#### Privileged Remote Access Azure SAML Integration Guide

#### **Table of Contents**

Configure SAML 2.0 for Privileged Remote Access using the BeyondTrust SAML Azure	
АД Арр	3
Install and Configure the Azure AD App	4
Configure Privileged Remote Access to use the SAML Azure AD App	8

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

## Configure SAML 2.0 for Privileged Remote Access using the BeyondTrust SAML Azure AD App

Azure Active Directory (Azure AD), part of Microsoft Entra, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against a wide range of cybersecurity attacks.

A BeyondTrust app, available in Azure AD App Gallery, provides Single Sign-On and provisioning via SAML. This app supports Remote Support and public portals, Privileged Remote Access, Password Safe, and Password Safe Cloud.

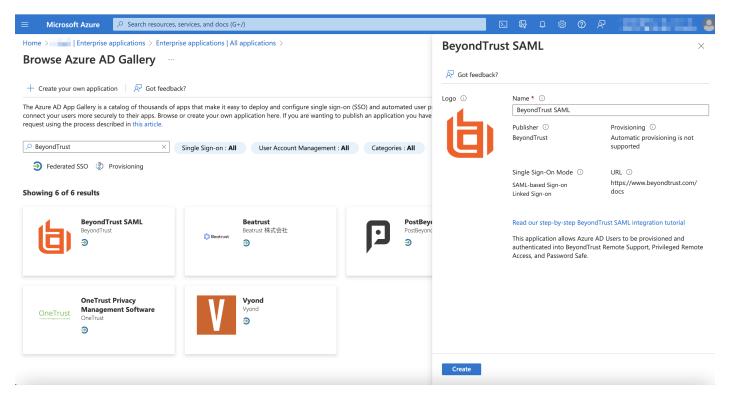
SALES: www.beyondtrust.com/contact SUPPORT: www.beyondtrust.com/support DOCUMENTATION: www.beyondtrust.com/docs

©2003-2024 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.

#### Install and Configure the Azure AD App

Follow the steps below to install and configure this app.

1. Locate the BeyondTrust SAML app in Microsoft Azure AD Gallery.

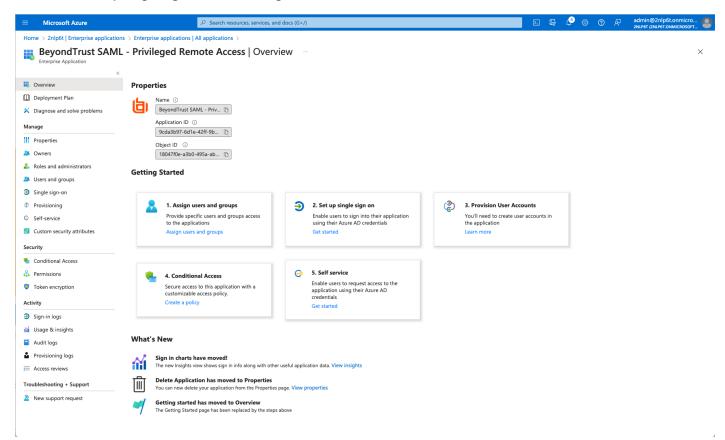


2. Change the name to your preferred descriptive name, for example, BeyondTrust SAML – Privileged Remote Access.

**Note:** While a single instance of the app can service multiple BeyondTrust products simultaneously, we recommend creating a separate app instance for Password Safe, if you are using that product.

3. Click Create.

- 4. Information about the BeyondTrust SAML app displays when creation is completed.
- 5. Click Set up single sign on under Getting Started.



6. Configure Basic SAML Configuration to match your Privileged Remote Access instance. The Entity IDs are specific to the instances for each product.

	≫ Search resources, services, and docs (G+/)	国家 🖓 🔅 ⑦ 尺 admin@2nlp6t.onmicro 💄
Home > 2nlp6t   Enterprise applicatio	ns > Enterprise applications   All applications > BeyondTrust SAML - Privileged Remote Access	Basic SAML Configuration ×
BeyondTrust SAML - F	Privileged Remote Access   SAML-based Sign-on	
Enterprise Application		Save Save Got feedback?
«	$\overline{\uparrow}$ Upload metadata file $~>$ Change single sign-on mode $~\equiv~$ Test this application $~ ~~ \nearrow$ G	
iii Overview		Identifier (Entity ID) * ③ The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in
Deployment Plan	Set up Single Sign-On with SAML	your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.
X Diagnose and solve problems	An SSO implementation based on federation protocols improves security, reliability, and end user exp	
Manage	implement. Choose SAML single sign-on whenever possible for existing applications that do not use more.	https://pra1.acme.com
Properties	Read the configuration guide 😅 for help integrating BeyondTrust SAML - Privileged Remote Access.	Add identifier
A Owners		Patterns: https://remote1.acme.com, https://pra1.acme.com, https://is1.acme.com/public_portal, https://ps1.acme.com/eEye.RetinaCSSAML
Roles and administrators	Basic SAML Configuration	ntps://ps.acme.com/ecye.retmac.soAwic
Users and groups	Identifier (Entity ID) https://pra1.acme.com	Reply URL (Assertion Consumer Service URL) * ①
Single sign-on	Reply URL (Assertion Consumer Service URL) https://pra1.acme.com/saml/sso Sign on URL https://pra1.acme.com/saml	The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion
Provisioning	Relay State (Optional) Optional Logout Url (Optional) Optional	Consumer Service" (ACS) in SAML
Self-service	aggest en (apriorie) apriories	Index Default
Custom security attributes	2 Attributes & Claims	https://pra1.acme.com/saml/sso
Converting 1	Attributes & claims	Add reply URL
Security	Username user.userprincipalname Email user.mail	Patterns: https://remote1.acme.com/saml/sso, https://pra1.acme.com/saml/sso, https://rs1.acme.com/process, https://ps1.acme.com/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
Conditional Access	LastName user.surname	
Permissions	FirstName user.givenname Unique User Identifier user.userprincipalname	Sign on URL (Optional)
Token encryption	Group user.groups	Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for
Activity		your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.
Sign-in logs	3 SAML Certificates	https://pra1.acme.com/saml
🖬 Usage & insights	Token signing certificate	
Audit logs	Status         Active           Thumbprint         2E0327F4A9A7B82E358328E0A073EAD097	Relay State (Optional) ①
Provisioning logs	Expiration 8/23/2026, 7:30:44 AM	<sup>3</sup> The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.
≆ Access reviews	Notification Email admin@2nlp6t.onmicrosoft.com App Federation Metadata Url https://login.microsoftonline.com/b23838	
Troubleshooting + Support	Certificate (Base64) Download	
New support request	Certificate (Raw) Download Federation Metadata XML Download	Logout Url (Optional)
<ul> <li>wew support request</li> </ul>		Logout On (Optional) This URL is used to send the SAML logout response back to the application.
	Verification certificates (optional)	Enter a logout uri
	Required No Active 0	······································

7. Change the Unique Identifier (Name ID) to the Persistent format.

■ Microsoft Azure	$\mathcal P$ Search resources, services, and docs (G+/)	Σ.	R	¢ @	(?)	R	admin@2nlp6t.onmicro
Home > 2nlp6t   Enterprise applicatio	ns > Enterprise applications   All applications > BeyondTrust SAML - Privileged Remote Access   SAML-based Sign-on > SAML-based Sign-on > Attributes & Clai						2NLP6T (2NLP6T.ONMICROSOFT
Manage claim							×
🔲 Save 🗙 Discard changes 🛛 🖗	♀ Got feedback?						
Name	nameidentifier						
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims						
∧ Choose name identifier format							
Name identifier format *	Persistent					$\sim$	
Source *	Attribute      Transformation      Directory schema extension (Preview)						
Source attribute *	user.userprincipalname					$\sim$	•
Claim conditions							

8. Configure **Attributes & Claims** sources and values as shown in the table below, then add a group claim as show in the image below:

Source	Value
Username	user.principalname
FirstName	user.givenname
LastName	user.surname
Email	user.email
Group Claim	Group ID

	${\cal P}$ Search resources, services, and docs (G+/)	D III 🖉 🇐 🧑 Л admin@2nlp6t.onmicro 🧕
Home > 2nlp6t   Enterprise applications > Enterprise application Attributes & Claims	ns   All applications > BeyondTrust SAML - Privileged Remote Access   SAML-based Sign-on > SAML-based Sign-or	$\underset{\mbox{Manage the group claims used by Azure AD to populate SAML tokens issued to your app}}{\mbox{Group claims used by Azure AD to populate SAML tokens issued to your app}} \label{eq:group}$
+ Add new claim + Add a group claim ≣≣ Columns   \$	Got feedback?	Which groups associated with the user should be returned in the claim?           None         All groups
Required claim		Security groups
Claim name	Type Value	O Directory roles
Unique User Identifier (Name ID)	SAML user.userprincipalname [ ***	<ul> <li>Groups assigned to the application</li> </ul>
Additional claims		Source attribute *
Claim name	Type Value	Group ID V
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML user.groups [Application ***	Emit group name for cloud-only groups ①
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Email	SAML user.mail ***	∧ Advanced options
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/FirstName	SAML user.givenname ***	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/LastName	SAML user.surname ***	Filter groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Username	SAML user.userprincipalname ***	Attribute to match
<ul> <li>Advanced settings</li> </ul>		Match with  String  Customize the name of the group claim  Name (required)  Groups  Namespace (optional)  Emit groups as role claims ③ Apply regex replace to groups claim content Expose claim in JWT tokens in addition to SAML tokens
		Save
		L. L

Note: The group claim must be configured to use only groups assigned to the application, to prevent errors that may occur if a user belongs to more than 150 AD groups. For more information, please see <u>Configure group claims for applications by using</u> Azure Active Directory at https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-fed-groupclaims.

- 9. Click Edit on the SAML certificates section.
- 10. For Signing Option, select Sign SAML response and assertion.
- 11. Download the Federation Metadata XML.

# Configure Privileged Remote Access to use the SAML Azure AD App

Once the app has been configured, follow these steps to add the provider to Privileged Remote Access:

- 1. Log in to Privileged Remote Access.
- 2. Navigate to Users & Security > Security Providers.
- 3. Click +ADD.
- 4. Select SAML2.
- 5. Upload the Identity Provider metadata downloaded from the Azure AD App.

Status	BeyondTrust Users & Security
L My Account	Privileged Security
	Remote Access USERS ACCESS INVITE SECURITY PROVIDERS VENDORS SESSION POLICIES GROUP POLICIES KERBEROS KEYTAB
🛃 Jump	CANCEL SAVE
🗗 Vault	
🖳 Access Console	EDIT SECURITY PROVIDER
📇 Users & Security	Required field
Reports	Name •
-	SAML2
😥 Management	C Enabled
Appliance	User Provision  Servision users using this provider  Provision users using a different provider  User provision can only be set while creating the provider.
	Identity Provider Settings A
	Metadata 🕄 Entity ID • Server certificate • 🕃
	+ UPLOAD IDENTITY PROVIDER METADATA https://sts.windows.net/b23838ca-394b-4027-9f8a-6e0ct • Subject: CN=Microsoft Azure Federated SSO Certificate • Issuer: CN=Microsoft Azure Federated SSO Certificate
:	Ssour: CN=Microsoft Azure Federated SSO Certificate     Single Sign-On Service URL     SSO URL Protocol Binding     SSO URL Protocol Binding     Valid To: 2025-11-29 15:22:30 UTC
	https://login.microsoftonline.com/b23838ca-394b-4027-! HTTP POST
	Service Provider Settings  V User Attribute Settings  Authorization Settings  V
«	

©2003-2024 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.

6. Verify that User Attribute Settings match the Claims in Azure AD App

🥪 Status	BeyondTrust Users & Secu	urity.	Q	📮 Admin 🔻
💄 My Account	Privileged	inty	<b>x</b>	
	Remote Access USERS ACCESS INVITE	SECURITY PROVIDERS VENDORS SESSION POLICIES	GROUP POLICIES KERBEROS KEYTAB	
手 Jump	CANCEL SAVE			
🕂 Vault	User Provision			
🖳 Access Console	<ul> <li>Provision users using this provider</li> <li>Provision users using a different provider</li> </ul>			
🐣 Users & Security	⚠️ User provision can only be set while creating the pro	vider.		
🛱 Reports	Collapse All			
<b>ලි</b> Management	Identity Provider Settings			
Appliance	Metadata 🚯	Entity ID •	Server certificate • ()	
	+ UPLOAD IDENTITY PROVIDER METADATA	https://sts.windows.net/b23838ca-394b-4027-9f8a-6e0ct	Current Certificate <ul> <li>Subject: CN=Microsoft Azure Federated SSO Certificate</li> </ul>	
	Single Sign-On Service URL •	SSO URL Protocol Binding	<ul> <li>Issuer: CN=Microsoft Azure Federated SSO Certificate</li> <li>Valid From: 2022-11-29 15:22:30 UTC</li> <li>Valid To: 2025-11-29 15:22:30 UTC</li> </ul>	
	https://login.microsoftonline.com/b23838ca-394b-4027-	HTTP POST V	+ REPLACE CERTIFICATE	
	Service Provider Settings 🗸			
	User Attribute Settings 🔨			
	Enter the SAML attribute name for each user attribute.		_	
	Username •	E-mail •	Use case-insensitive comparison for NamelDs	
	Osemaine		Do not enable this feature unless your IdP requires case-insensitivity for the NameID attribute.	
	Display Name •			
	{FirstName} {LastName}			
	If multiple SAML attributes are used to populate a single use	r attribute, then surround each SAML attribute name with brace	es: {samlAttributeName}.	
	Authorization Settings 🐱			
*				

7. Configure Authorization Settings to match Azure AD Groups and assign a default Group Policy.

🥪 Status	BeyondTrust Users & Security	Q Admin -
L My Account	Privileged	
Configuration	Remote Access USERS ACCESS INVITE SECURITY PROVIDERS VENDORS SESSION POLICIES GROUP POLICIE	ES KERBEROS KEYTAB
手 Jump	CANCEL SAVE	
🕂 Vault	Name • SAML2	
🖳 Access Console	✓ Enabled	
Users & Security	User Provision      Provision users using this provider      Provision users using a different provider	
🔞 Management	User provision can only be set while creating the provider.	
Appliance	Collapse All	
	Identity Provider Settings 🔺	
	Metadata  Entity ID  E	ertificate
	Single sign-On Service URL • SSU URL Protocol Binding • Value	fer: CN=Microsoft Azure Federated SSO Certificate d From: 2022-11-29 15:22:30 UTC d To: 2025-11-29 15:22:30 UTC
	https://login.microsoftonline.com/b23838ca-394b-4027-4	ACE CERTIFICATE
	Service Provider Settings 🗸	
	User Attribute Settings 🗸	
	Authorization Settings 🔺	
		It Group Policy • 1 dors V 🖸
«	«	

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

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