



BeyondTrust

Privileged Remote Access Azure SAML Integration Guide

Table of Contents

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

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

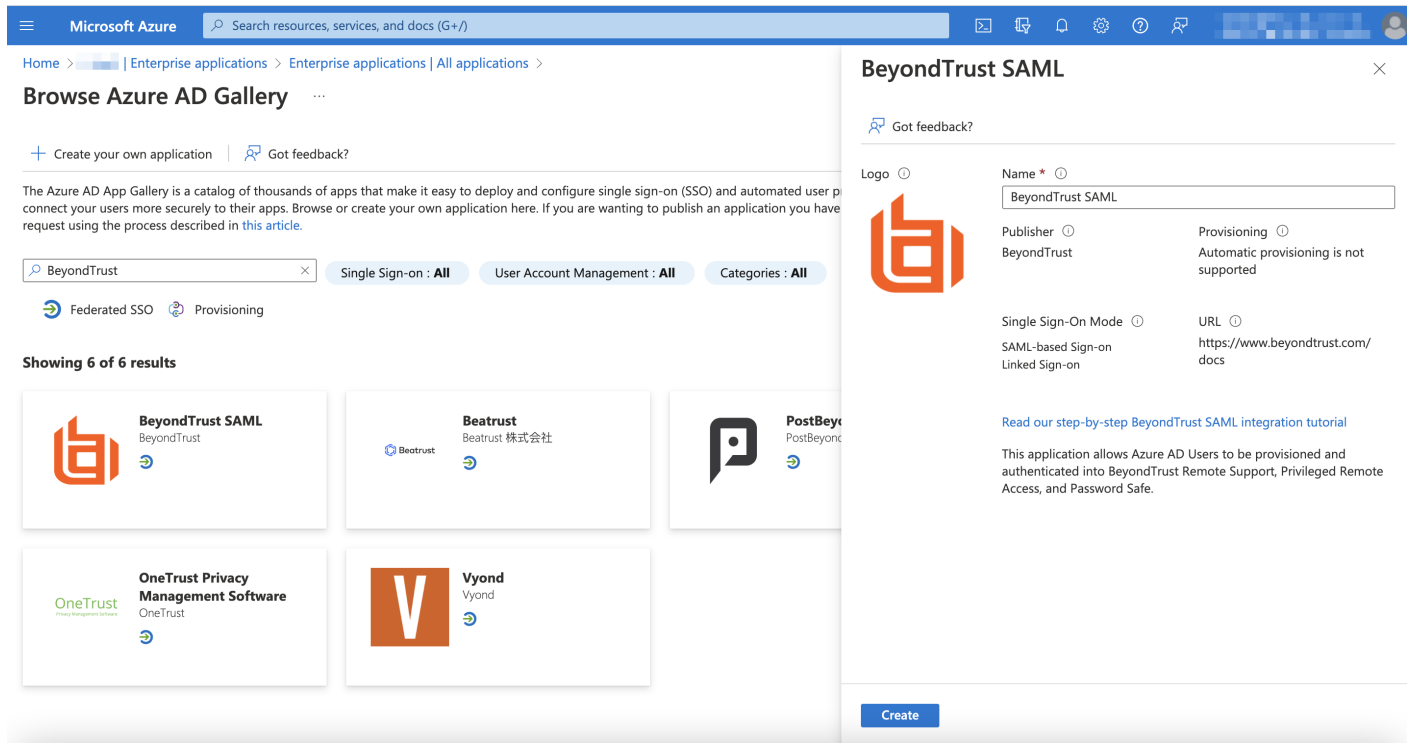
Azure Active Directory (Azure AD), part of Microsoft Entra, is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against a wide range of cybersecurity attacks.

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.

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.



The screenshot shows the Microsoft Azure portal interface. On the left, the 'Browse Azure AD Gallery' page is displayed with a search for 'BeyondTrust'. The search results show several apps, including 'BeyondTrust SAML'. On the right, the details for the 'BeyondTrust SAML' app are shown. The app name is 'BeyondTrust SAML', the publisher is 'BeyondTrust', and the provisioning status is 'Automatic provisioning is not supported'. The URL is 'https://www.beyondtrust.com/docs'. A 'Create' button is visible at the bottom right of the app details panel.

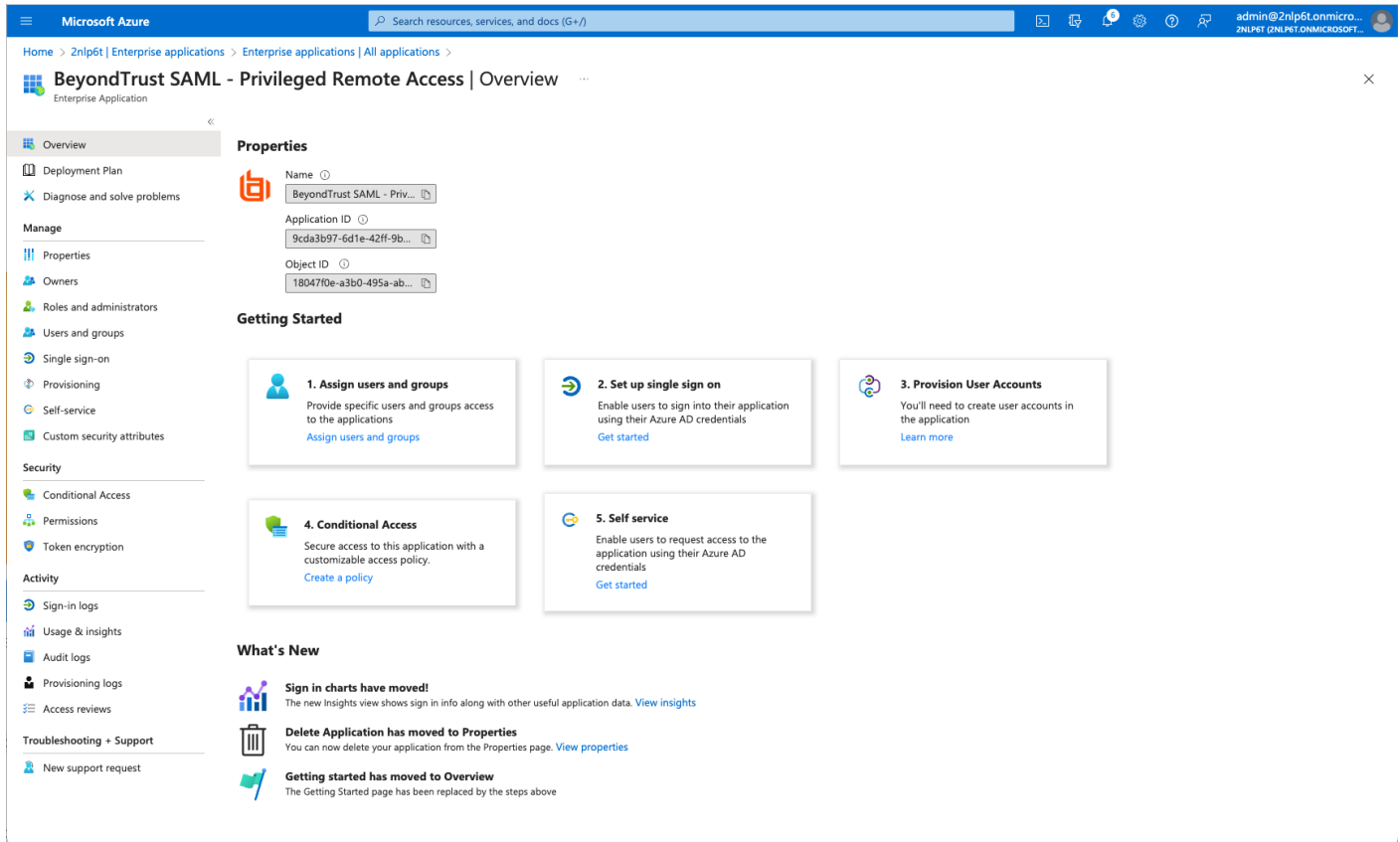
2. Change the name to your preferred descriptive name, for example, BeyondTrust SAML – Privileged Remote Access.



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**.

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



Microsoft Azure | Search resources, services, and docs (G+)

Home > 2nlp6t | Enterprise applications > Enterprise applications | All applications >

BeyondTrust SAML - Privileged Remote Access | Overview

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Self-service
 - Custom security attributes
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs
 - Provisioning logs
 - Access reviews
- Troubleshooting + Support
 - New support request

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

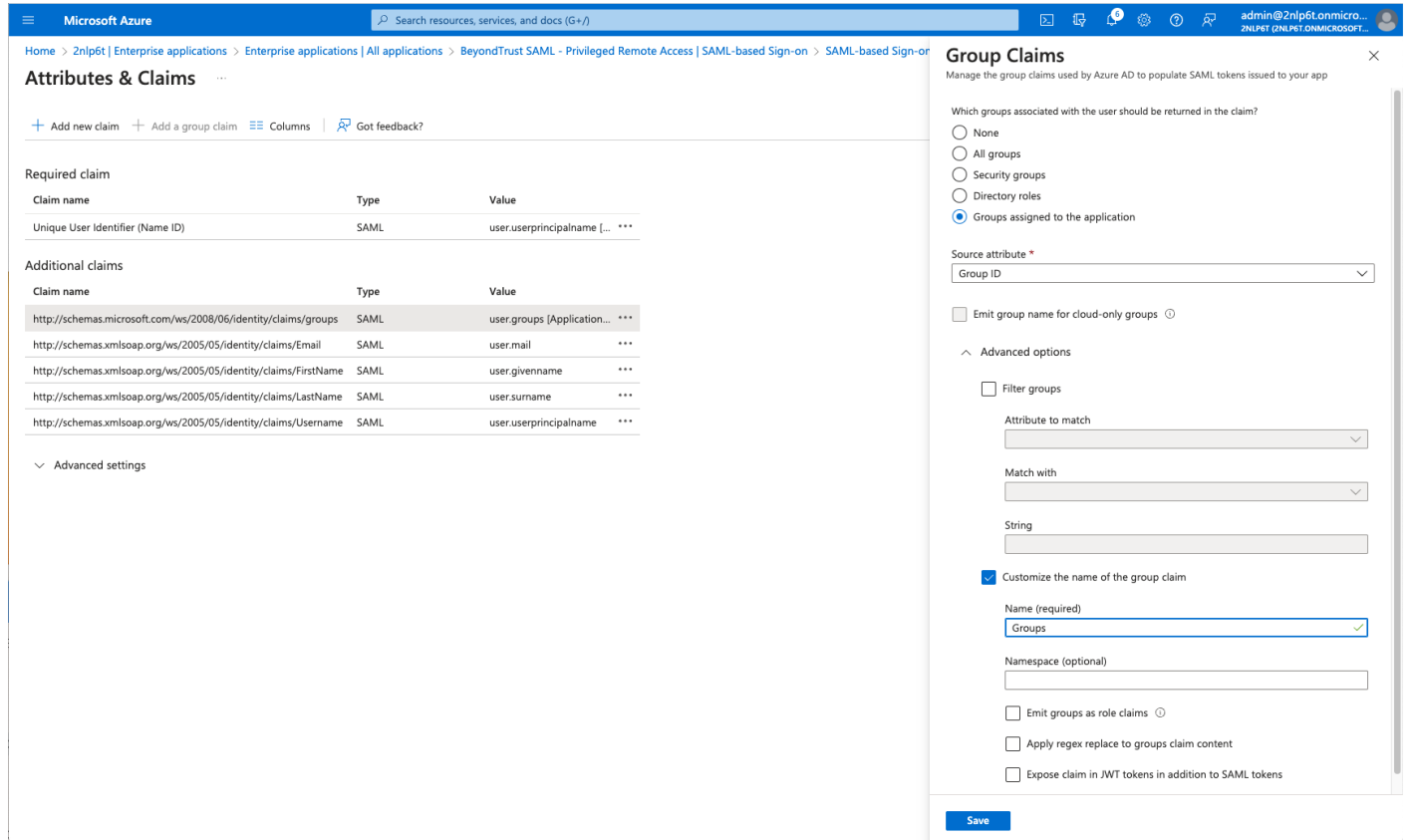
- Sign in charts have moved!**
The new Insights view shows sign in info along with other useful application data. [View insights](#)
- Delete Application has moved to Properties**
You can now delete your application from the Properties page. [View properties](#)
- Getting started has moved to Overview**
The Getting started page has been replaced by the steps above

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


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

- 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



The screenshot shows the Microsoft Azure portal interface for configuring SAML-based Sign-on. The main section is titled "Attributes & Claims" and displays a table of claims. The "Required claim" table has one entry: Unique User Identifier (Name ID) with Type SAML and Value user.userprincipalname [...]. The "Additional claims" table lists several claims including groups, email, givenname, surname, and userprincipalname. On the right, the "Group Claims" configuration pane is open, showing options for which groups to return in the claim (selected: Groups assigned to the application) and the source attribute (Group ID). Advanced options include filtering groups and customizing the group claim name (set to "Groups").

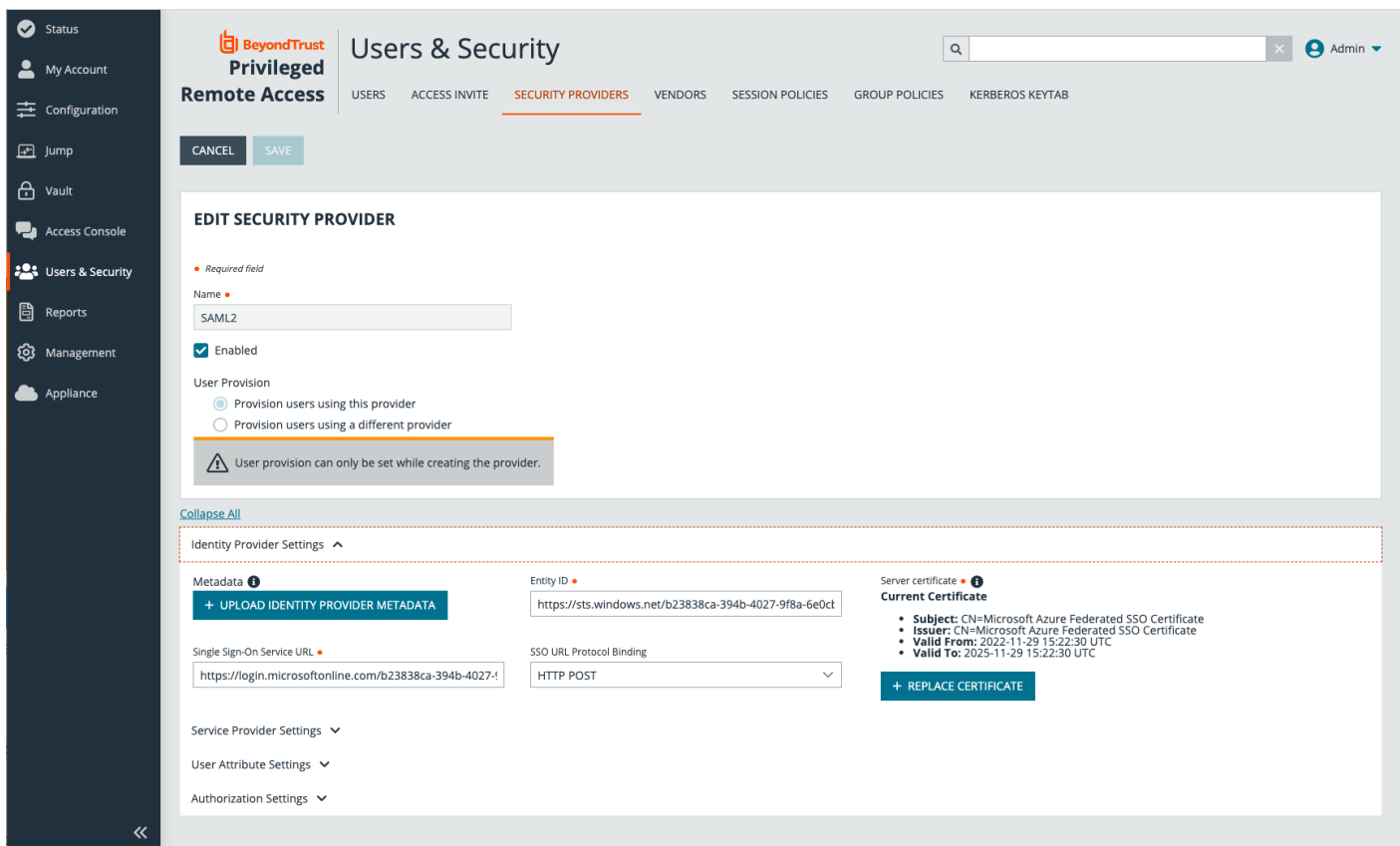
 **Note:** The group claim must be configured to use only groups assigned to the application, to prevent errors that may occur if a user belongs to more than 150 AD groups. For more information, please see [Configure group claims for applications by using Azure Active Directory](https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connec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

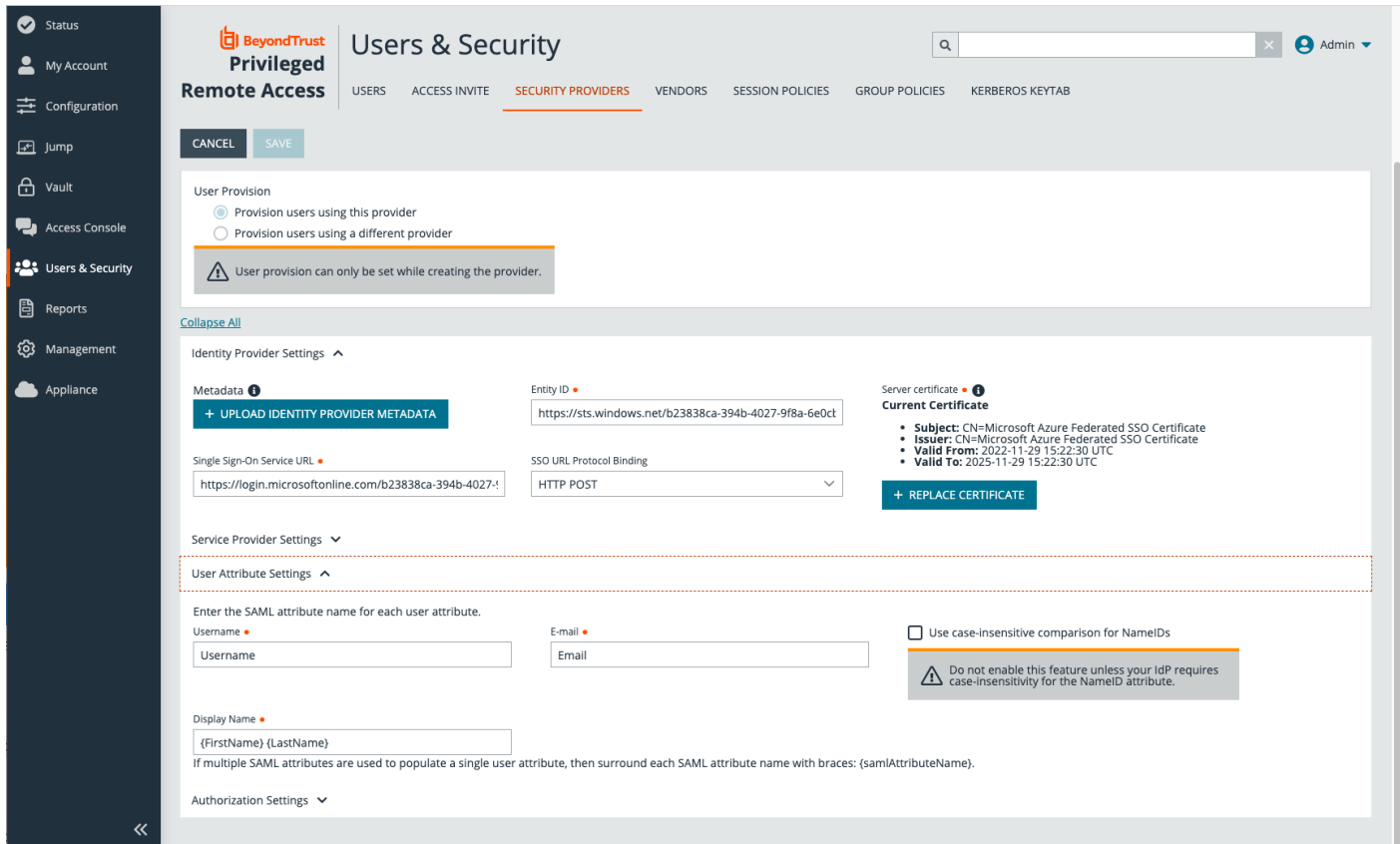
Once the app has been configured, follow these steps to add the provider to Privileged Remote Access:

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.



The screenshot displays the 'Users & Security' management console. The 'Security Providers' tab is active, showing the configuration for a SAML2 provider. The 'Name' field is set to 'SAML2' and is marked as a required field. The 'Enabled' checkbox is checked. Under 'User Provision', the option 'Provision users using this provider' is selected. A warning message states: 'User provision can only be set while creating the provider.' The 'Identity Provider Settings' section is expanded, showing fields for 'Metadata' (with an upload button), 'Entity ID' (https://sts.windows.net/b23838ca-394b-4027-9f8a-6e0ct), 'Single Sign-On Service URL' (https://login.microsoftonline.com/b23838ca-394b-4027-4...), and 'SSO URL Protocol Binding' (HTTP POST). The 'Server certificate' section shows the 'Current Certificate' details: Subject: CN=Microsoft Azure Federated SSO Certificate, Issuer: CN=Microsoft Azure Federated SSO Certificate, Valid From: 2022-11-29 15:22:30 UTC, and Valid To: 2025-11-29 15:22:30 UTC. A 'REPLACE CERTIFICATE' button is visible.

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



The screenshot displays the 'Users & Security' configuration page in the BeyondTrust Privileged Remote Access console. The 'SECURITY PROVIDERS' tab is active, and the 'User Attribute Settings' section is highlighted with a dashed red border. The settings are as follows:

- User Provision:**
 - Provision users using this provider
 - Provision users using a different provider
- Identity Provider Settings:**
 - Metadata:** + UPLOAD IDENTITY PROVIDER METADATA
 - Entity ID:** https://sts.windows.net/b23838ca-394b-4027-9f8a-6e0ct
 - Single Sign-On Service URL:** https://login.microsoftonline.com/b23838ca-394b-4027-4
 - SSO URL Protocol Binding:** HTTP POST
 - Server certificate:**
 - Current Certificate:**
 - Subject: CN=Microsoft Azure Federated SSO Certificate
 - Issuer: CN=Microsoft Azure Federated SSO Certificate
 - Valid From: 2022-11-29 15:22:30 UTC
 - Valid To: 2025-11-29 15:22:30 UTC
 - + REPLACE CERTIFICATE
- User Attribute Settings:**
 - Enter the SAML attribute name for each user attribute.
 - Username:** Username
 - E-mail:** Email
 - Display Name:** {FirstName} {LastName}
 - Note: If multiple SAML attributes are used to populate a single user attribute, then surround each SAML attribute name with braces: {samlAttributeName}.
 - Use case-insensitive comparison for NameIDs
 - Warning: Do not enable this feature unless your IdP requires case-insensitivity for the NameID attribute.

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

The screenshot shows the 'Users & Security' console with the 'SECURITY PROVIDERS' tab selected. A SAML2 provider is being configured. The 'Authorization Settings' section is expanded, showing the following configuration:

- Group Lookup Attribute Name: Groups
- Delimiter: (empty)
- Available Groups: team_a
- Default Group Policy: Vendors



For more information, please see [SAML for Single Sign-On Authentication](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm) 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](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.