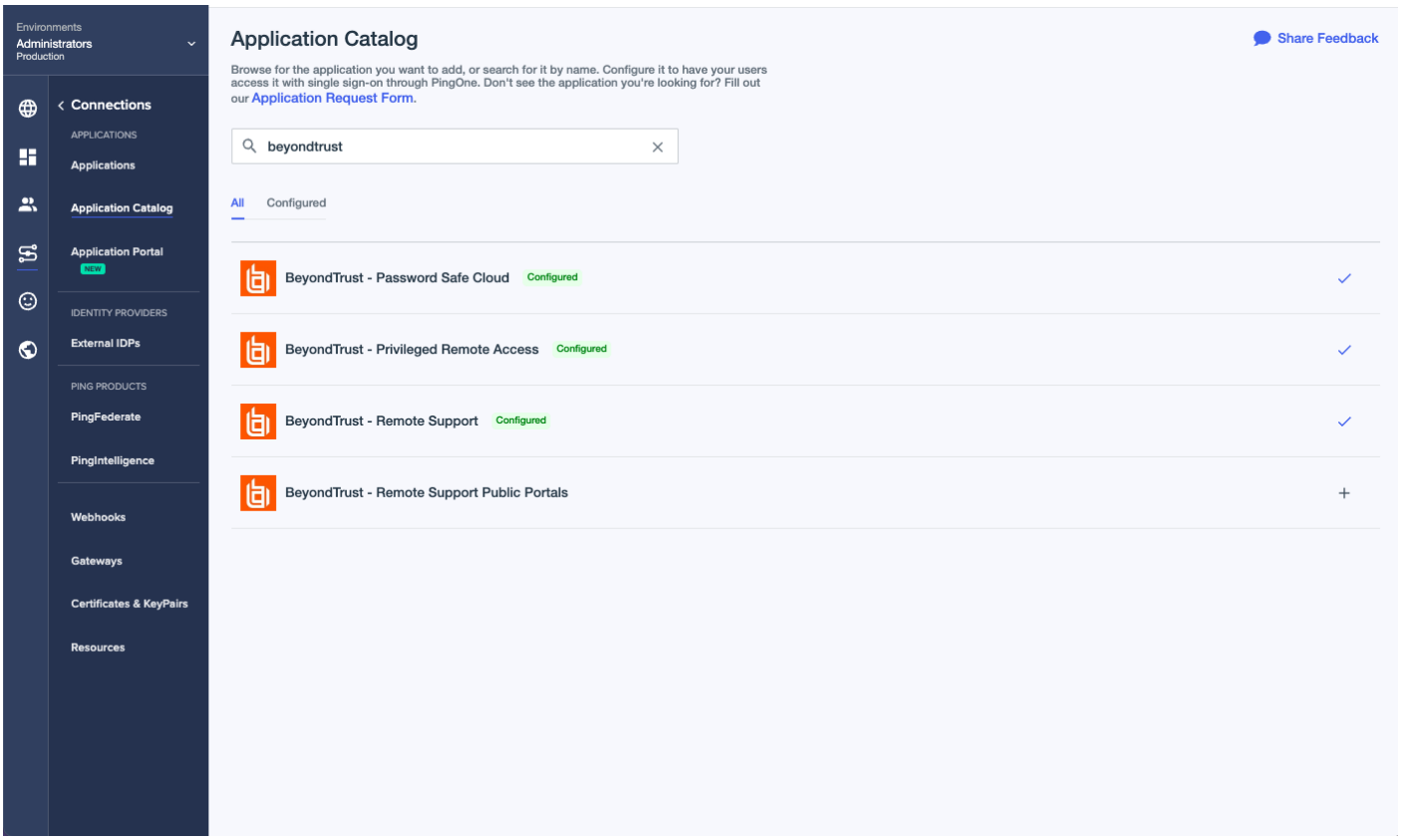
SAML Users are managed by the Identity Provider, which is PingOne.



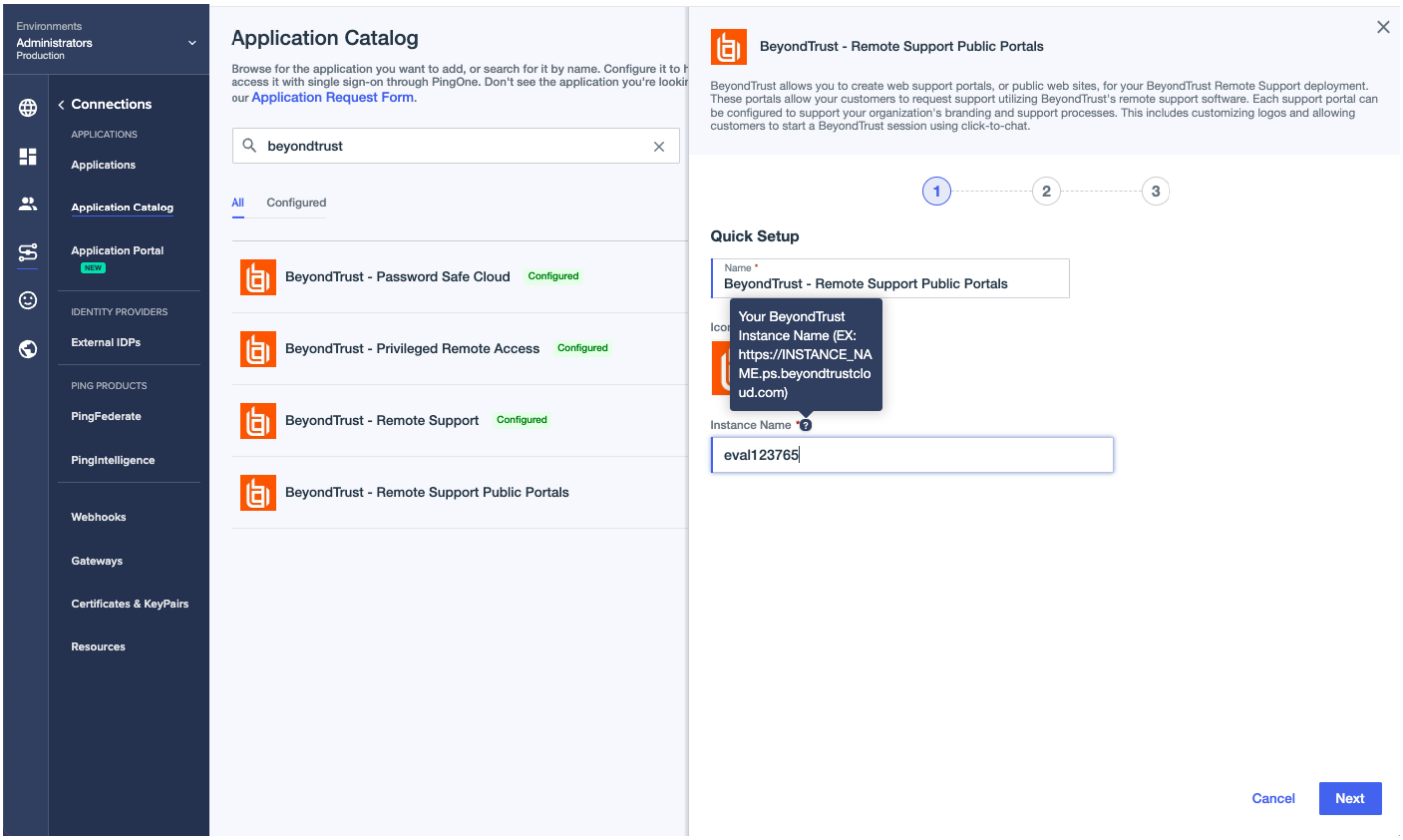
Configure PingOne for Remote Support Public Portals

Configuring the PingOne integration with BeyondTrust Remote Support Portals requires steps in both applications. Start in PingOne, and follow these steps:

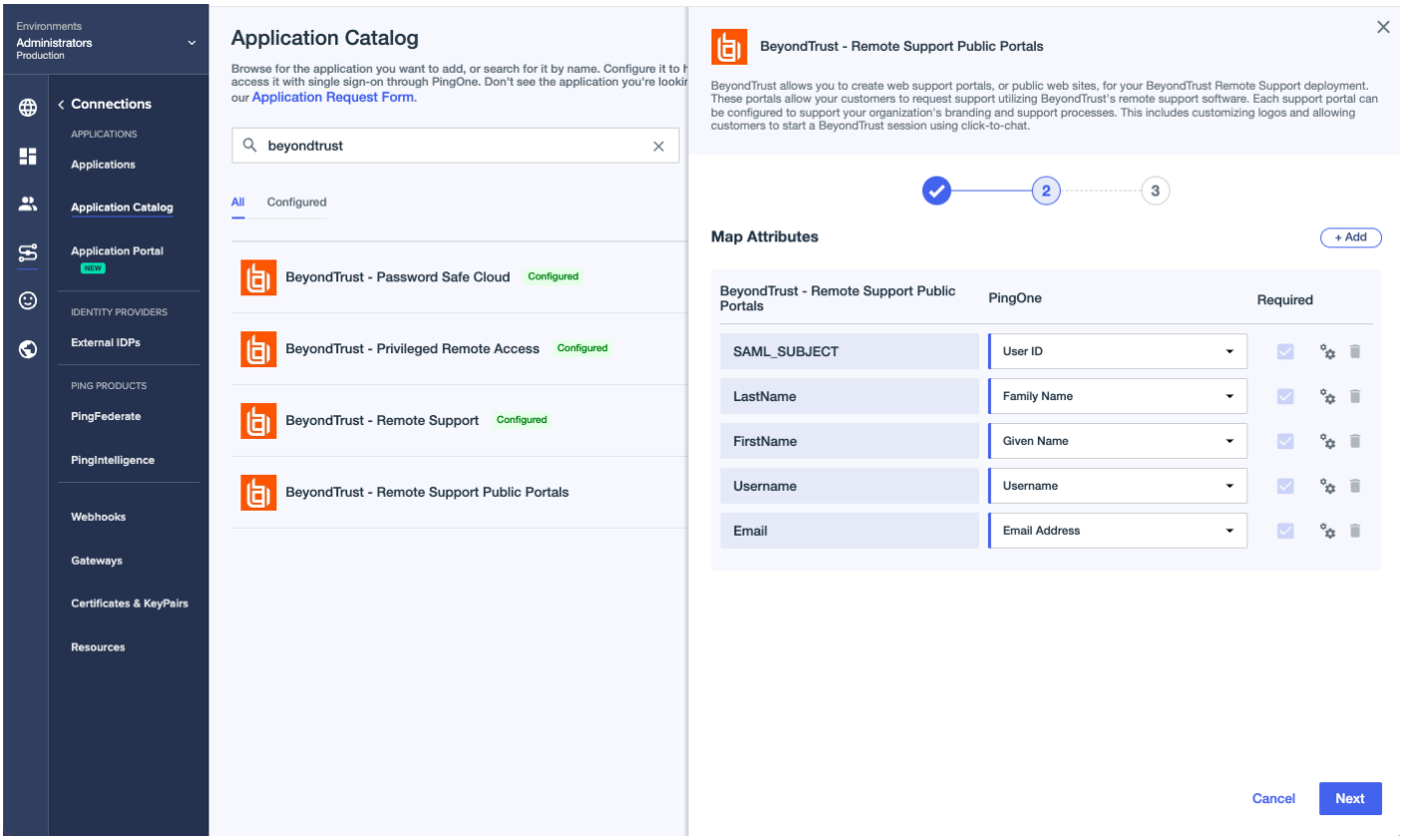
1. Log in to PingOne.
2. Navigate to the **Application Catalog**.
3. Search for *BeyondTrust*. The search results show the various BeyondTrust applications and their configuration status.



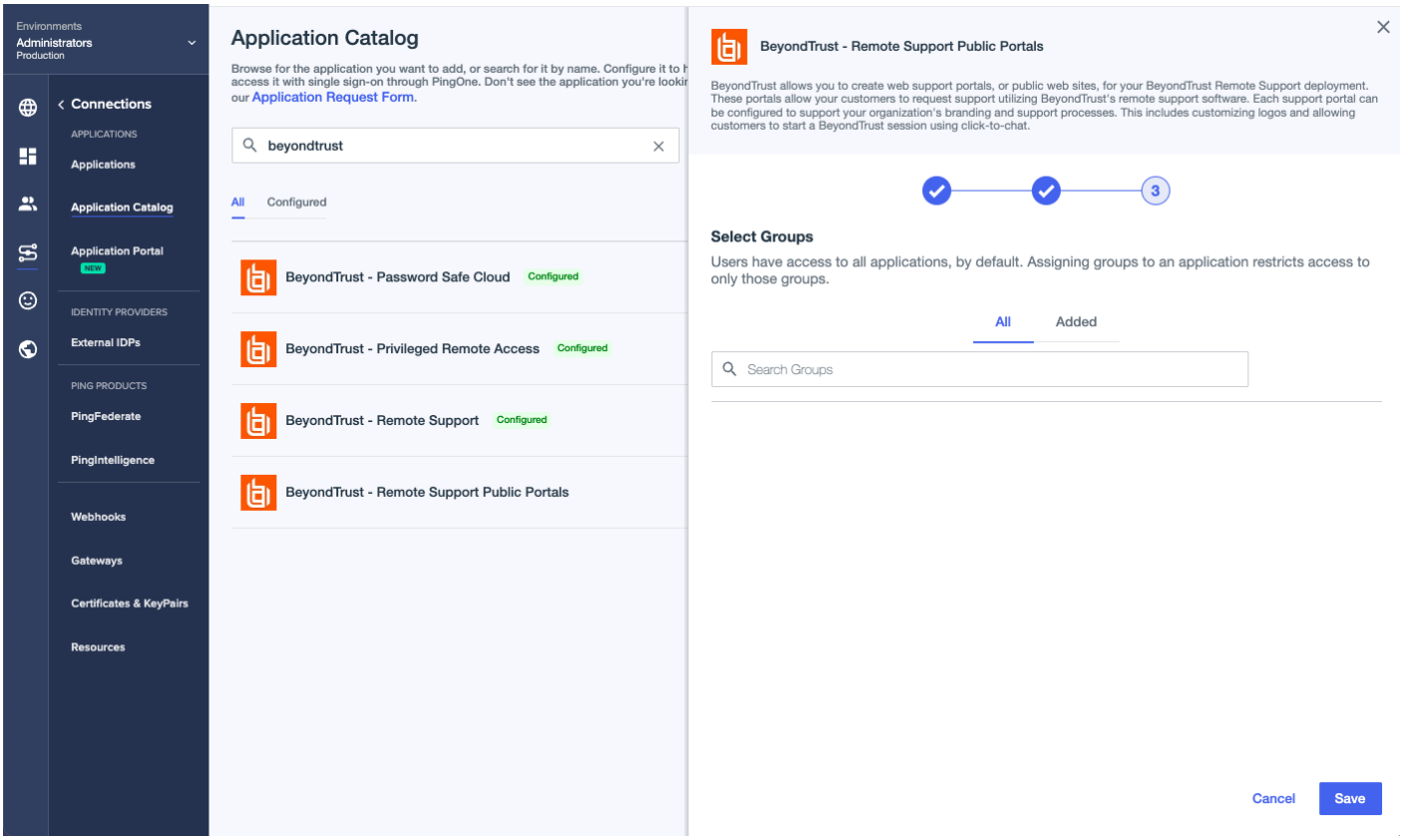
4. Click the **+** icon at the end of the row for **BeyondTrust - Remote Support** Public Portals.
5. Enter your instance name.



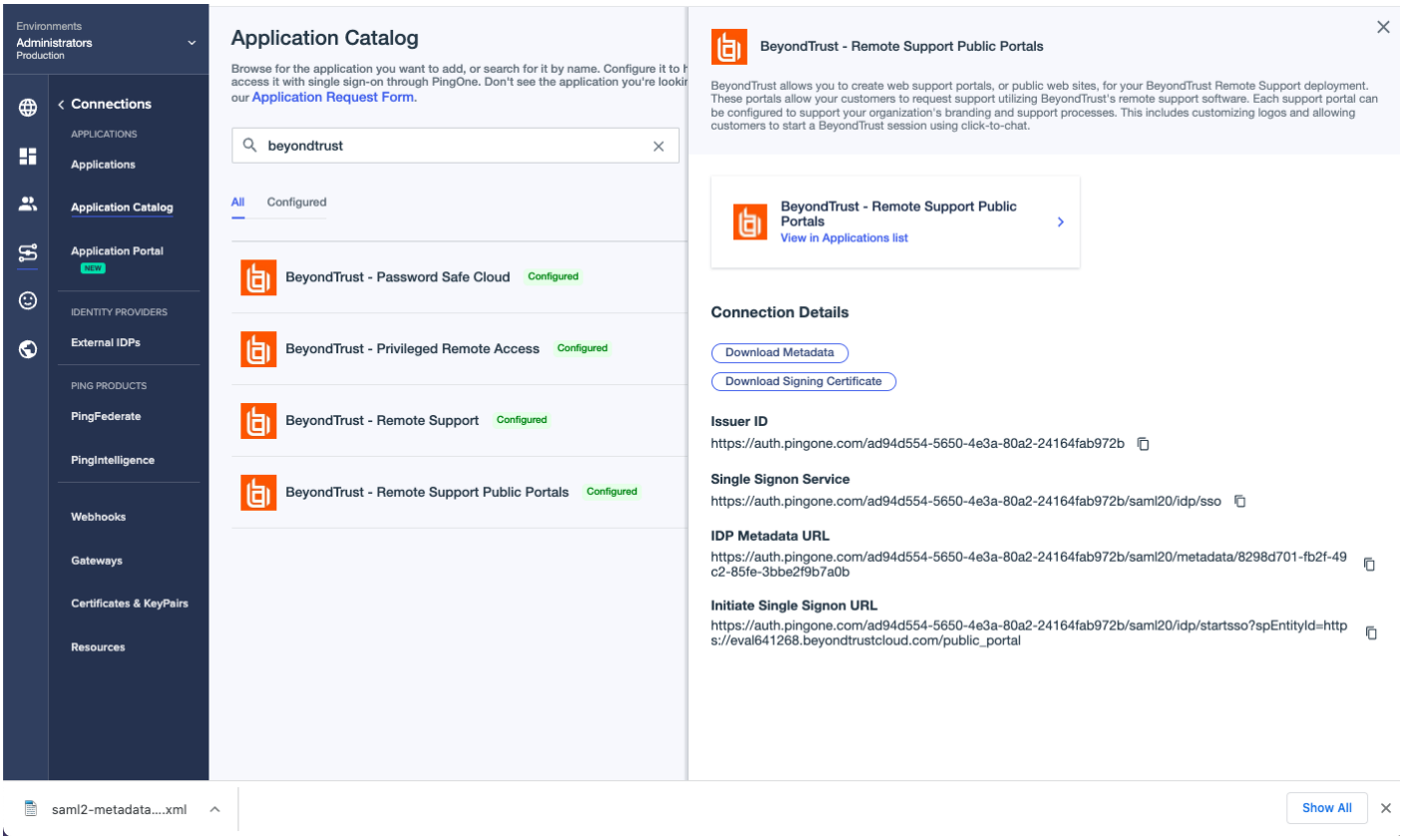
6. Click **Next**.



7. On the Map Attributes page, click **Next.**
8. Access Control Groups in PingOne can be used to limit access to the Application. Leave the page empty for now and click **Save**.



9. On the Connection Details page, click **Download Metadata**.

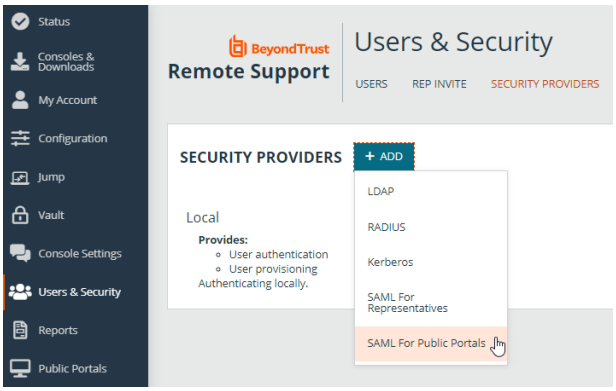


10. Continue the configuration in BeyondTrust Remote Support.

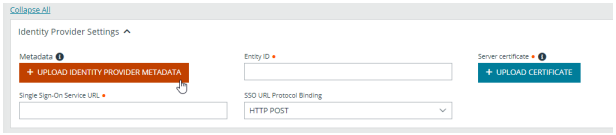
Configure Remote Support Portals for PingOne

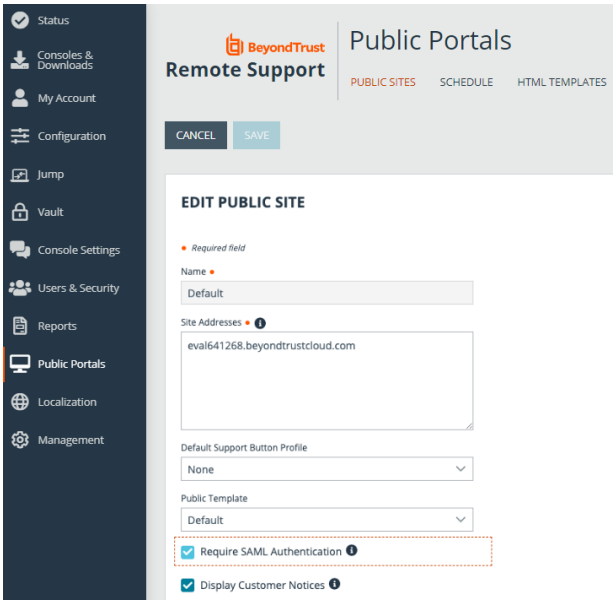
Follow these steps to create a new SAML Provider for Ping Identity PingOne.

1. Log in to BeyondTrust Remote Support.
2. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
3. Click **Add** and select **SAML for Public Portals**.
4. Enter a name to identify this provider, such as *SAML-For-Public-Portals*.

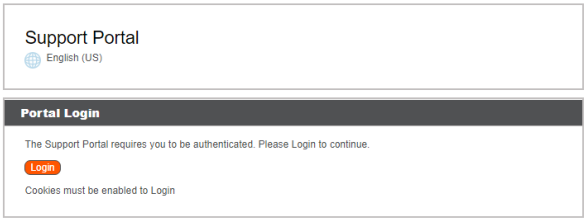


5. Under **Identity Provider Settings**, click **UPLOAD IDENTITY PROVIDER METADATA**.
6. Browse to the metadata file downloaded from PingOne and select it.
7. The **Single Sign-On Service URL** and the **Entity ID** are populated by the metadata file. Leave the **SSO URL Protocol Binding** as *HTTP POST*.
8. Leave the **User Attribute Settings** at their defaults.
9. Click **SAVE** at the top of the screen.
10. Click **Public Portals** on the left menu, and then click **Public Sites**.
11. Click the pencil icon to edit the selected portal.
12. Check **Require SAML Authentication**.
13. Click **SAVE** at the top of the screen.





PingOne supports Identity Provider (IdP) initiated Single Sign-On, via a direct link or the Apps portal for Users. Remote Support supports Service Provider (SP) initiated Single Sign-On. The public portal enabled for SAML authentication displays a login button.



Once authenticated via PingOne, the user will see the **Your Name** field populated.