



# BeyondTrust

## **Privileged Remote Access Ping Identity PingOne Integration**

## Table of Contents

---

<b>Configure SAML 2.0 for Privileged Remote Access using Ping Identity PingOne .....</b>	<b>3</b>
<b>Configure PingOne for Privileged Remote Access .....</b>	<b>4</b>
<b>Configure Privileged Remote Access for PingOne .....</b>	<b>11</b>

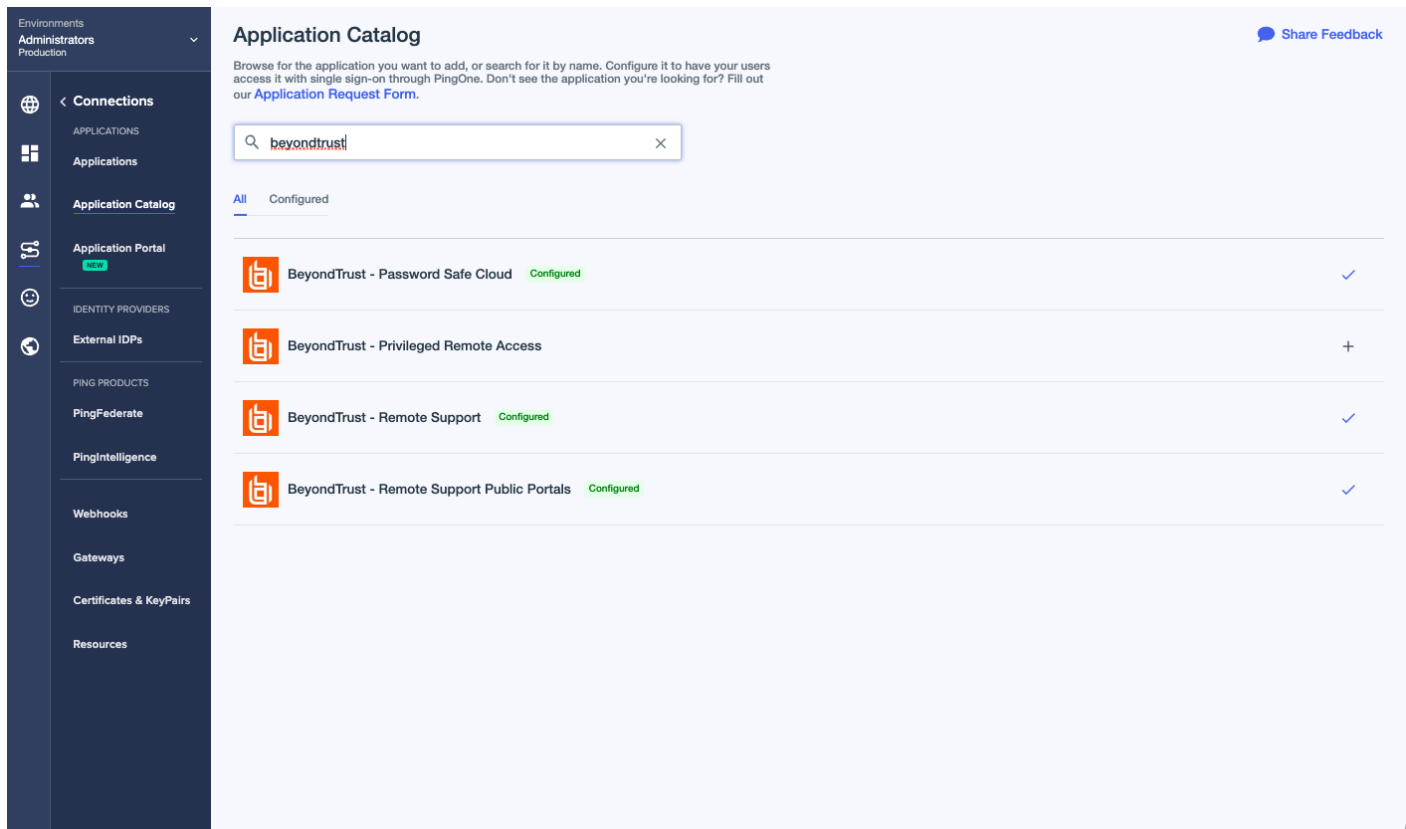
# Configure SAML 2.0 for Privileged Remote Access using Ping Identity PingOne

Ping Identity offers a PingOne SSO solution that integrates with BeyondTrust Privileged Remote Access. This guide shows how to configure PingOne and Privileged Remote Access integrations.

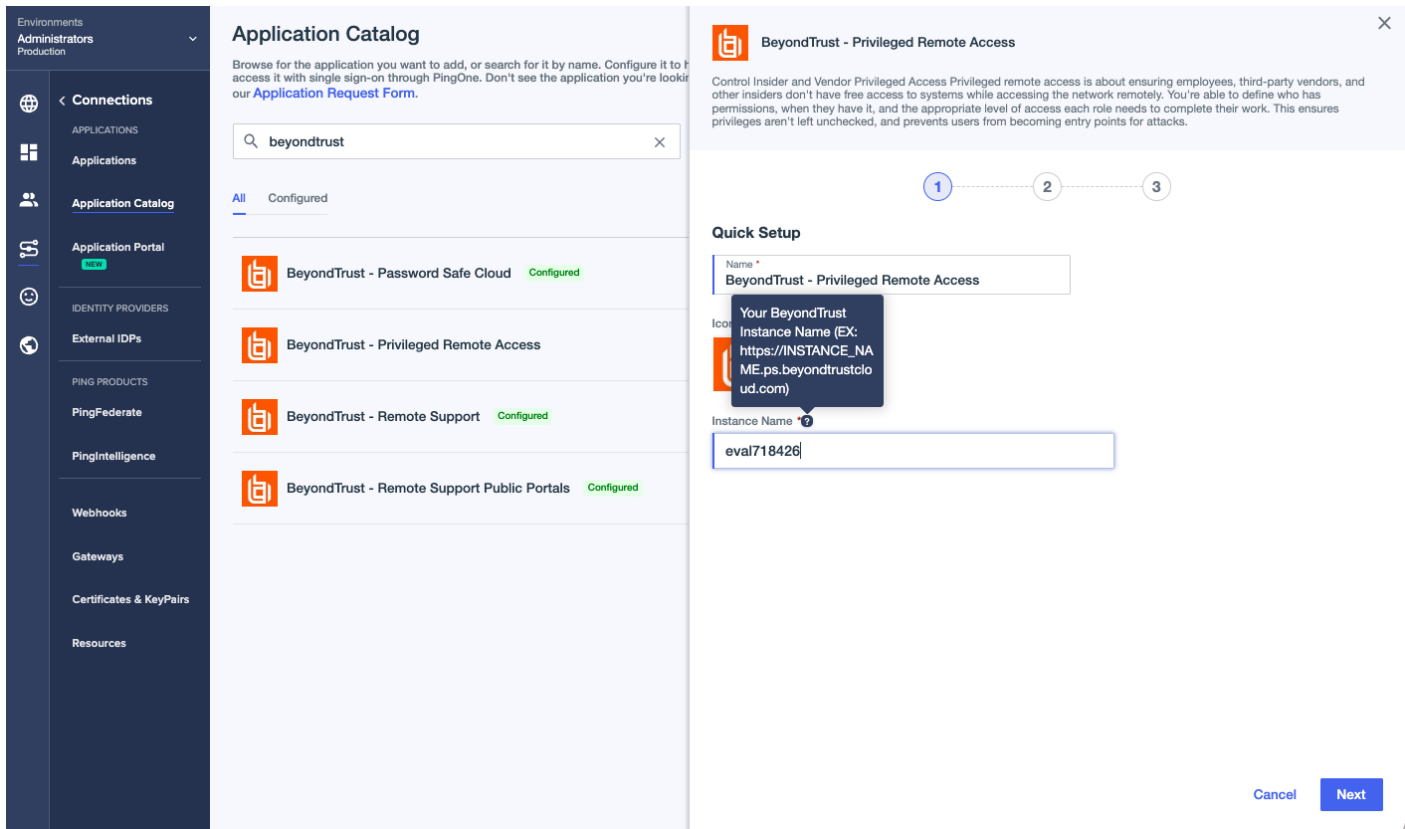
# Configure PingOne for Privileged Remote Access

Configuring the PingOne integration with BeyondTrust Privileged Remote Access 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.

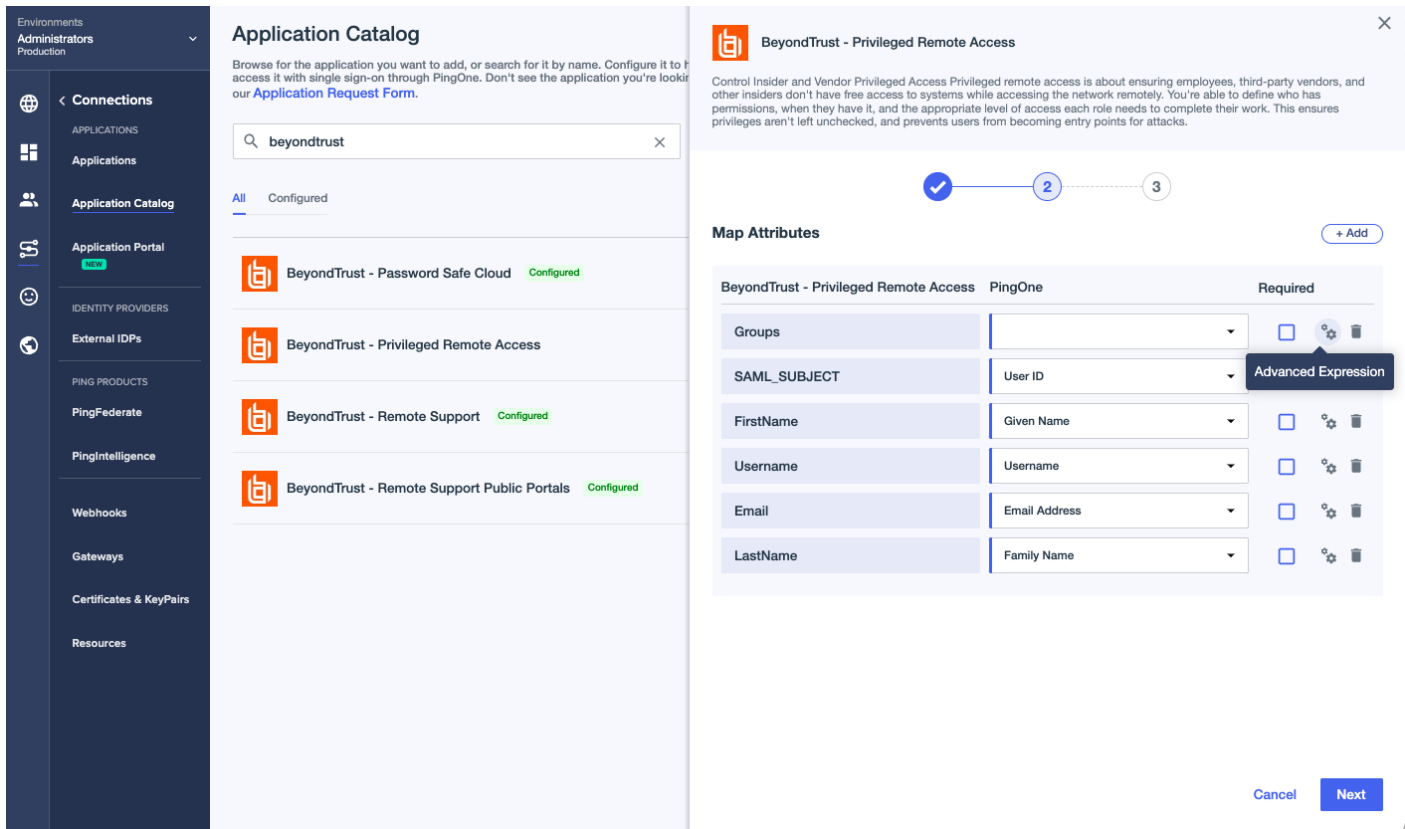


4. Click the **+** icon at the end of the row for **BeyondTrust - Privileged Remote Access**.
5. Enter your instance name.

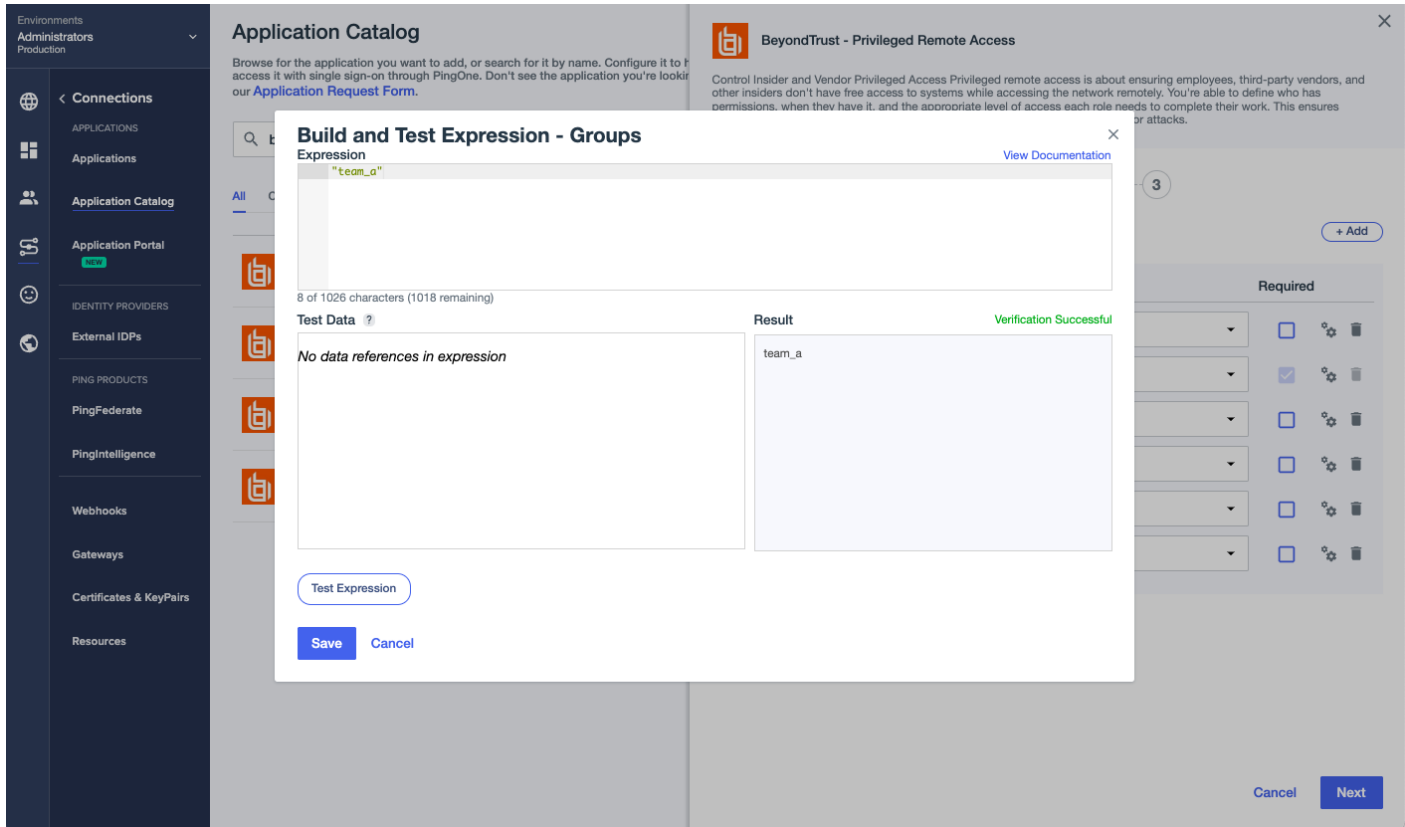


The screenshot shows the BeyondTrust Application Catalog interface. On the left is a navigation sidebar with categories like Administrators, Connections, Applications, Application Catalog, Application Portal, Identity Providers, External IDPs, Ping Products, PingFederate, PingIntelligence, Webhooks, Gateways, Certificates & KeyPairs, and Resources. The main area displays the 'Application Catalog' with a search bar containing 'beyondtrust'. Below the search bar, there are filters for 'All' and 'Configured'. A list of applications is shown, including 'BeyondTrust - Password Safe Cloud', 'BeyondTrust - Privileged Remote Access', 'BeyondTrust - Remote Support', and 'BeyondTrust - Remote Support Public Portals'. A modal window titled 'BeyondTrust - Privileged Remote Access' is open, showing a 'Quick Setup' form. The form includes a 'Name' field with the value 'BeyondTrust - Privileged Remote Access', an 'Instance Name' field with the value 'eval718426', and a 'Next' button.

6. Click **Next**.



- On the Map Attributes page, complete the configuration for the Groups attribute. Privileged Remote Access 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 Privileged Remote Access. In this example, `team_a` is used.
- The Map Attributes page should look like the image below.



The screenshot displays the BeyondTrust Privileged Remote Access interface. A modal dialog titled "Build and Test Expression - Groups" is open, showing an expression field with the text `"team_a"`. Below the expression field, it indicates "8 of 1026 characters (1018 remaining)". The dialog is divided into two sections: "Test Data" and "Result". The "Test Data" section shows "No data references in expression". The "Result" section shows "Verification Successful" and the output `team_a`. At the bottom of the dialog, there are buttons for "Test Expression", "Save", and "Cancel". In the background, the "Application Catalog" is visible, and a "Required" section on the right side of the interface shows a list of items with checkboxes and settings icons.

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 access it 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
- BeyondTrust - Remote Support Configured
- BeyondTrust - Remote Support Public Portals Configured

BeyondTrust - Privileged Remote Access
✕

Control Insider and Vendor Privileged Access Privileged remote access is about ensuring employees, third-party vendors, and other insiders don't have free access to systems while accessing the network remotely. You're able to define who has permissions, when they have it, and the appropriate level of access each role needs to complete their work. This ensures privileges aren't left unchecked, and prevents users from becoming entry points for attacks.

1
2
3

#### Map Attributes

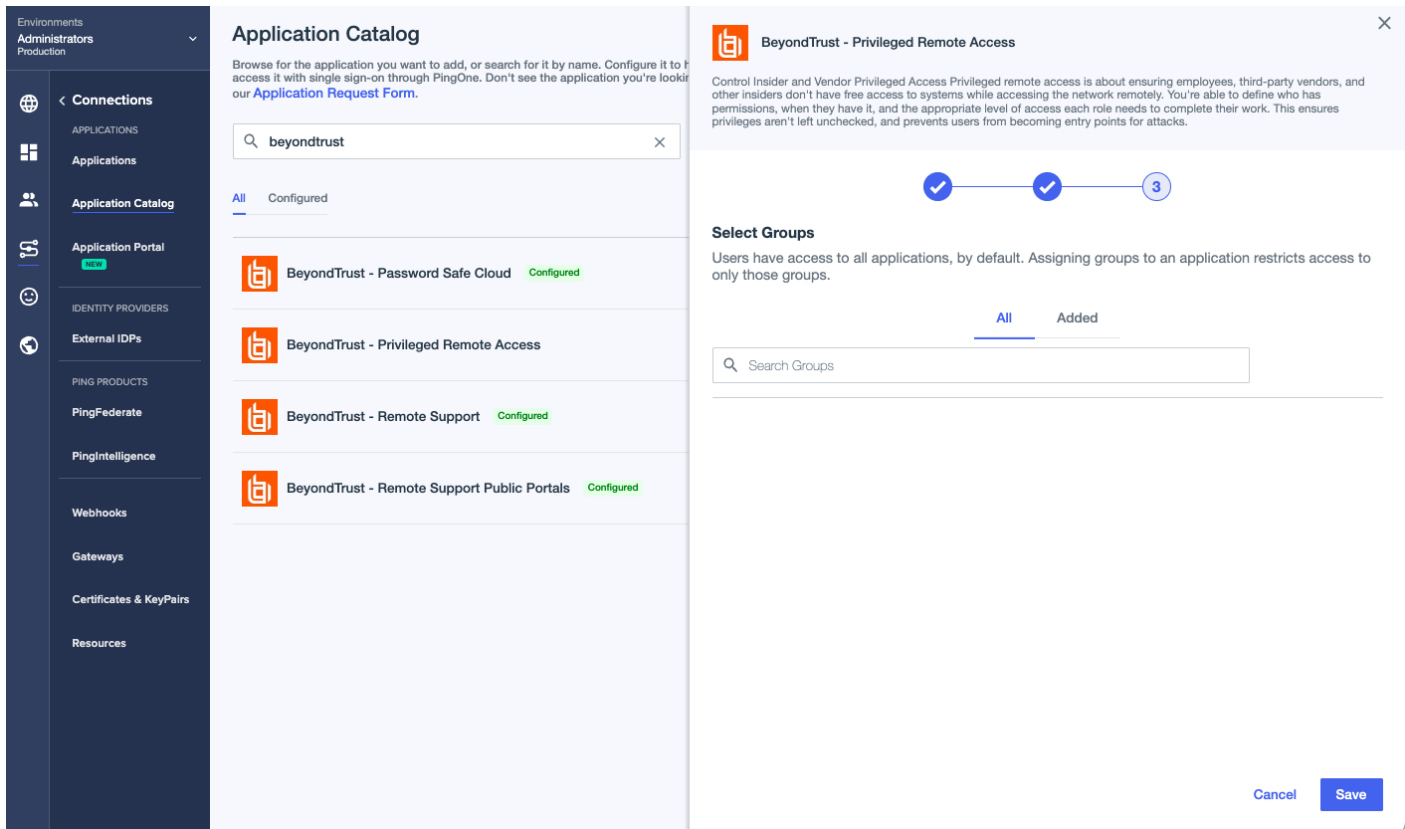
+ Add

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

Cancel
Next

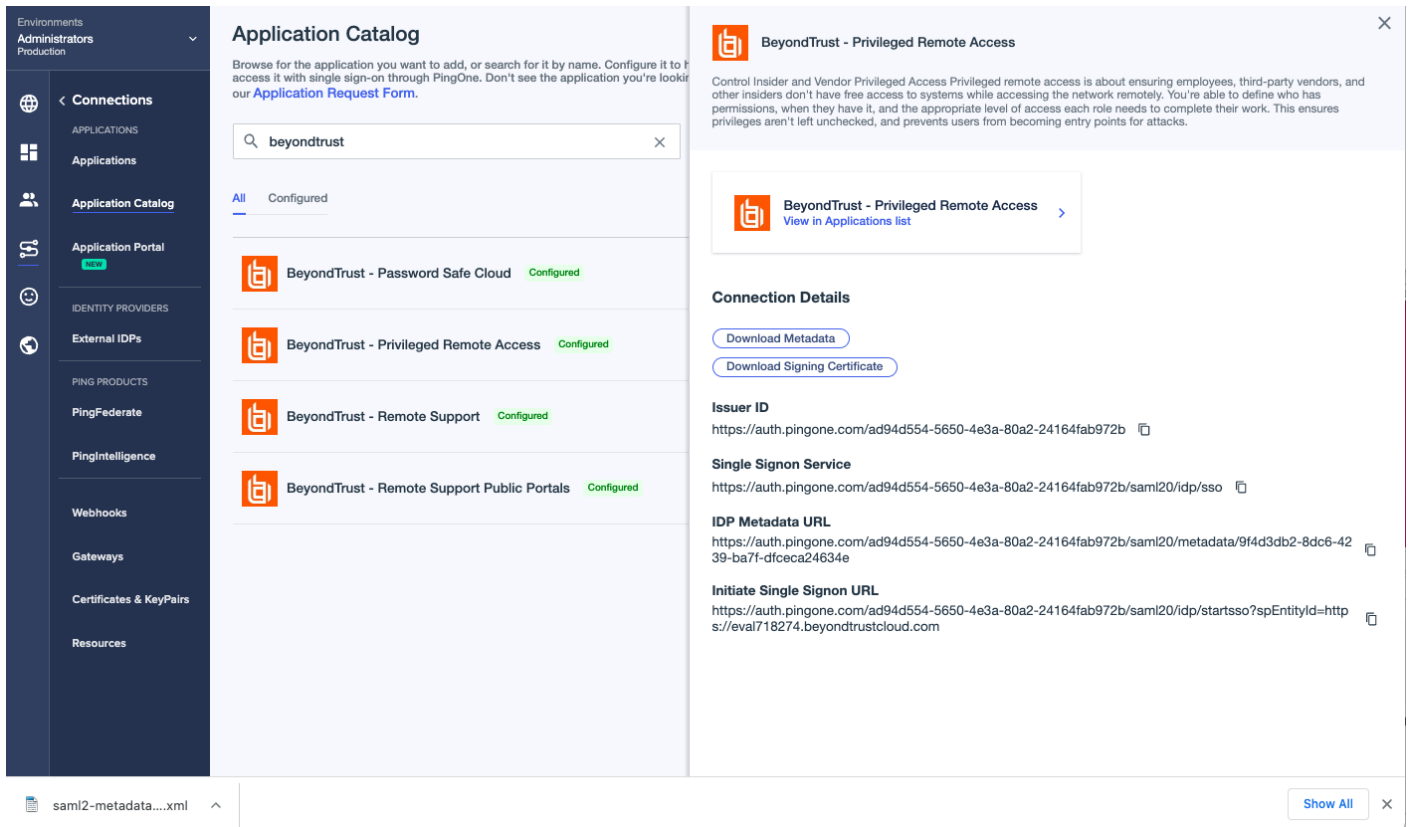
10. Access Control Groups in PingOne can be used to limit access to the Application. Leave the page empty for now and click **Save**.





The screenshot displays the BeyondTrust Application Catalog interface. On the left is a navigation sidebar with categories like Administrators, Connections, Applications, Application Catalog, 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 tabs for 'All' and 'Configured'. A list of applications is shown, including 'BeyondTrust - Password Safe Cloud', 'BeyondTrust - Privileged Remote Access', 'BeyondTrust - Remote Support', and 'BeyondTrust - Remote Support Public Portals', each with a 'Configured' status. An overlay window titled 'BeyondTrust - Privileged Remote Access' is open on the right, showing a progress indicator with three steps (1, 2, 3), where steps 1 and 2 are completed. The 'Select Groups' section is active, with a search bar for 'Search Groups' and tabs for 'All' and 'Added'. 'Cancel' and 'Save' buttons are at the bottom right of the overlay.

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



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', 'Webhooks', 'Gateways', 'Certificates & KeyPairs', and 'Resources'. The main area shows a search for 'beyondtrust' with a list of four configured applications:

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

A modal window is open for 'BeyondTrust - Privileged Remote Access', providing the following details:

- 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/ldp/ssp`
- IDP Metadata URL:** `https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/metadata/9f4d3db2-8dc6-4239-ba71-dfeca24634e`
- Initiate Single Signon URL:** `https://auth.pingone.com/ad94d554-5650-4e3a-80a2-24164fab972b/saml20/ldp/startssos?spEntityId=https://eval718274.beyondtrustcloud.com`

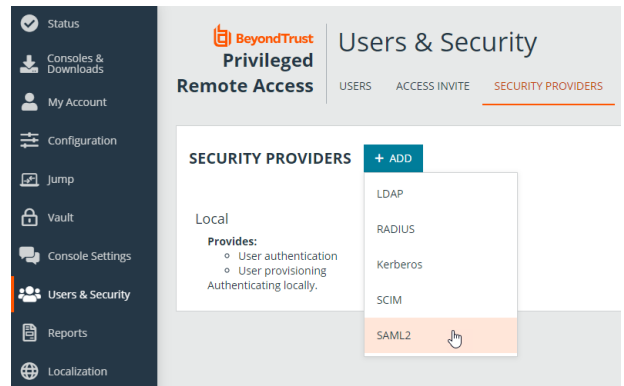
At the bottom of the modal, there is a 'Show All' button.

12. Continue the configuration in BeyondTrust Privileged Remote Access.

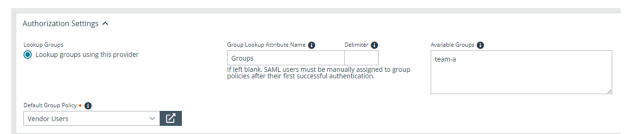
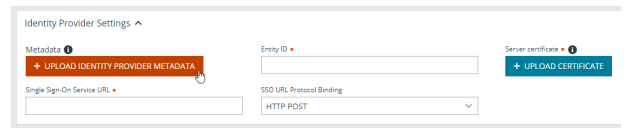
# Configure Privileged Remote Access for PingOne

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

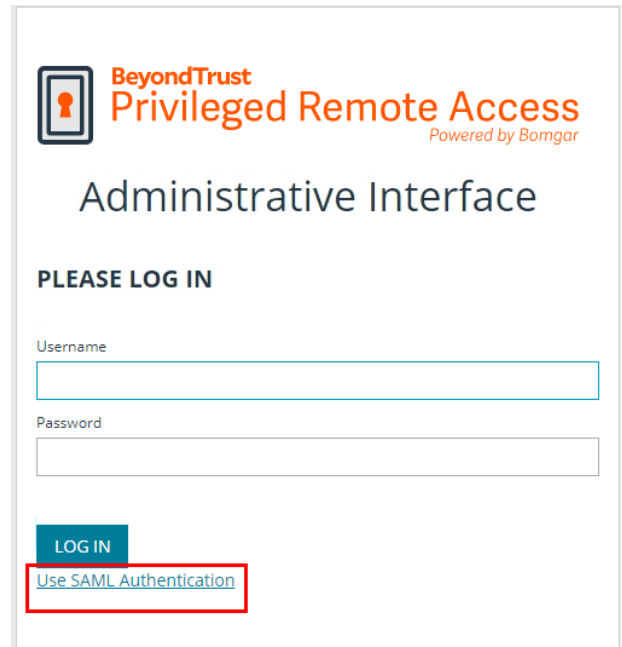
1. Log in to BeyondTrust Privileged Remote Access.
2. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
3. Click **Add** and select **SAML**.
4. Enter a name to identify this provider, such as *SAML2*.



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. Privileged Remote Access 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.

