BeyondTrust

Privileged Remote Access Beyond Identity SAML Integration Guide

2

Table of Contents

Configure SAML 2.0 for Privileged Remote Access using Beyond Identity	3
Download the Beyond Identity App	4
Configure Beyond Identity	4
Test Beyond Identity on your Device	7

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

3

Configure SAML 2.0 for Privileged Remote Access using Beyond Identity

Using Beyond Identity with SAML for Privileged Remote Access provides several benefits:

- Provides strong, unphishable multi-factor access and policy-based access controls to ensure high-trust authentication for admin accounts.
- Ensures only devices that meet the company's security policy have access to admin accounts.
- Establishes identity before privileged actions on an endpoint are allowed, using a frictionless step-up authentication.
- Creates a zero-trust PAM architecture: the system doesn't trust the user until they pass a high-assurance authentication and doesn't trust their device unless it meets security policies.
- Eliminates passwords and the corresponding vulnerabilities from privileged accounts.

Beyond Identity can validate a device's security posture before allowing access to Privileged Remote Access.

V BEYOND IDENTITY		@
Edit Policy	Edit Rule	Cancel Publish changes
Displaying 2 rules	with the following matching attributes: Any user Add attribute ④	Add rule
	AND if device platform is macOS • • • • • • • • • • • • • • • • • • •	THEN. Allow
DEFAULT	event AND Firewall is - On - On - Add attribute •	THEN: Deny
	AND If integration is JAMF Connection is Available Add attribute	
	AND Any Authenticator version Add attribute 🕣	
	Then Allow -	
	Delete Rule 3	

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

Beyond Identity can provide insights into access activity.



To use the Beyond Identity app, you must download and install the application, and configure it and BeyondTrust Privileged Remote Access to work together. The integration is configured using POST, not redirect.

Download the Beyond Identity App

Go to the Beyond Identity Download site at https://app.byndid.com.

Download and install the Beyond Identity app, and then use the app to authenticate your instance of Beyond Identity.



4

Configure Beyond Identity

Follow the steps below to download and configure the Beyond Identity app:

BeyondTrust

- 1. If Beyond Identity is already open in a browser tab, open a new browser tab for BeyondTrust Privileged Remote Access.
- 2. Go to the admin interface of the Privileged Remote Access instance.
- 3. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
- 4. Click Add and select SAML2.
- 5. Scroll down and expand the Service Provider Settings.
- 6. Locate the Assertion Consumer Service URL and the Entity ID. These are required for Beyond Identity. Alternately, click Download Service Provider Metadata.

- 7. If Beyond Identity is not already open, open it in a new browser tab.
- 8. Click Integrations on the left menu.
- 9. Click the SAML tab.
- 10. Click Add SAML Connection.







- 11. If you have downloaded the service provider metadata, click **Upload XML** and locate the file on your device.
- 12. If you have not downloaded the information, then:
 - Copy the Assertion Consumer Service URL in Privileged Remote Access to SP Single Sign On URL in Beyond Identity.
 - Copy the Entity ID in Privileged Remote Access to SP
 Audience URI in Beyond Identity.



5

13. In Beyond Identity, configure **Attribute Statements**. Groups includes a PRA group to be assigned via the SAML assertion.

14. In Beyond Identity, click Save Changes.

BeyondTrust

- 15. In the **SAML Connections** panel, locate the connection just added.
- 16. For the new connection:
 - Click the Download Certificate icon.
 - Click the Download Metadata icon </>>.

;) C 💼				🕑 🖈 🗯 🖬 🏝 🗄			
Ý	BEYOND	Authentication Context Class		¥				
	ORING Insights	Signed Response ③ UNSIGNED 〇						
۲	Events	X509 Signing Certificate (optional) (1) SAML SP public is	No file selected					
ENAN	IT				. Connection			
•	Users	Attribute Statements						
**	Groups	(optional)						
3	1-1	Name Username Name fo	mat unspecified valu	e {(UserName)} +	Remove			
`	Integratio	Name Email Name fo	mat unspecified 👻 Valu	e ((Email))	Remove			
<u>×</u>	Policy	Name DisplayName Name fo	mat unspecified - Valu	e ((DisplayName)) 👻	Remove			
	Settings	Name Groups Name fo	mat unspecified 👻 Valu	e Vendor 👻	Remove			
		+ Add						
		Delete This Connection		Cancel Sav	e Changes			
	© 2022 Beyond Identity Terms and Conditions							



- 17. Return to the browser tab for the admin interface of the BeyondTrust Privileged Remote Access instance.
- 18. In the Privileged Remote Access admin interface:
 - Click Upload Identity Provider Metadata and locate the file on your device.
 - Click Upload Certificate (or Replace Certificate, if required), and locate the file on your device.

• •	Status My Account Configuration	BeyondTrust Privileged Remote Access	Users	rs & Sec	SECURITY PROVIDERS	VENDORS	9 • •		
		CANCEL SAVE							
		Identity Provider Settings 🔺							
۹.		Metadata							
2	Users & Security	+ UPLOAD IDENTITY PROVIDER METADATA							
8									
		Single Sign-On Service URL •							
٠		SSO URL Protocol Binding							
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	HTTP POST Server certificate • • Current Certificate • Subject:		v			1		

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

BeyondTrust

- 19. Scroll down and expand the User Attribute Settings.
- 20. Configure based on the attribute names configured in Beyond Identity.

- 21. Scroll down and expand Authorization Settings.
- 22. Configure as required. A Default Group Policy must be selected.
- 23. Click Save.
- 24. Log out of BeyondTrust Privileged Remote Access.

0	Status	BeyondTrust Users & Security 9
-	My Account	Privileged
	Configuration	
	Jump™	CANCEL SAVE
	Vault	Service Provider Settings 🗸
۰.	Access Console	User Attribute Settings 🔺
*	Users & Security	Enter the SAML attribute name for each user attribute. Username •
Ð	Reports	Username
ൽ	Management	E-mail •
Ĩ		Email
-	Appliance	Use case-insensitive comparison for NameIDs
		▲ Do not enable this feature unless your IdP requires case-insensitivity for the NameID attribute.
	«	Display Name • DisplayName Immittiple SAML attributes are used to populate a single user attribute, then surround each SAML attribute name we braces: stam/AttributeName).
0	Status	BeyondTrust Users & Security 9
-	My Account	
	Configuration	
	Jump™	CANCEL SAVE
	Vault	Service Provider Settings 🗸
	Access Console	User Attribute Settings 🗸
		Authorization Settings 🔺
~~	Users & Security	Group Lookup Attribute Name 0 Delimiter 0
₿	Reports	Groups If left blank. SAML users must be manually assigned to
	Management	group policies after their first successful authentication.
	Appliance	Vendor
		Default Group Policy • 🕕
	*	

Test Beyond Identity on your Device

To test Single Sign-On using SAML with the Beyond Identity app, ensure you are logged out of all instances of BeyondTrust Privileged Remote Access.

On the login page for Privileged Remote Access, click **Use SAML Authentication**.

← → C [*] (a) eval-fa74c61f.beyond	trustcloud.com/login/login	i£ ☆	* 0 4
	Beyond Trust Privileged Remote Access Privileged Remote Access Powerd by Benger		
	PLEASE LOG IN		
	Password		
	LOG IN Use SAMLAuthentication		
	🕀 _{English (US)}		

7

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

1

A screen shows the Beyond Identity app verifying identity.



After successful verification, you are authenticated in Privileged Remote Access.

Status	BeyondTrust Privileged	Status	9
	Remote Access	INFORMATION USERS WHAT'S N	VEW
Imp™		Your software license will	
🔒 Vault		expire in days.	
Access Console		Please contact BeyondTrust for more	
Users & Security		information. BeyondTrust	
Reports		Privileged Remote Access	
😥 Management	SITE STATUS		
Appliance			
	Primary Hostname	API Version	US/Eastern V
	Company/Division Name	ECM Protocol Version	Welcome!
«	Company API Name	Appliance GUID	Let's get you setup!

For more information, please see SAML for Single Sign-On Authentication at https://www.beyondtrust.com/docs/privileged- remote-access/how-to/integrations/security-providers/saml/index.htm.

Should you need any assistance, please log into the Customer Portal at <u>https://beyondtrustcorp.service-now.com/csm</u> to chat with Support.