# BeyondTrust

### Privileged Remote Access PortalGuard Integration Guide

2

#### **Table of Contents**

Integrate BeyondTrust Privileged Remote Access with PortalGuard	3
Configure Privileged Remote Access for Integration with PortalGuard	3
Configure PortalGuard for Integration with Privileged Remote Access	4

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

#### Integrate BeyondTrust Privileged Remote Access with PortalGuard

Integrating BeyondTrust Privileged Remote Access with Bio-key PortalGuard's Identity and Access Management platform provides multifactor authentication with Identity-Bound Biometrics. Bio-key portal guard allows for biometric support including voice recognition, which provides a flexible yet very secure gate keeper in front of BeyondTrust Privileged Remote Access. At login time, it asks the user to repeat specific words or numbers, and matches the voice patterns. Implementing steps like these helps enforce stronger security and compliance.

#### Configure Privileged Remote Access for Integration with PortalGuard

Configuration of this integration requires obtaining a file from PortalGuard, and then following these steps in BeyondTrust Privileged Remote Access:

- 1. Sign in to PortalGuard.
- Download your PortalGuard metadata by navigating to the following page: <u>https://{YOUR-PG-SITE}.onbio-key.com/sso/metadata.ashx</u>.
- 3. Sign in to the BeyondTrust Privileged Remote Access site.
- 4. Navigate to the Users & Security page, Security Providers tab.
- 5. Click ADD next to Security Providers.



- Upload the metadata downloaded from PortalGaurd to the Privileged Remote Access site by clicking Upload Identity Provider Metadata. This auto-populates the Entity ID, Single Sign-On Service URL, SSO URL Protocol Binding, and the Current Certificate fields.
- 7. Make note of the **Entity ID** and **Assertion Consumer Service URL**. You need these for the PortalGuard configuration.
- 8. Ensure the **User Attribute Settings** fields have the following values:
  - Username: Username
  - E-mail: Email
  - Display Name: {firstName} {LastName}
- 9. Under Authorization Settings, add *Vendor* to the Available Groups. You need at least one available group specified here.
- 10. Select the **Default Group Policy** for this configuration. You can use



HTTP Redirect

vider Settings



3

<sup>©2003-2024</sup> BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or TC: 3/4/2024 depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.



the General Members policy.

11. Click Save.

#### **Configure PortalGuard for Integratio**

.....

- 1. Within the PortalGuard IDaaS Admin Panel, navigate to the Sil Sign On tab within the navigation menu on the left side.
- 2. Click New SAML on the top of the page.



- 3. This opens a new window showing configuration fields for the new SAML SSO connection. Enter the following information:
  - Name: The name of the configuration. This field is not shown to users and is used only within the Admin Panel.
  - Description: Any description info for the configuration. Again, this field is not shown to users and is only used within the Admin Panel.
  - · Enabled: Toggles whether the config is enabled and in use or not. You can disable it if you do not want it to be used at the moment.
  - · Identifiers: The Entity ID from your Privileged Remote Access site.
  - · Binding: Set this to POST.
  - Assertion Consumer URL: The Assertion Consumer Service URL from your Privileged Remote Access site.
  - Use ACS from SAMLRequest: Disabled.
- 4. Navigate to the **Identity Claims** tab on the left side of the SSO configuration.
- 5. Leave the top three settings at the default values. These are Attribute Store, Dynamically Determine Attribute Store, and IdP Signing Certificate.

Attribute Store The attribute store from where identity claims for the user will be pulled. When dynamic attribute store resolution is enabled, the selected Attribute Store acts as the default if no more-specific match is found.	sql [SQL]	\$
Dynamically Determine Attribute Store The attribute store is typically a hard-coded setting. Checking this box will attempt to dynamically choose the correct attribute store. This is done by corregaring a username prefix or suffix against any defined on the Resolution tab of all Allowine these second stores and the store advection and the store attribute store when the second store attribute store above acts as the default if no more-specific match is found.		
IdP Signing Certificate You can now choose which IdP Signing Certificate to use if multiple are defined. If not specifick that current' disfault' cort will be used. Otherwise, you can 'pin' this configuration to use a specific cert. Pinning ensures a cert will be used regardless of whether it is the default.	PGIDaaS	\$

4

	U			6633
🍫 BIO-key	BEYONDTRUST: Sin	gle Sign-On (SSO) 📑	New SAML + New CAS	+ New OAuth + New F
Active Organization	Search by SSO Name Q		Sort By Alphab	etical 🗘 🔳 List View
	BeyondTrust Privileged Bernote Access Connection Type: SAML Active 0 Groups, 0 Users, and	BeyondTrust Remote Support Public Portal Connection Type: SAML Active O Groups, O Users, and	Beyond Rust Remote Support Representatives Connection Type SAML Active O Groups: 0 Users, and	
	Construction Cons	BIC-Key     BEYONDTRUST: Sin      Active Organization      Monorhat     C      three      Search System      Search System	BIC-Key     BEYONDTRUST: Single Sign-On (SSO      Actor Organization      Second Particle      Second Parite      Second Particle      Second Particle      Second Particle	BLC-KCY     BEYONDTRUST: Single Sign-On (SSO • 400 MC) • 100 CO      Actor Organization      Beyonfloat Prologing      Construct Prologing      Source Prologing      Sourc

A short, unique name for this contiguration. May only contain alphanumeric (a-z, A-Z, 0-9), hyphen (-'), underscore (_) and space (') characters.	Beyond Irust Privileged Remote Access
Description Descriptive notes about this configuration and how it may be used.	BeyondTrust Privileged Remote Access
Inabled The configuration can be disabled if it should not be available to end users. Disabling is an alternative to deleting the configuration if it will be enabled at a later time.	
Identifiers	Add
https://pra-1kosmos.beyondtrustdoud.com	Edit
Binding The type of attribute store PortalGuard should query for user claims.	POST
Assertion Consumer URL The BIL: on which the RP listnass for incoming SAML responses. This value must be provided by the RP and can typically be found in its metadata as 'AssertionConsumerService' or 'ACS'.	https://pra-1kosmos.beyondtrustcloud.com/saml/kso
Use ACS from SANLRequest Some service provides use the same entity(D)/dentifier for multiple systems which can lead to probemic disinguiper (SET vs. PROD environments. This sating will and the SANLRequents et ble KansenforConsum/ServiceURL' stributes in the SANLRequest set bit ble Service Provide (Present.	

## BeyondTrust

- 6. Create six new Identity Claims with the following information:
  - Name: NameID
    - Check Send as NamelD
    - Schema Type: urn:oasis:names:tc:SAML:2.0:nameidformat:persistent
    - Value Type: Formatted String
    - Composite Value Format: [EMAIL]
  - Name: Username
    - Schema Type: Username
    - Value Type: Formatted String
    - Composite Value Format: [USERNAME]
  - Name: Email
    - Schema Type: Email
    - Value Type: Formatted String
    - Composite Value Format: [EMAIL]
  - Name: FirstName
    - Schema Type: FirstName
    - Value Type: Formatted String
    - Composite Value Format: [FIRSTNAME]
  - Name: LastName
    - Schema Type: LastName
    - Value Type: Formatted String
    - Composite Value Format: [LASTNAME]
  - Name: Groups
    - Schema Type: Groups
    - Value Type: Formatted String
    - Composite Value Format: Vendor
- Navigate to the IdP-Initiated tab on the left side of the SSO configuration.
  - Set the **Display Text** to *BeyondTrust Privileged Remote Access* or a similar description. This is displayed on the PortalGuard SSO Jump Page as a tile.
  - Set the **Help Text** to *BeyondTrust Privileged Remote Access* or a similar description. This is displayed when a user hovers over the tile on the PortalGuard SSO Jump Page.
  - Set the Display Image to img\default.jpg for the default SSO image. To add an image to your IDaaS instance to display here, please open a ticket within the PortalGuard

٢
L
L
L

Display Text	Reveal Track Data Second Reveals Assess
NOTE: This value must not contain special HTML characters.	beyond trust Privileged Remote Access
Main Taxt	BeyondTrust Privileged Remote Access SSO
The description of the relying party as displayed to the end user on the IdP-initiated jump page.	
NOTE: This value must not contain special HTML characters.	
Distantes	
Choose an optional image to display with the entry on the IdP-initiated jump page.	
Add any custom images to the 'img' folder in the 'C:\InetPub\PortalGuard\sso' directory.	img\default.iog
Only the relative path to the base folder should be entered in this field.	
NOTE: Leave this field blank to not display an image for this relying party.	
Hide on SSO Jump Page	
Check to hide the display tile on PortalGuard's SSO Jump Page.	
The configuration is still available and provides SSO but is simply not displayed on the Jump Page.	
IdP-initiated SSO not directly supported by RP	
Some relying parties do not support IdP-initiated SSO.	
PortaiGuard can still other users SSO from the IdP-Initiated jump page by redirecting the user to the "Dafault LIRL' below	
This will cause a SP-initiated SSO to be started.	
Defeate UPI	
The end user will simply be redirected to this relying party URL from the IdP-initiatd jump page.	
This setting is only used for relying parties that don't directly support IdP-initiated SSO.	

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

BeyondTrust

support portal.

- Select Hide on SSO Jump Page to not show this tile on the PortalGuard SSO Jump Page.
- Make sure IdP-initiated SSO not directly supported by RP is disabled.
- 8. Navigate to the **Authorization** tab on the left side of the SSO Configuration. Specify the users, groups, and OUs that access this application. Leave this empty to allow all users.
- 9. Click **Save** in the upper right of the page to save this configuration.
- 10. A red bar at the top of the screen states that there are changes not yet deployed. Click **Review and Deploy Changes** to apply these to your running PortalGuard instance.
- 11. Click Deploy.



Confirm the changes made below before deploying				
Modified Date	Config Type	Config/Doc Name	Modified By	
12/5/2022, 12:41:31 PM	SAML SSO	BeyondTrust Privileged Remote Access		

6

SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs