BeyondTrust

Remote Support
Azure SAML Integration Guide

TC:3/4/2024

Table of Contents

Configure SAML 2.0 for Remote Support using the BeyondTrust SAML Azure AD App

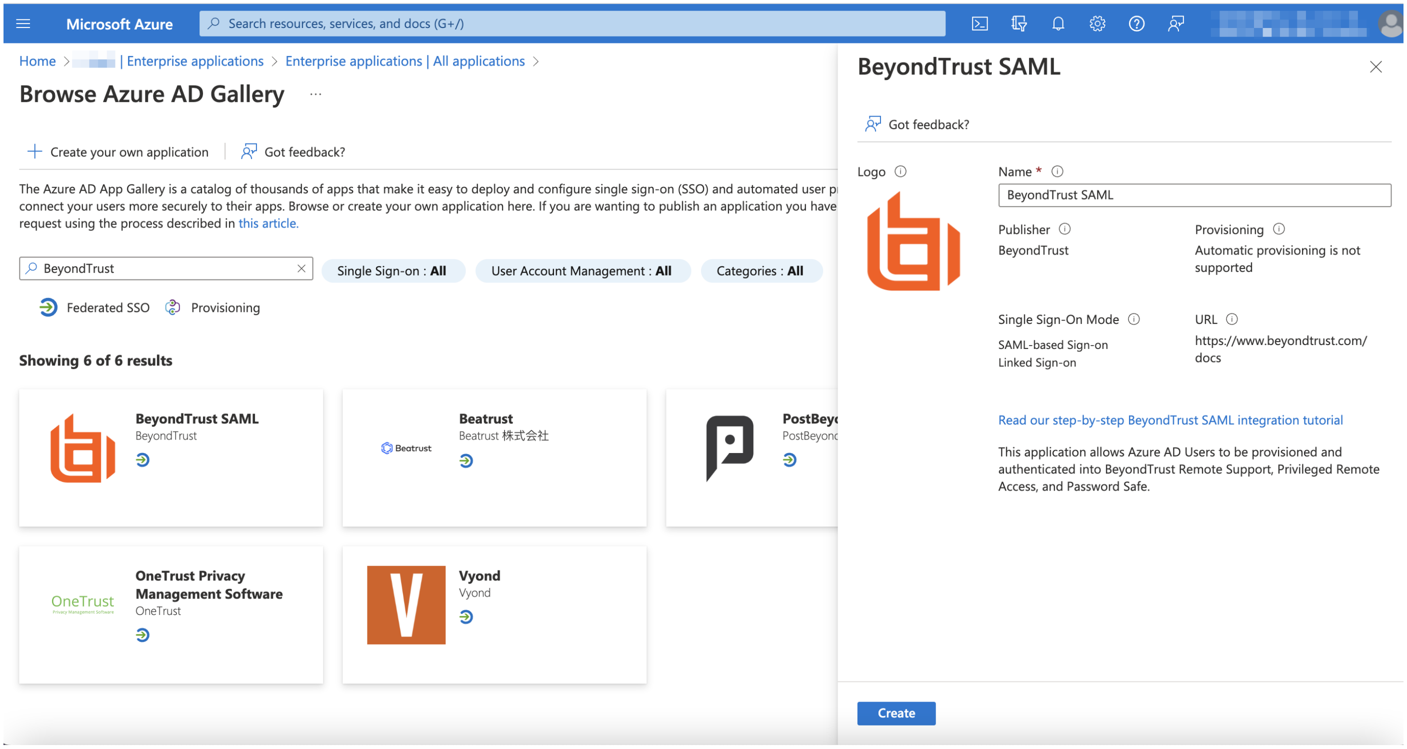
Azure Active Directory (Azure AD), part of Microsoft Entra, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against a wide range of cybersecurity attacks.

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.

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.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > | Enterprise applications > Enterprise applications | All applications >
Create your own application
Got feedback?
Single Sign-on : All
User Account Management : All
Categories : All
Federated SSO
Provisioning
Create

Browse Azure AD Gallery

The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user pr connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have request using the process described in this article.

BeyondTrust

Showing 6 of 6 results

BeyondTrust SAML
BeyondTrust

Beatrust
Beatrust 株式会社

PostBeyo
PostBeyond

OneTrust Privacy Management Software
OneTrust

Vyond
Vyond

BeyondTrust SAML

Got feedback?

Logo

Name *
BeyondTrust SAML

Publisher
BeyondTrust

Provisioning
Automatic provisioning is not supported

Single Sign-On Mode
SAML-based Sign-on
Linked Sign-on

URL
https://www.beyondtrust.com/docs

Read our step-by-step BeyondTrust SAML integration tutorial

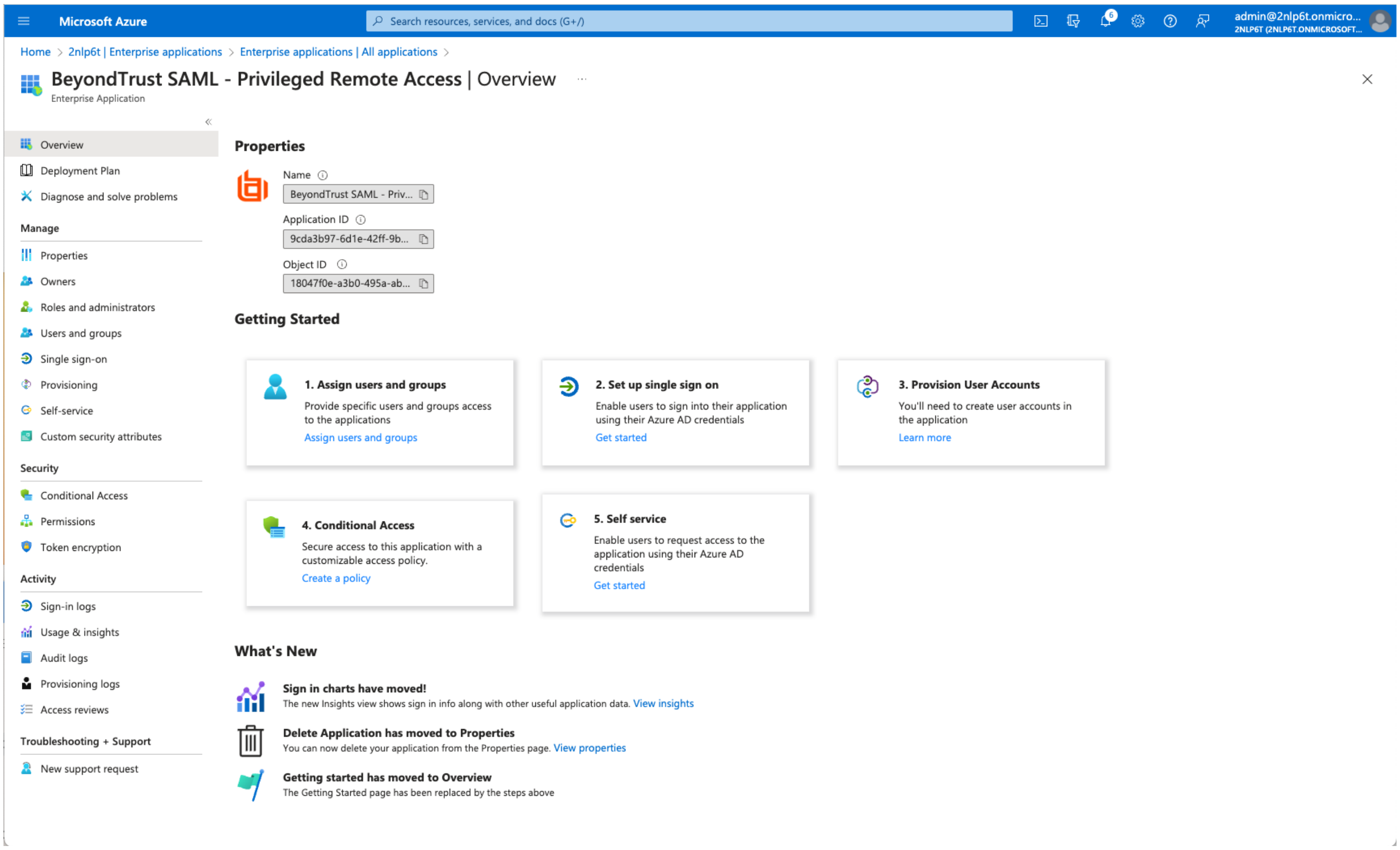
This application allows Azure AD Users to be provisioned and authenticated into BeyondTrust Remote Support, Privileged Remote Access, and Password Safe.

2. Change the name to your preferred descriptive name, for example, BeyondTrust SAML – Remote Support. Screenshots below use BeyondTrust Privileged Remote Access as the descriptive name, however the process is the same for either application.

> ***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**.



BeyondTrust SAML - Privileged Remote Access | Overview

Enterprise Application

Properties

Name: BeyondTrust SAML - Priv...

Application ID: 9cda3b97-6d1e-42ff-9b...

Object ID: 18047f0e-a3b0-495a-ab...

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

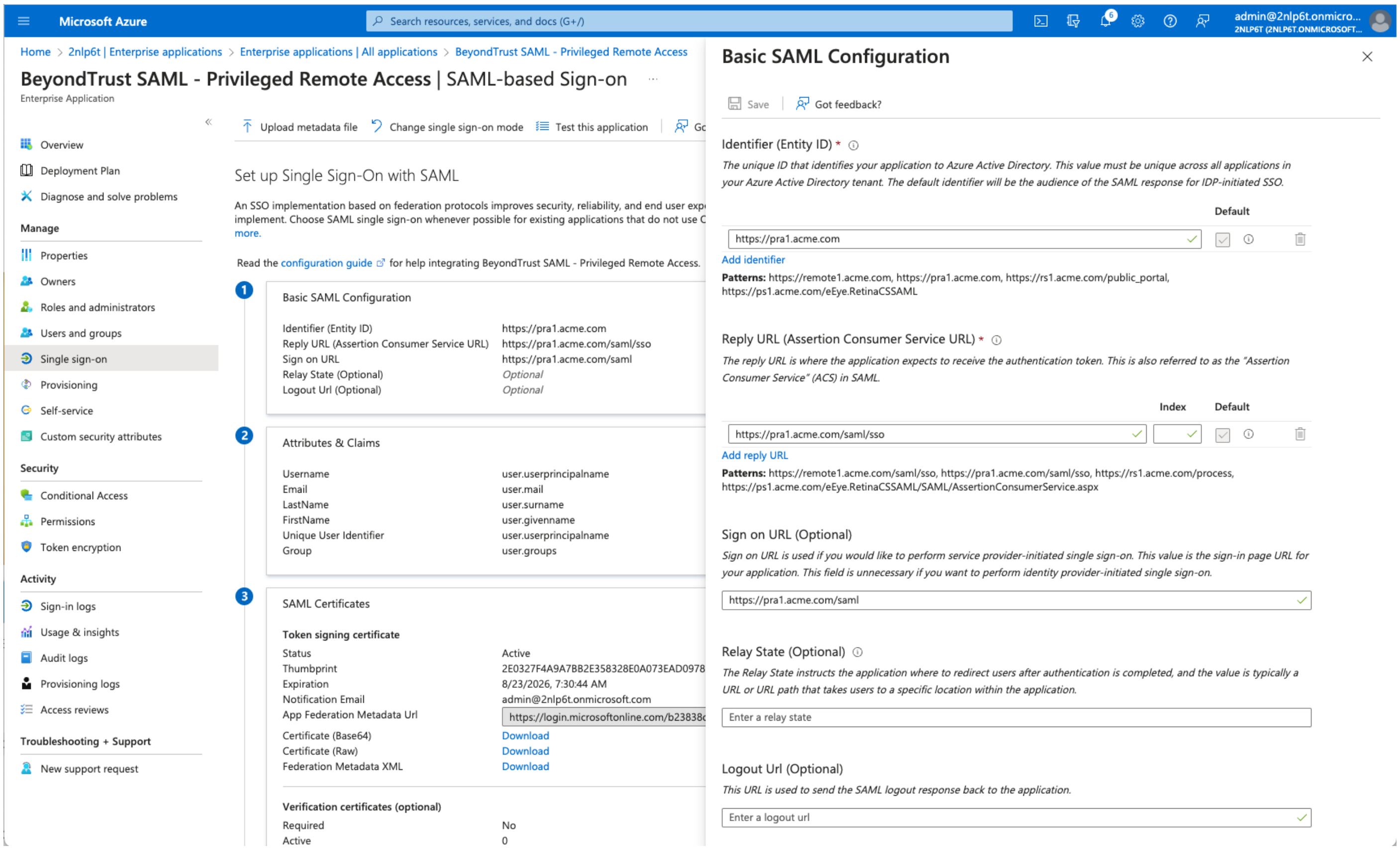
What's New

Sign in charts have moved!
The new Insights view shows sign in info along with other useful application data. View insights

Delete Application has moved to Properties
You can now delete your application from the Properties page. View properties

Getting started has moved to Overview
The Getting Started page has been replaced by the steps above

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



BeyondTrust SAML - Privileged Remote Access | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user exp implement. Choose SAML single sign-on whenever possible for existing applications that do not use C more.

Read the configuration guide for help integrating BeyondTrust SAML - Privileged Remote Access.

1 Basic SAML Configuration

Identifier (Entity ID)	https://pra1.acme.com
Reply URL (Assertion Consumer Service URL)	https://pra1.acme.com/saml/sso
Sign on URL	https://pra1.acme.com/saml
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

Username	user.userprincipalname
Email	user.mail
LastName	user.surname
FirstName	user.givenname
Unique User Identifier	user.userprincipalname
Group	user.groups

3 SAML Certificates

Token signing certificate

Status	Active
Thumbprint	2E0327F4A9A7BB2E358328E0A073EAD0978
Expiration	8/23/2026, 7:30:44 AM
Notification Email	admin@2nlp6t.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/b23838
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0

Basic SAML Configuration

Save | Got feedback?

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://pra1.acme.com	☑

Add identifier

Patterns: https://remote1.acme.com, https://pra1.acme.com, https://rs1.acme.com/public_portal, https://ps1.acme.com/eEye.RetinaCSSAML

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://pra1.acme.com/saml/sso		☑

Add reply URL

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

Sign on URL (Optional)

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 your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

https://pra1.acme.com/saml

Relay State (Optional)

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.

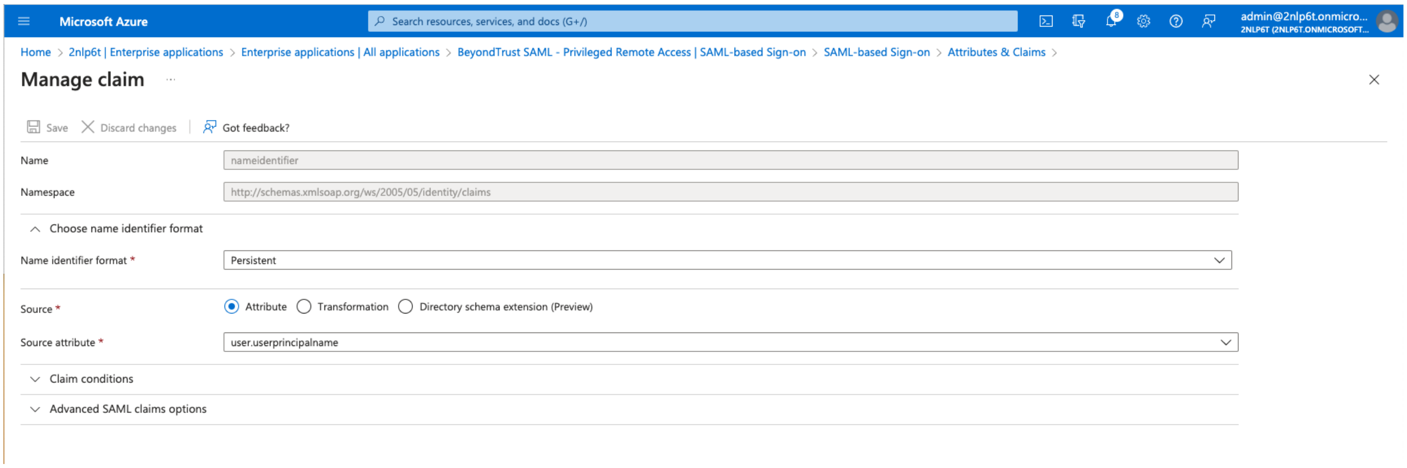
Enter a relay state

Logout Url (Optional)

This URL is used to send the SAML logout response back to the application.

Enter a logout url

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


Microsoft Azure
Search resources, services, and docs (G+/)
admin@2nlp6t.onmicro...
2NLP6T (2NLP6T.ONMICROSOFT...
Home > 2nlp6t | Enterprise applications > Enterprise applications | All applications > BeyondTrust SAML - Privileged Remote Access | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >
Save
Discard changes
Got feedback?

Manage claim

Name	nameidentifier
Namespace	http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

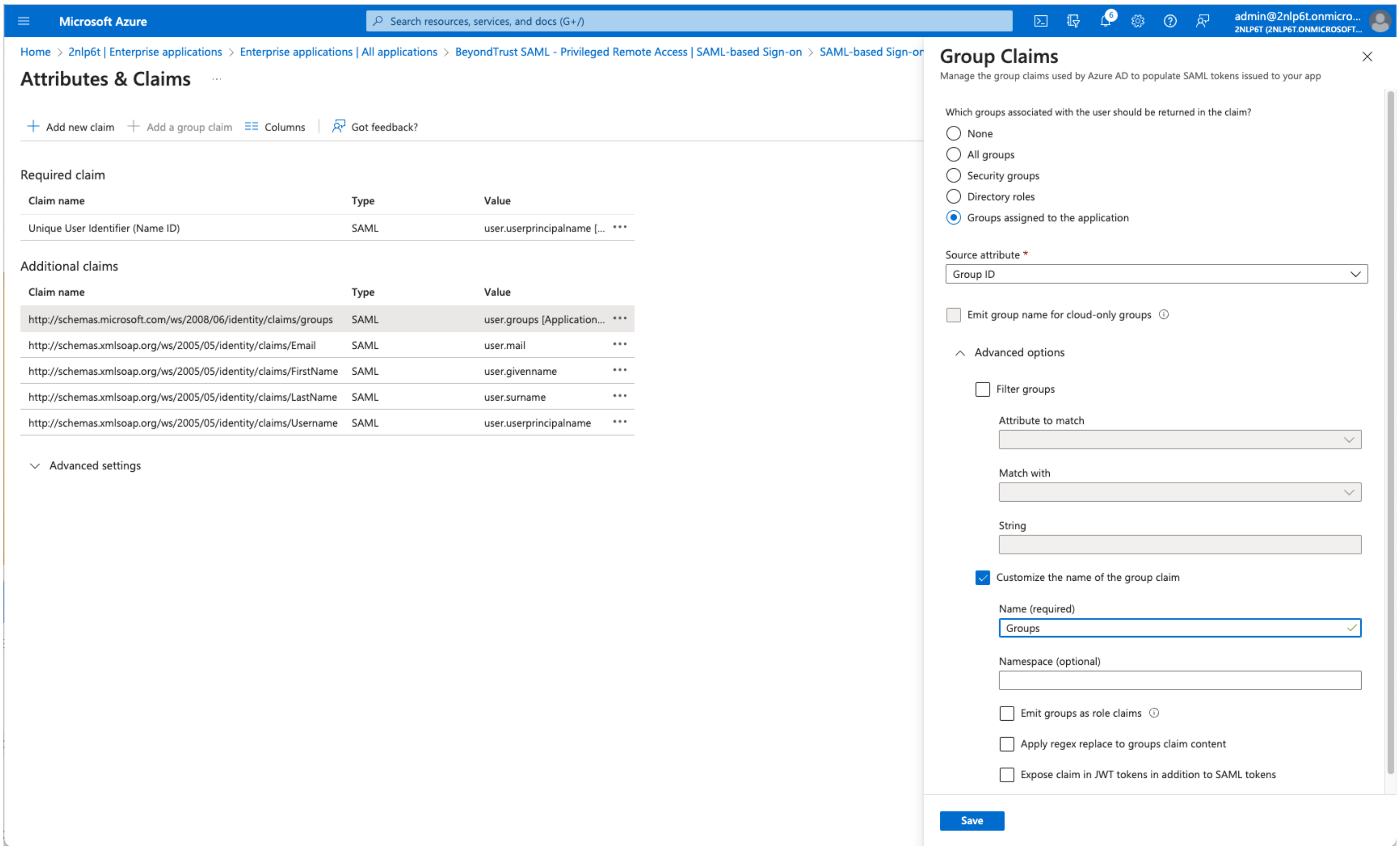
Name identifier format *	Persistent
Source *	● Attribute ○ Transformation ○ Directory schema extension (Preview)
Source attribute *	user.userprincipalname

Claim conditions

Advanced SAML claims options

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


Microsoft Azure
Search resources, services, and docs (G+/)
6
admin@2nlp6t.onmicro...
2NLP6T (2NLP6T.ONMICROSOFT...
Home > 2nlp6t | Enterprise applications > Enterprise applications | All applications > BeyondTrust SAML - Privileged Remote Access | SAML-based Sign-on > SAML-based Sign-on
+ Add new claim
+ Add a group claim
Columns
Got feedback?
Advanced settings
Save

Attributes & Claims

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [Application...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Email	SAML	user.mail
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
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/Username	SAML	user.userprincipalname

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

○ None
○ All groups
○ Security groups
○ Directory roles
● Groups assigned to the application

Source attribute *: Group ID

□ Emit group name for cloud-only groups

Advanced options

□ Filter groups

Attribute to match:

Match with:

String:

☑ Customize the name of the group claim

Name (required): Groups

Namespace (optional):

□ Emit groups as role claims

□ Apply regex replace to groups claim content

□ Expose claim in JWT tokens in addition to SAML tokens

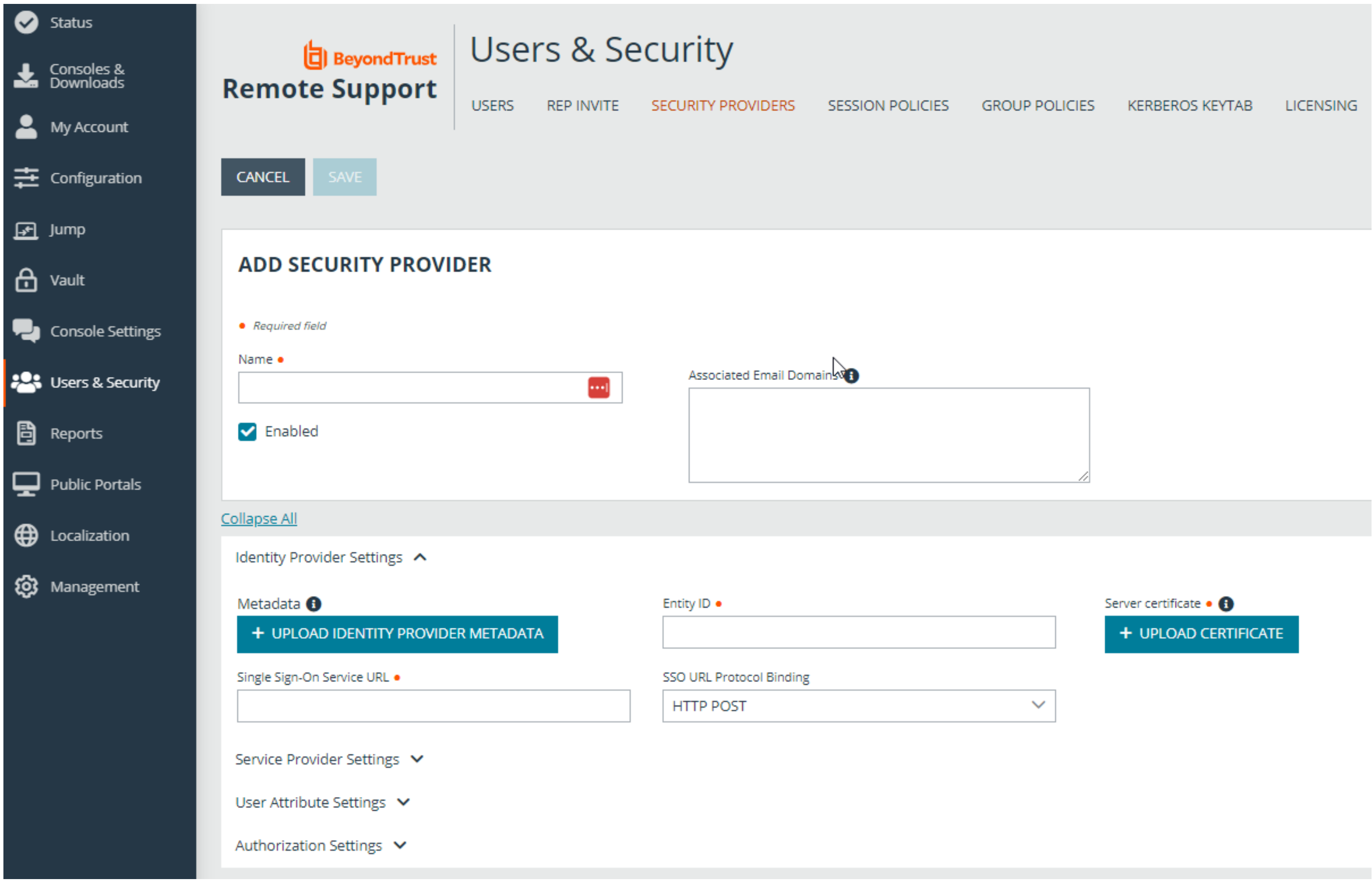
> ***Note:*** *The group claim must be configured to use only groups assigned to the application, to prevent errors that may occur if a user belongs to more than 150 AD groups. For more information, please see Configure group claims for applications by using Azure Active Directory at https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-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

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

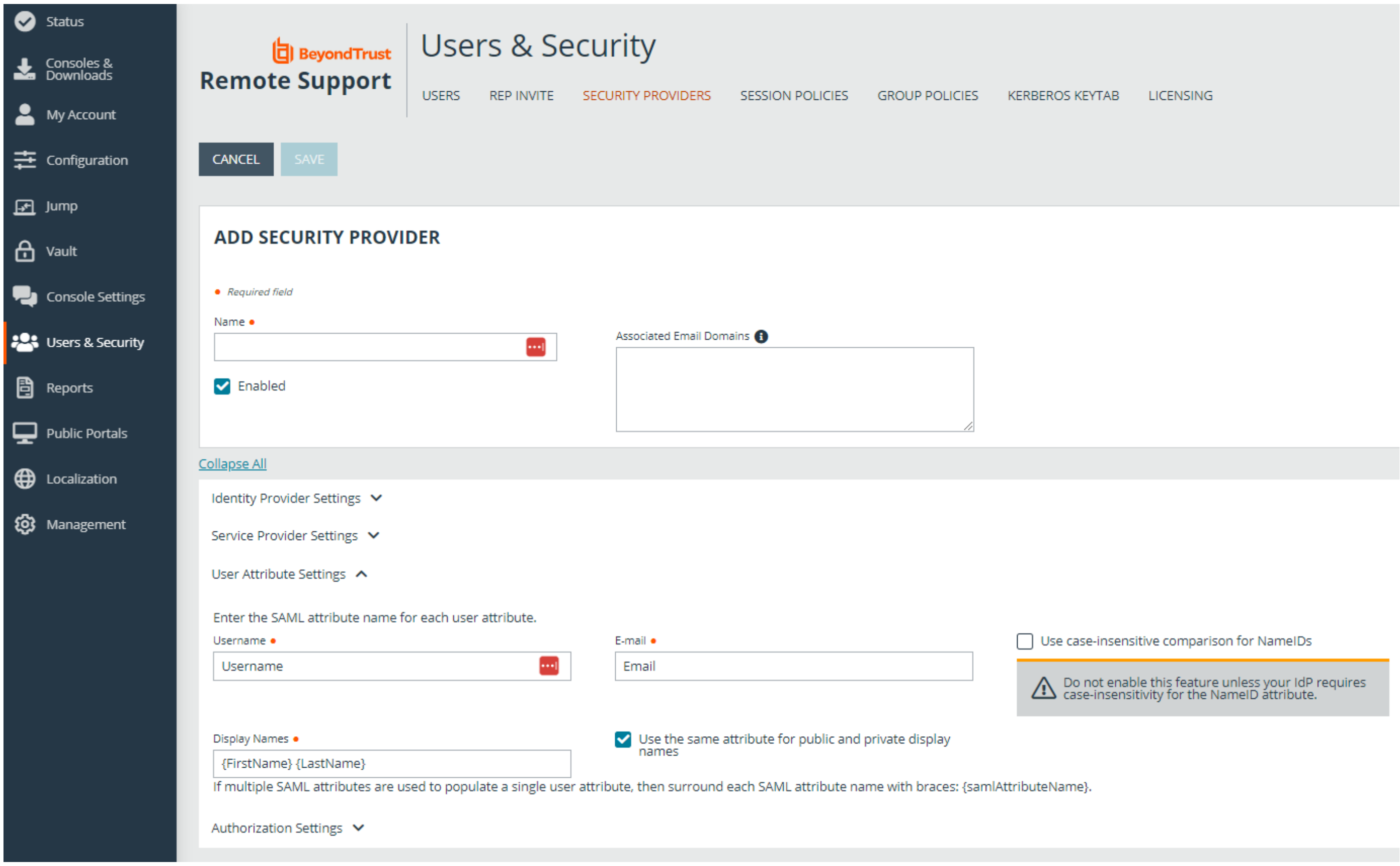
Configure Remote Support to use the SAML Azure AD App

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

1. Log in to Remote Support.
2. Navigate to **Users & Security > Security Providers**.
3. Click **+ADD**.
4. Select **SAML For Representatives** or **SAML for Public Portals**. Steps below are shown for **SAML For representatives**. The process is similar for public portals.
5. Upload the Identity Provider metadata downloaded from the Azure AD App.



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



ADD SECURITY PROVIDER

• *Required field*

Name •

Associated Email Domains

☑ Enabled

Enter the SAML attribute name for each user attribute.

Username •: Username

E-mail •: Email

☐ Use case-insensitive comparison for NameIDs

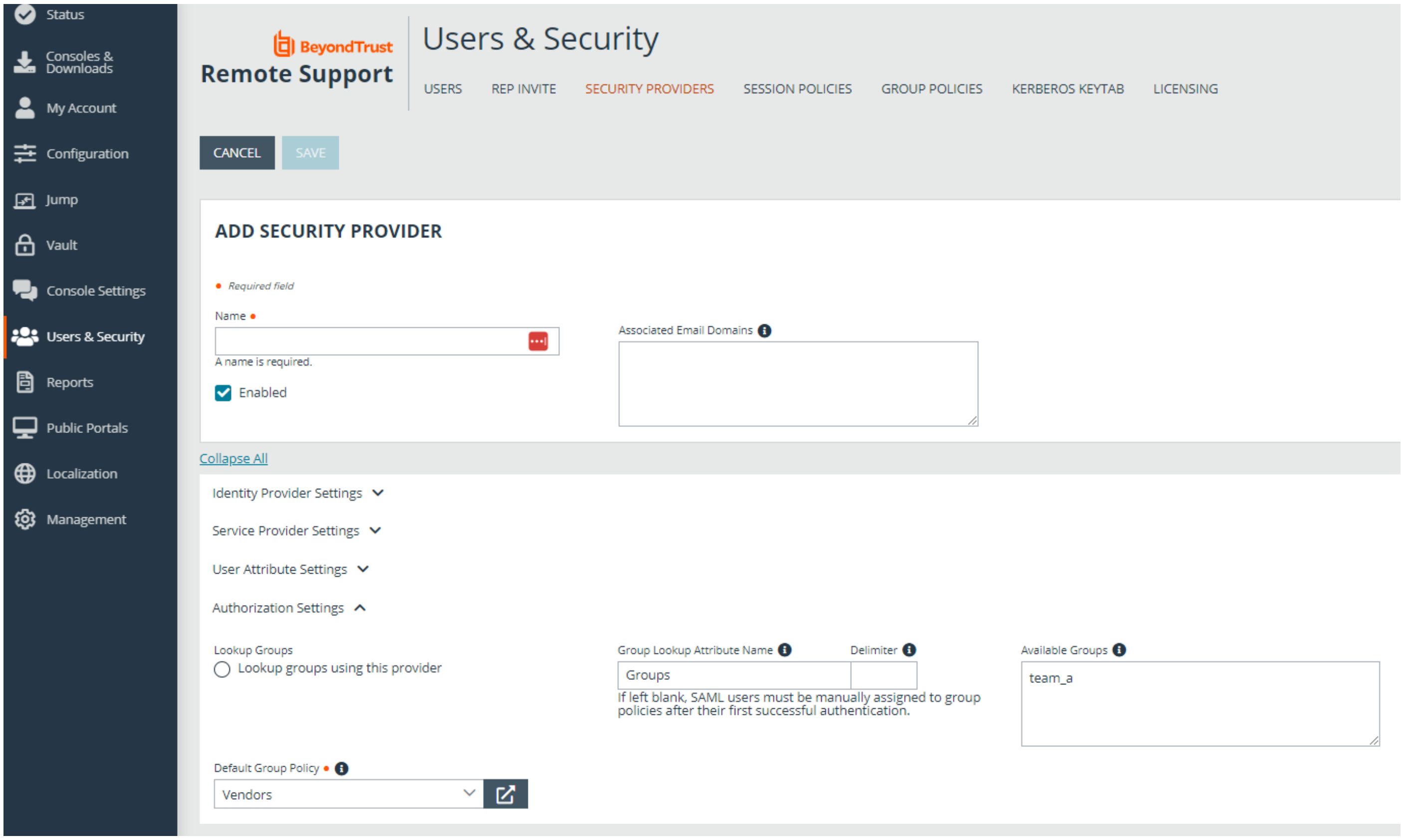
Do not enable this feature unless your IdP requires case-insensitivity for the NameID attribute.

Display Names •: {FirstName} {LastName}

☑ Use the same attribute for public and private display names

If multiple SAML attributes are used to populate a single user attribute, then surround each SAML attribute name with braces: {samlAttributeName}.

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



ADD SECURITY PROVIDER

• Required field

Name •

A name is required.

☑ Enabled

Associated Email Domains

Identity Provider Settings

Service Provider Settings

User Attribute Settings

Authorization Settings

Lookup Groups

○ Lookup groups using this provider

Group Lookup Attribute Name: Groups

Delimiter

If left blank, SAML users must be manually assigned to group policies after their first successful authentication.

Available Groups: team_a

Default Group Policy •: Vendors

For more information, please see SAML for Single Sign-On Authentication at https://www.beyondtrust.com/docs/remote-support/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.