



BeyondTrust

Remote Support Ping Identity PingOne Integration

Table of Contents

Configure SAML 2.0 for Remote Support using Ping Identity PingOne	3
Configure PingOne for Remote Support Representatives	4
Configure Remote Support Representatives for PingOne	11
Configure PingOne for Remote Support Public Portals	13
Configure Remote Support Portals for PingOne	18

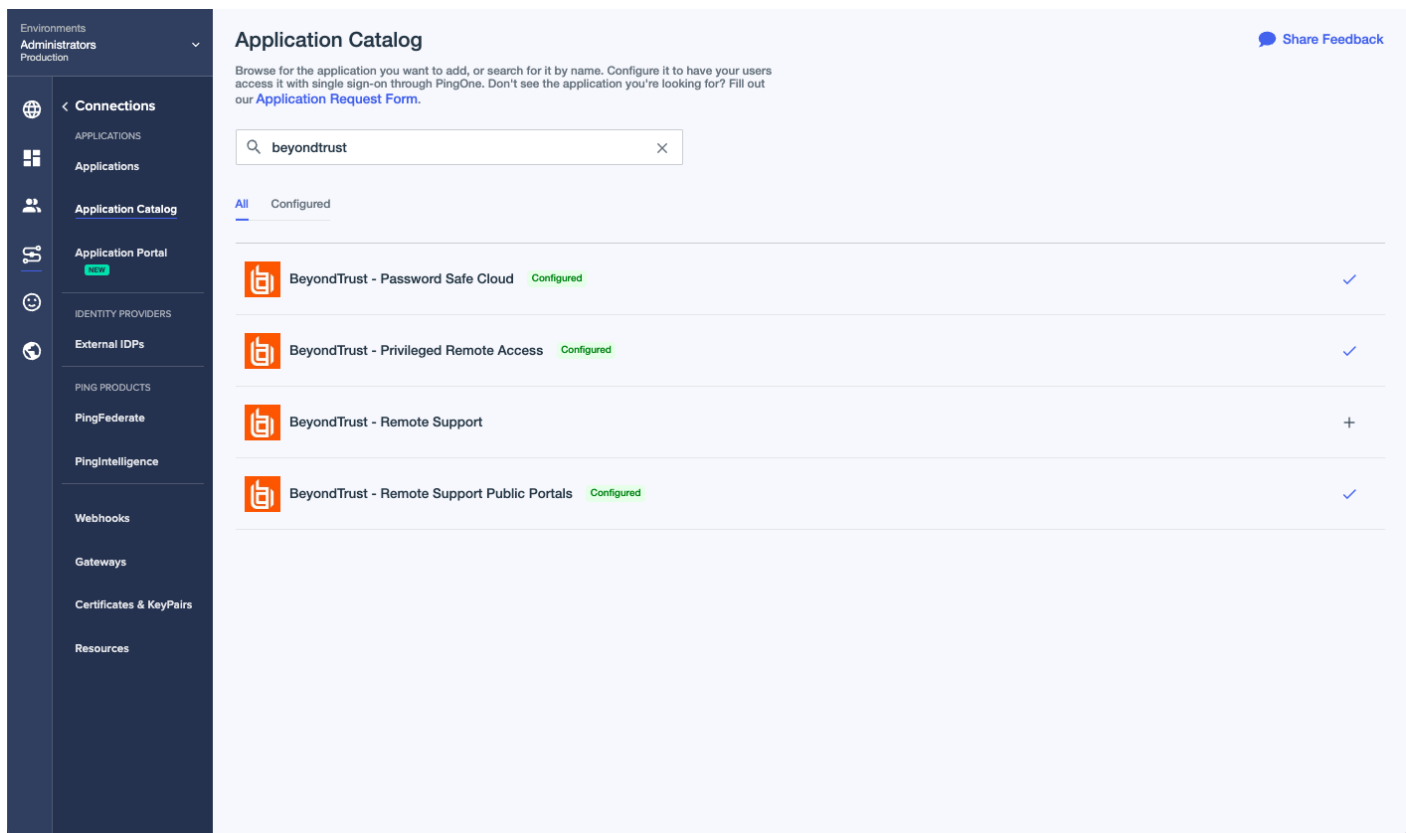
Configure SAML 2.0 for Remote Support using Ping Identity PingOne

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:

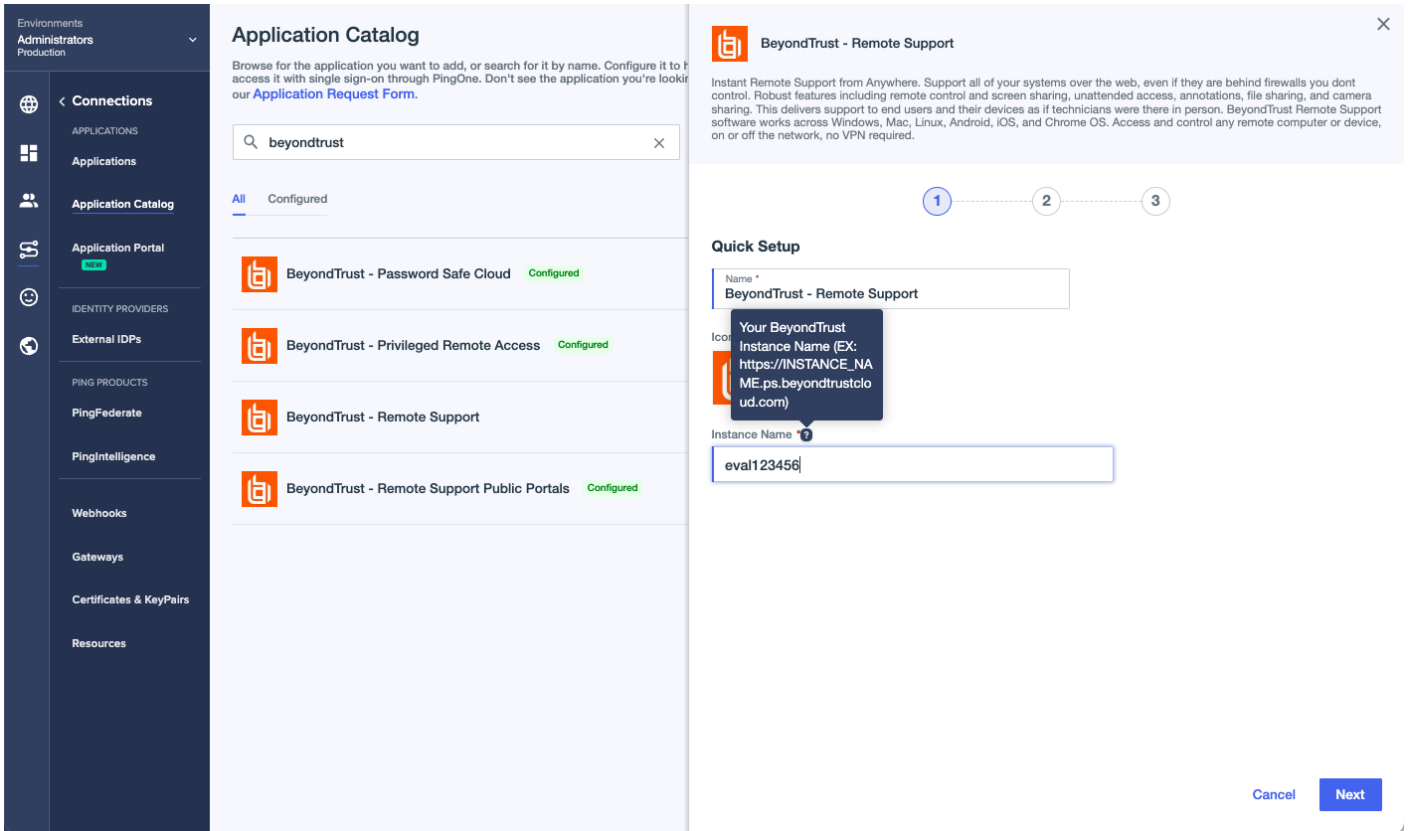
1. Log in to PingOne.
2. Navigate to the **Application Catalog**.
3. Search for *BeyondTrust*. The search results show the various BeyondTrust applications and their configuration status.



The screenshot shows the PingOne Application Catalog interface. The left sidebar contains navigation options: Environments (Production), Administrators, Connections (Applications, Application Catalog, Application Portal), IDENTITY PROVIDERS (External IDPs), PING PRODUCTS (PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, Resources), and a Share Feedback button. The main content area is titled 'Application Catalog' and features a search bar with 'beyondtrust' entered. Below the search bar, there are tabs for 'All' and 'Configured'. The search results list four applications:

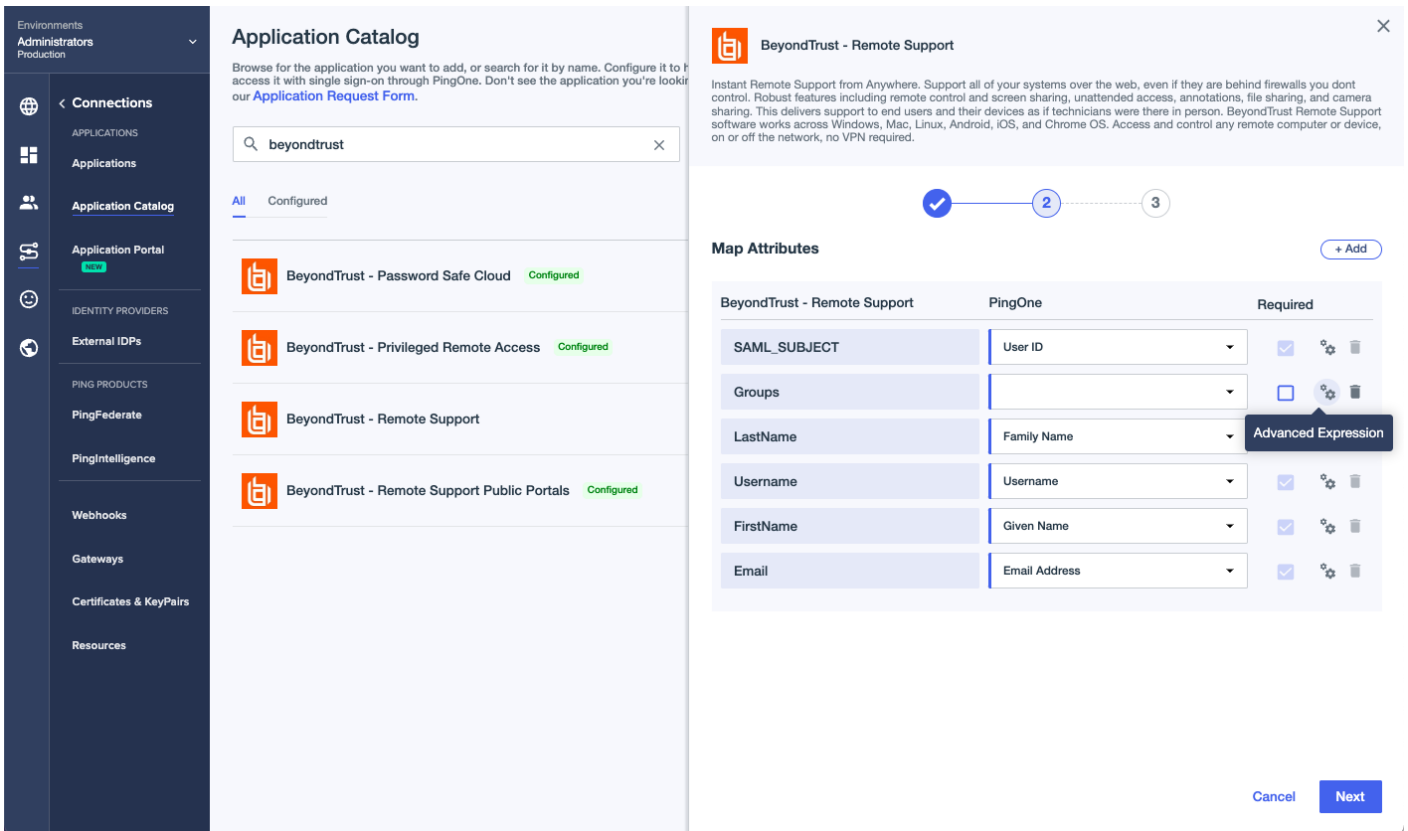
Application Name	Status	Action
BeyondTrust - Password Safe Cloud	Configured	✓
BeyondTrust - Privileged Remote Access	Configured	✓
BeyondTrust - Remote Support		+
BeyondTrust - Remote Support Public Portals	Configured	✓

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

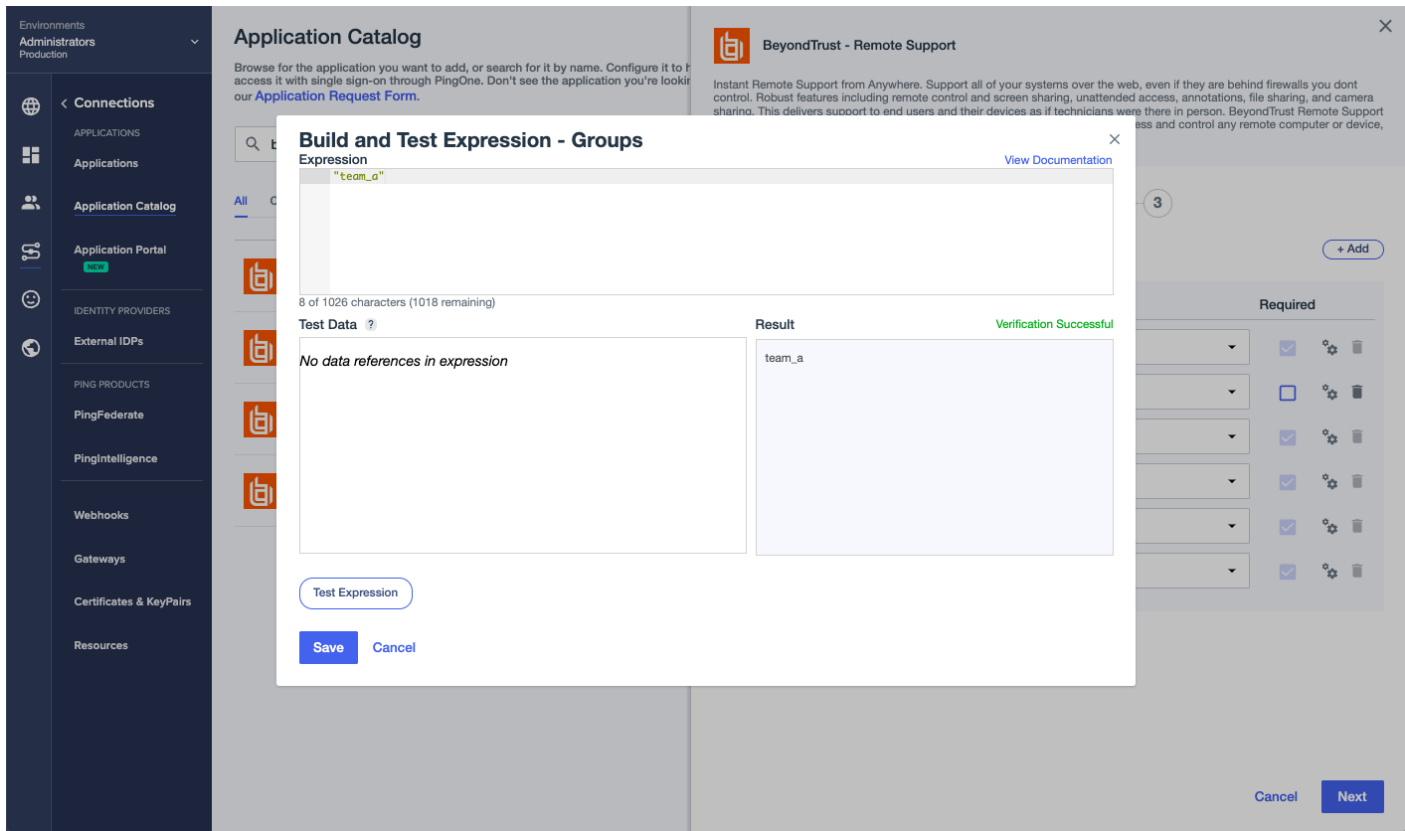


The screenshot shows the BeyondTrust Application Catalog interface. On the left is a navigation sidebar with categories like Environments, Administrators, Connections, Applications, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main area is titled "Application Catalog" and contains a search bar with "beyondtrust" entered. Below the search bar, there are four application entries, each with a BeyondTrust icon and a status: "BeyondTrust - Password Safe Cloud" (Configured), "BeyondTrust - Privileged Remote Access" (Configured), "BeyondTrust - Remote Support" (highlighted), and "BeyondTrust - Remote Support Public Portals" (Configured). A modal window titled "BeyondTrust - Remote Support" is open on the right. It contains a "Quick Setup" section with a "Name" field containing "BeyondTrust - Remote Support" and an "Instance Name" field containing "eval123456". A tooltip points to the Instance Name field, providing an example: "Your BeyondTrust Instance Name (EX: https://INSTANCE_NAME.ps.beyondtrustcloud.com)". At the bottom right of the modal are "Cancel" and "Next" buttons.

6. Click **Next**.



- 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.
- The Map Attributes page should look like the image below.



The screenshot displays the BeyondTrust Application Catalog interface. A modal dialog titled "Build and Test Expression - Groups" is open, showing an expression field with the value "team_a". Below the expression field, there is a "Test Data" section with the message "No data references in expression" and a "Result" section showing "team_a" with a "Verification Successful" status. The dialog includes "Test Expression", "Save", and "Cancel" buttons. In the background, the "BeyondTrust - Remote Support" application is visible, and a "Next" button is located at the bottom right of the main interface.

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

Environments
Administrators
Production

< Connections

APPLICATIONS

Applications

Application Catalog

Application Portal
NEW

IDENTITY PROVIDERS

External IDPs

PING PRODUCTS

PingFederate

PingIntelligence

Webhooks

Gateways

Certificates & KeyPairs

Resources

Application Catalog

Browse for the application you want to add, or search for it by name. Configure it to be accessed with single sign-on through PingOne. Don't see the application you're looking for? Contact our [Application Request Form](#).

All Configured

- BeyondTrust - Password Safe Cloud Configured
- BeyondTrust - Privileged Remote Access Configured
- BeyondTrust - Remote Support
- BeyondTrust - Remote Support Public Portals Configured

BeyondTrust - Remote Support
✕

Instant Remote Support from Anywhere. Support all of your systems over the web, even if they are behind firewalls you don't control. Robust features including remote control and screen sharing, unattended access, annotations, file sharing, and camera sharing. This delivers support to end users and their devices as if technicians were there in person. BeyondTrust Remote Support software works across Windows, Mac, Linux, Android, iOS, and Chrome OS. Access and control any remote computer or device, on or off the network, no VPN required.

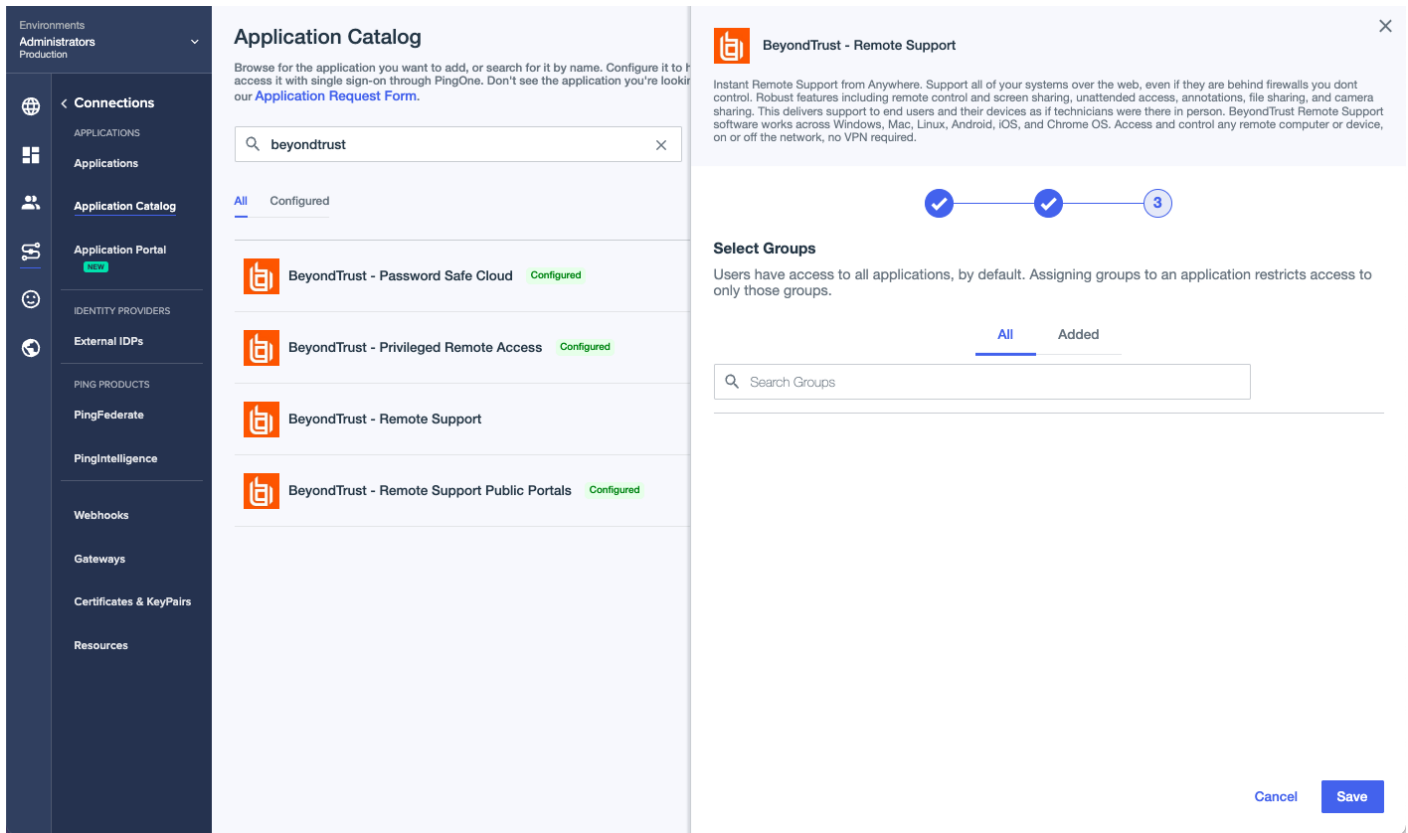
1 — 2 — 3

Map Attributes + Add

BeyondTrust - Remote Support	PingOne	Required
SAML_SUBJECT	User ID	<input checked="" type="checkbox"/>
Groups	Expression: \${"team_a"}	<input type="checkbox"/>
LastName	Family Name	<input checked="" type="checkbox"/>
Username	Username	<input checked="" type="checkbox"/>
FirstName	Given Name	<input checked="" type="checkbox"/>
Email	Email Address	<input checked="" type="checkbox"/>

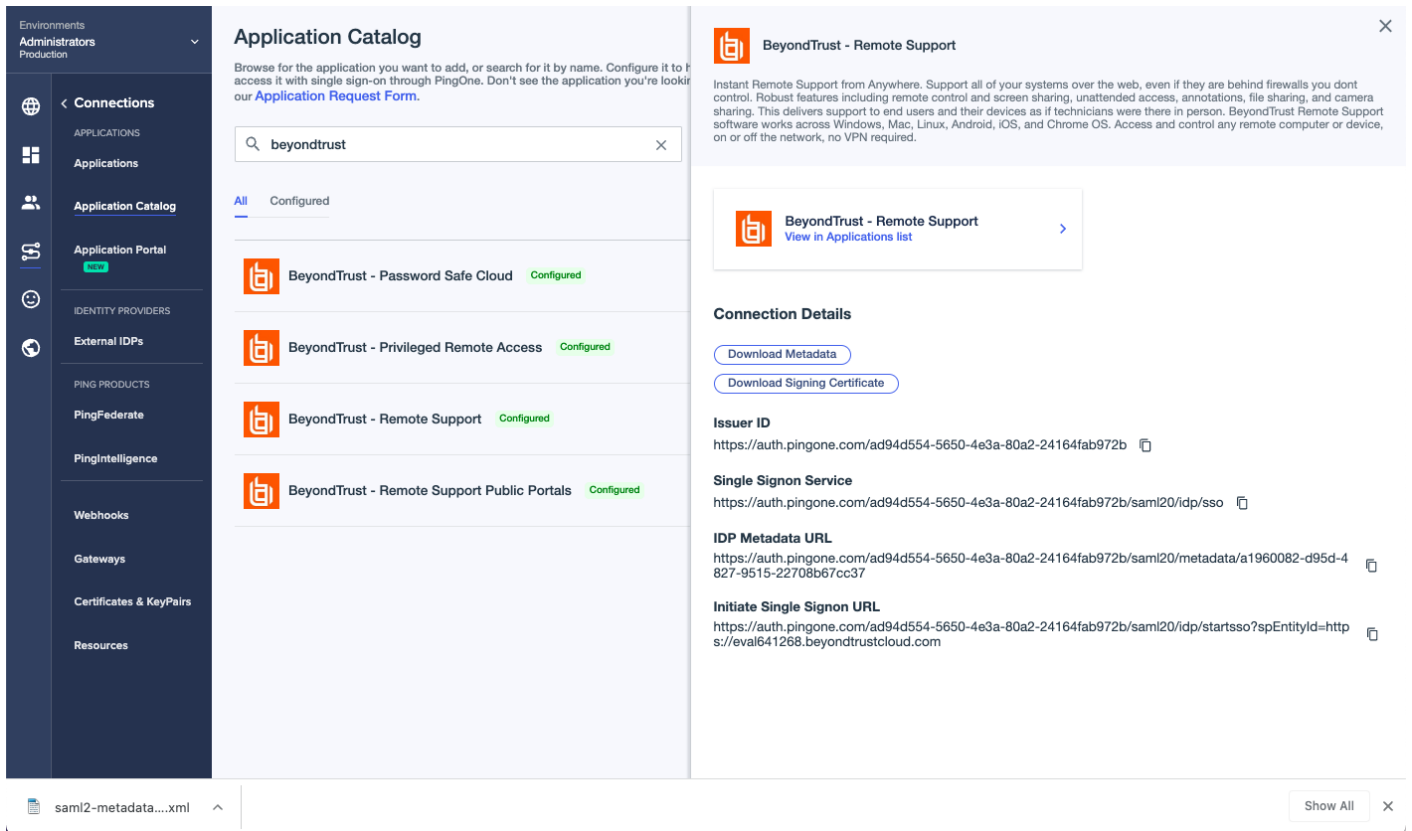
Cancel Next

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



The screenshot displays the 'Application Catalog' interface. On the left is a navigation sidebar with categories like 'Connections', 'Applications', 'Application Portal', 'Identity Providers', 'Ping Products', and 'Webhooks'. The main area shows a search for 'beyondtrust' with a list of four applications, all marked as 'Configured'. A modal window titled 'BeyondTrust - Remote Support' is open, showing a progress indicator with three steps (the third is active), a 'Select Groups' section with a search bar, and 'All' and 'Added' tabs. 'Cancel' and 'Save' buttons are at the bottom right of the modal.

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



The screenshot displays the BeyondTrust Application Catalog interface. On the left is a navigation sidebar with categories like Environments, Administrators, Connections, Applications, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main content area is titled "Application Catalog" and shows a search for "beyondtrust" with a list of four configured applications: BeyondTrust - Password Safe Cloud, BeyondTrust - Privileged Remote Access, BeyondTrust - Remote Support, and BeyondTrust - Remote Support Public Portals. A detailed view for "BeyondTrust - Remote Support" is open on the right, showing connection details such as Issuer ID, Single Signon Service, IDP Metadata URL, and Initiate Single Signon URL. A file browser at the bottom shows a file named "saml2-metadata....xml".

12. Continue the configuration in BeyondTrust Remote Support.

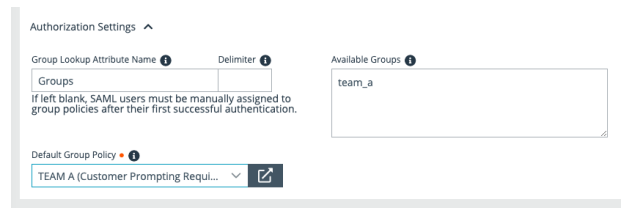
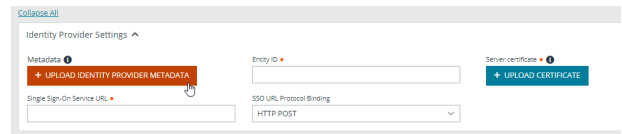
Configure Remote Support Representatives for PingOne

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

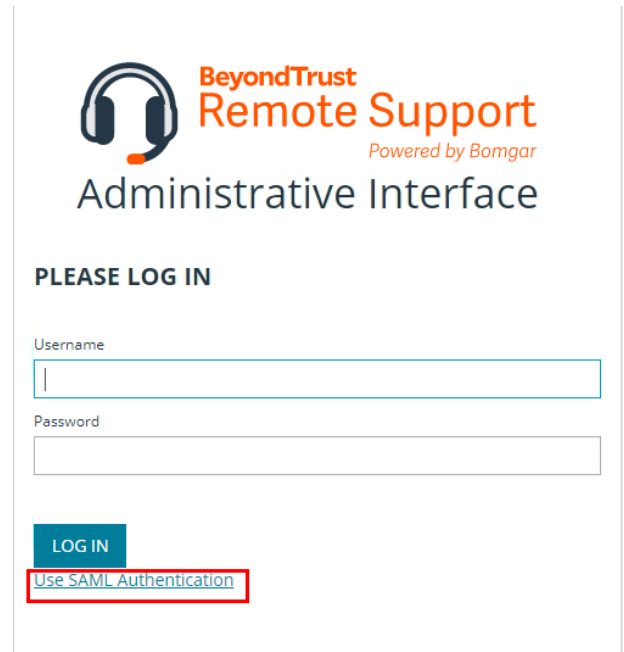
1. Log in to BeyondTrust Remote Support.
2. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
3. Click **Add** and select **SAML for Representatives**.
4. Enter a name to identify this provider, such as *SAML For Representatives*.



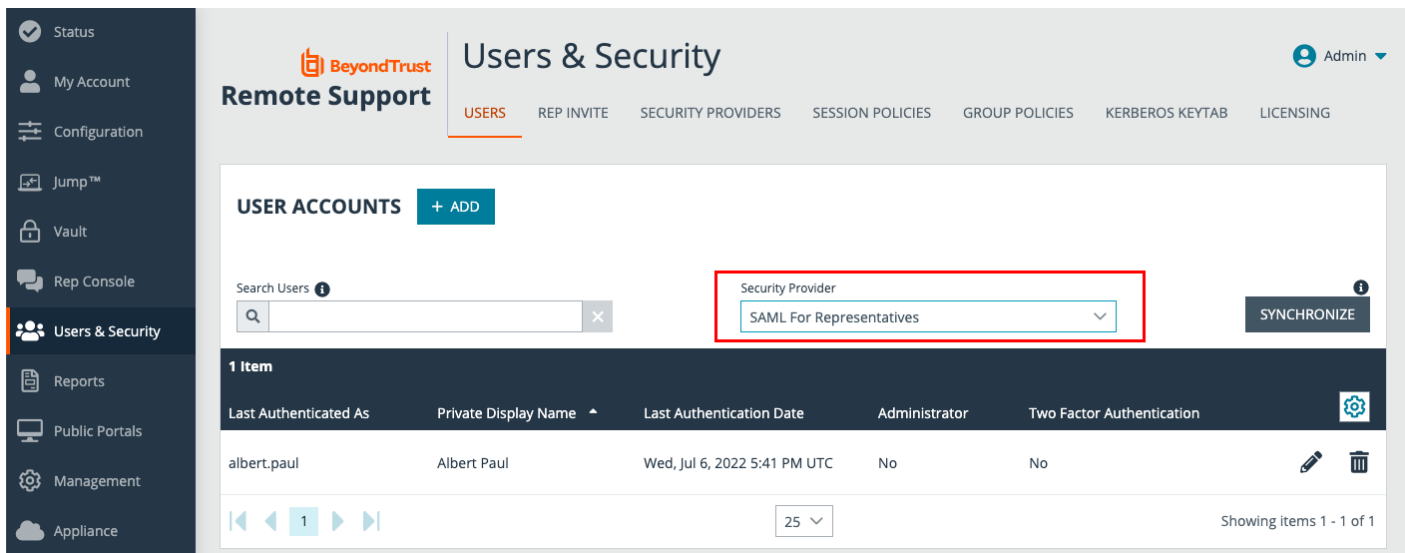
5. Under **Identity Provider Settings**, click **UPLOAD IDENTITY PROVIDER METADATA**.
6. Browse to the metadata file downloaded from PingOne and select it.
7. The **Single Sign-On Service URL** and the **Entity ID** are populated by the metadata file. Leave the **SSO URL Protocol Binding** as *HTTP POST*.
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.



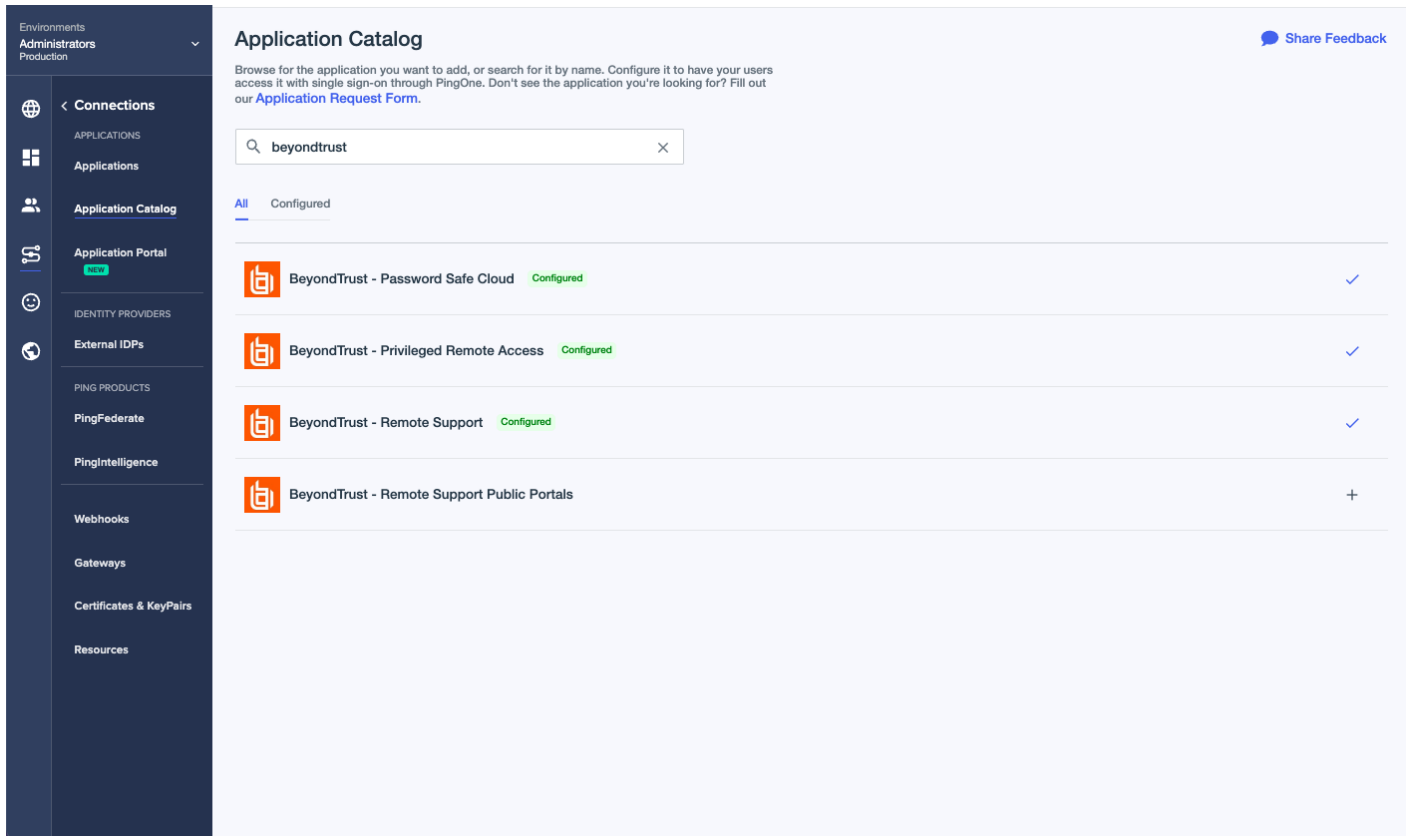
SAML Users are managed by the Identity Provider, which is PingOne.



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:

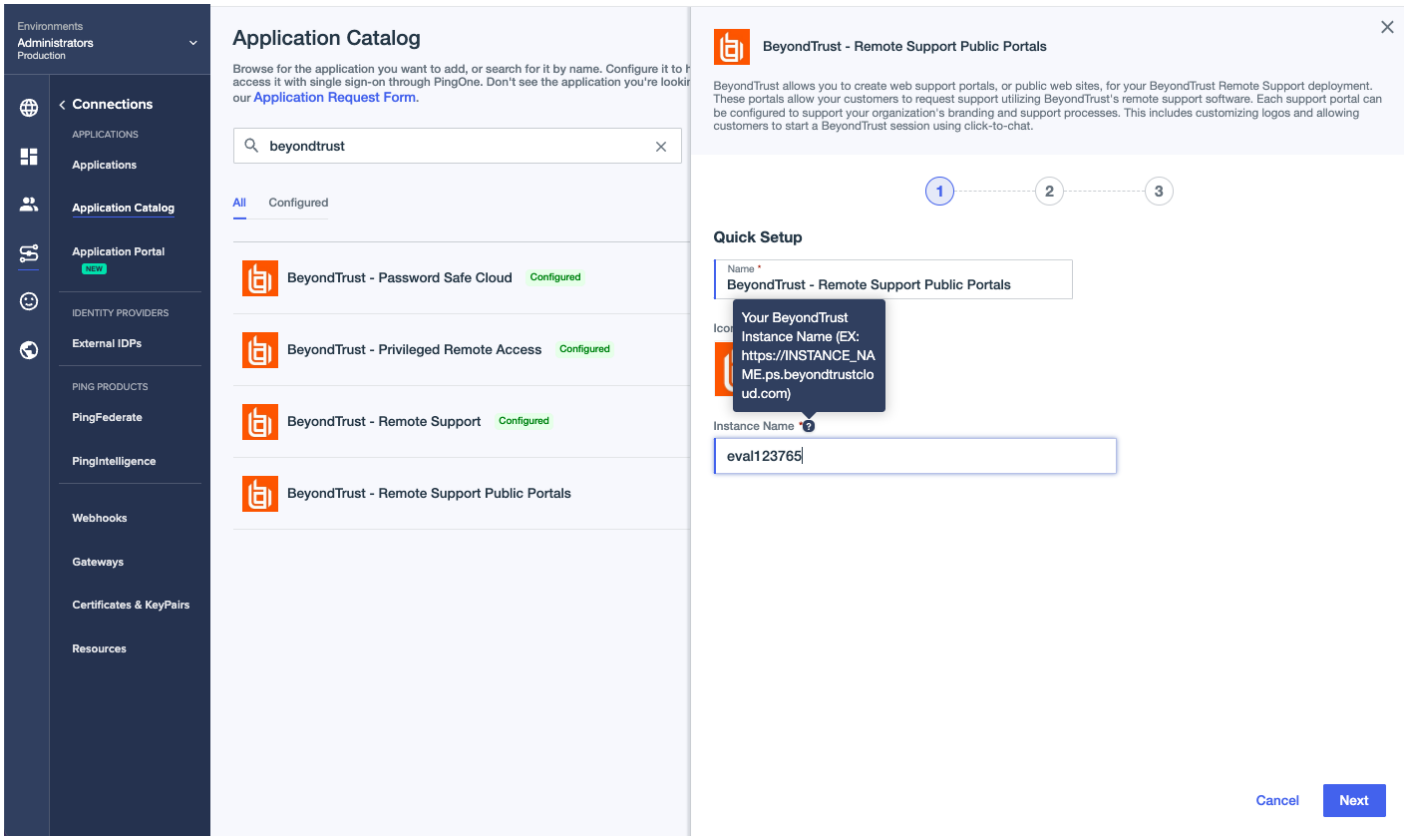
1. Log in to PingOne.
2. Navigate to the **Application Catalog**.
3. Search for *BeyondTrust*. The search results show the various BeyondTrust applications and their configuration status.



The screenshot displays the PingOne Application Catalog interface. On the left is a dark navigation sidebar with categories like Connections, Applications, Application Portal, Identity Providers, Ping Products, and Webhooks. The main content area is titled "Application Catalog" and includes a search bar with "beyondtrust" entered. Below the search bar, there are tabs for "All" and "Configured". A list of four applications is shown, each with a BeyondTrust logo, name, and status:

Application Name	Status	Action
BeyondTrust - Password Safe Cloud	Configured	✓
BeyondTrust - Privileged Remote Access	Configured	✓
BeyondTrust - Remote Support	Configured	✓
BeyondTrust - Remote Support Public Portals		+

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



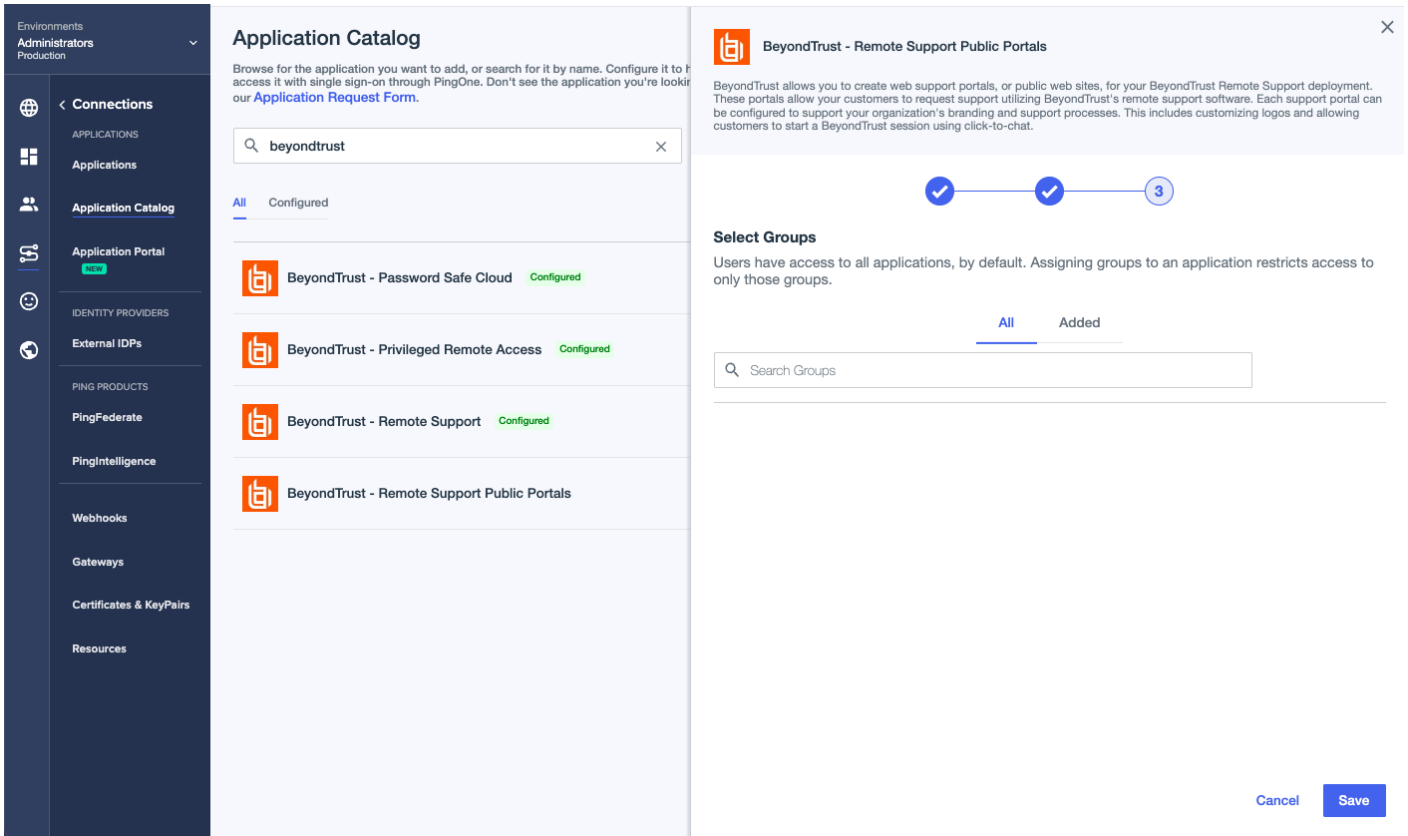
The screenshot shows the BeyondTrust Administration console. On the left is a navigation sidebar with categories like Environments, Administrators, Connections, Applications, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main area displays the 'Application Catalog' with a search bar containing 'beyondtrust' and a list of applications, including 'BeyondTrust - Remote Support Public Portals'. A configuration window for this application is open on the right, showing a 'Quick Setup' section with a 'Name' field containing 'BeyondTrust - Remote Support Public Portals' and an 'Instance Name' field containing 'eval123765'. A tooltip explains the Instance Name format: 'Your BeyondTrust Instance Name (EX: https://INSTANCE_NAME.ps.beyondtrustcloud.com)'. At the bottom right of the window are 'Cancel' and 'Next' buttons.

6. Click **Next**.

The screenshot shows the 'Application Catalog' interface. On the left is a navigation sidebar with categories like 'Connections', 'Applications', 'Application Portal', 'Identity Providers', 'Ping Products', and 'Webhooks'. The main area displays a search for 'beyondtrust' with a list of applications, including 'BeyondTrust - Remote Support Public Portals'. A modal window titled 'BeyondTrust - Remote Support Public Portals' is open, showing a progress indicator with step 2 selected. Below the progress indicator is the 'Map Attributes' section, which contains a table mapping attributes from the application to PingOne attributes.

BeyondTrust - Remote Support Public Portals	PingOne	Required
SAML_SUBJECT	User ID	<input checked="" type="checkbox"/>
LastName	Family Name	<input checked="" type="checkbox"/>
FirstName	Given Name	<input checked="" type="checkbox"/>
Username	Username	<input checked="" type="checkbox"/>
Email	Email Address	<input checked="" type="checkbox"/>

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



The screenshot displays the BeyondTrust Administration console. On the left is a navigation sidebar with categories like Environments, Administrators, Connections, Applications, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main area is titled 'Application Catalog' and shows a search for 'beyondtrust' with a list of four applications, all marked as 'Configured'. A modal window titled 'BeyondTrust - Remote Support Public Portals' is open, showing a progress indicator with three steps (1, 2, 3), where steps 1 and 2 are completed. Below the progress bar is a 'Select Groups' section with a description: 'Users have access to all applications, by default. Assigning groups to an application restricts access to only those groups.' There are tabs for 'All' and 'Added', and a search box for groups. At the bottom right of the modal are 'Cancel' and 'Save' buttons.

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

Application Catalog

Browse for the application you want to add, or search for it by name. Configure it to be accessed with single sign-on through PingOne. Don't see the application you're looking for? Visit our [Application Request Form](#).

Search:

All Configured

- BeyondTrust - Password Safe Cloud Configured
- BeyondTrust - Privileged Remote Access Configured
- BeyondTrust - Remote Support Configured
- BeyondTrust - Remote Support Public Portals Configured

BeyondTrust - Remote Support Public Portals

BeyondTrust allows you to create web support portals, or public web sites, for your BeyondTrust Remote Support deployment. These portals allow your customers to request support utilizing BeyondTrust's remote support software. Each support portal can be configured to support your organization's branding and support processes. This includes customizing logos and allowing customers to start a BeyondTrust session using click-to-chat.

BeyondTrust - Remote Support Public Portals
[View in Applications list](#)

Connection Details

- [Download Metadata](#)
- [Download Signing Certificate](#)

Issuer ID
<https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b>

Single Signon Service
<https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/ldap/sso>

IDP Metadata URL
<https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/metadata/8298d701-fb2f-49c2-85fe-3bbe2f9b7a0b>

Initiate Single Signon URL
https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/ldap/startssso?spEntityId=https://eval641268.beyondtrustcloud.com/public_portal

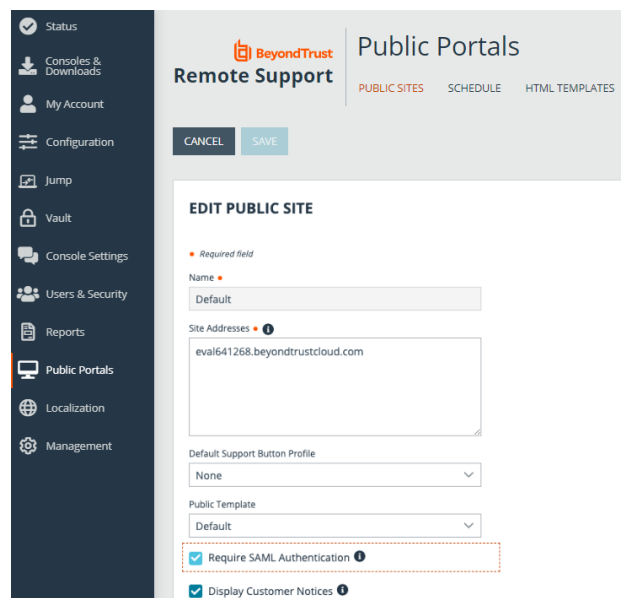
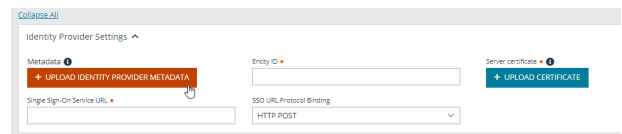
saml2-metadata....xml [Show All](#)

10. Continue the configuration in BeyondTrust Remote Support.

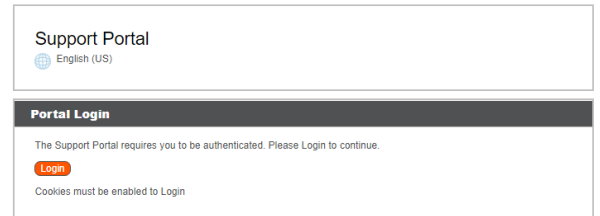
Configure Remote Support Portals for PingOne

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

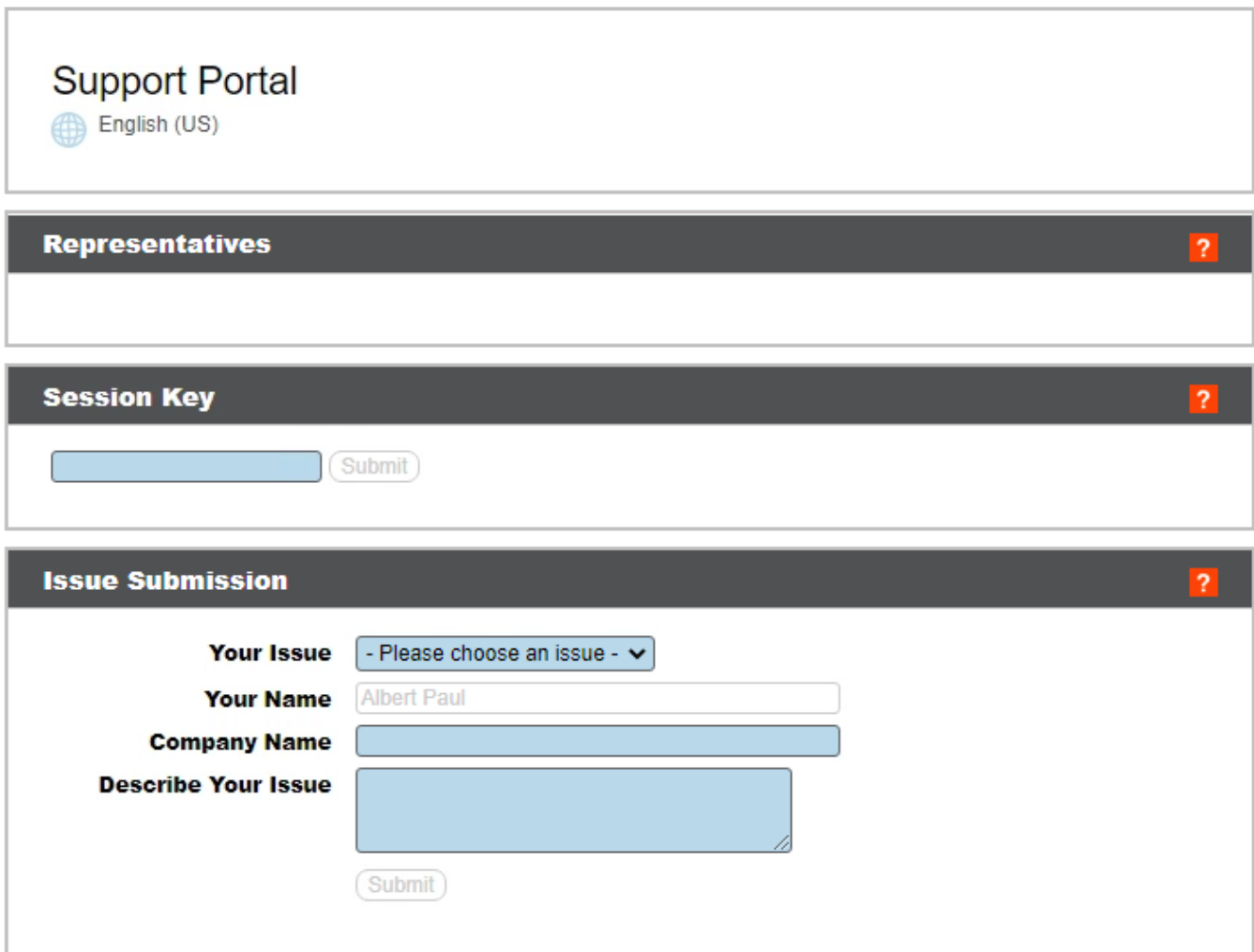
1. Log in to BeyondTrust Remote Support.
2. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
3. Click **Add** and select **SAML for Public Portals**.
4. Enter a name to identify this provider, such as *SAML-For-Public-Portals*.
5. Under **Identity Provider Settings**,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



Copyright © 2002-2021 BeyondTrust Corporation. Redistribution Prohibited. All Rights Reserved.

BeyondTrust Remote Support