BeyondTrust

Privileged Remote Access
Beyond Identity SAML Integration Guide

TC:3/4/2024

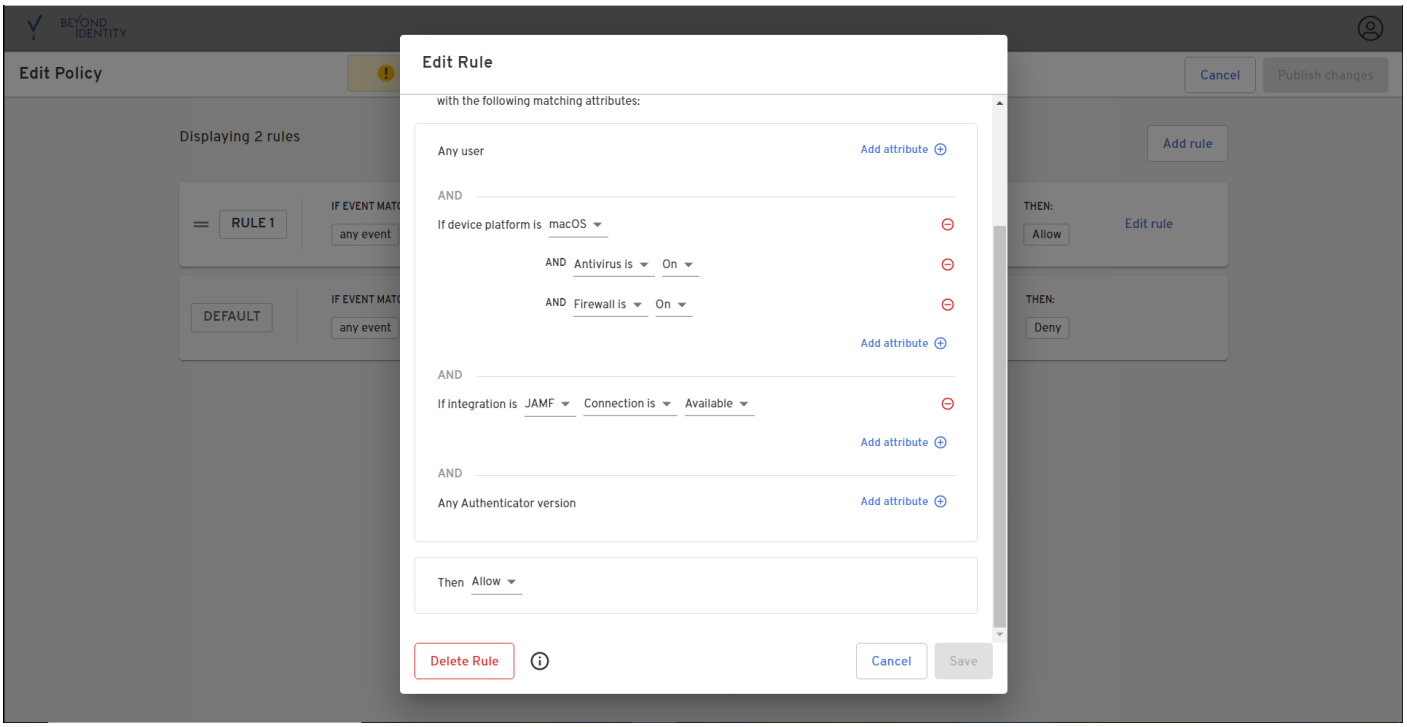
Table of Contents

Configure SAML 2.0 for Privileged Remote Access using Beyond Identity

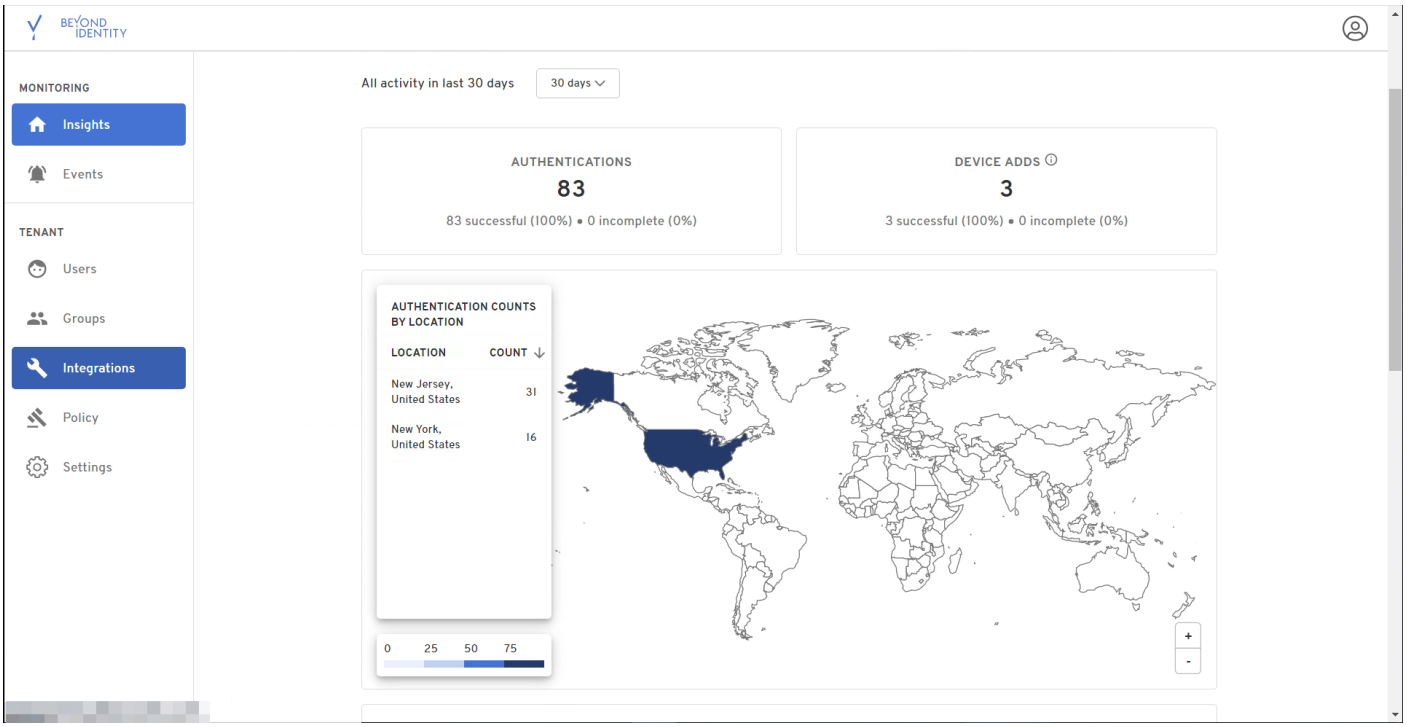
Using Beyond Identity with SAML for Privileged Remote Access provides several benefits:

- 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.



Beyond Identity can provide insights into access activity.

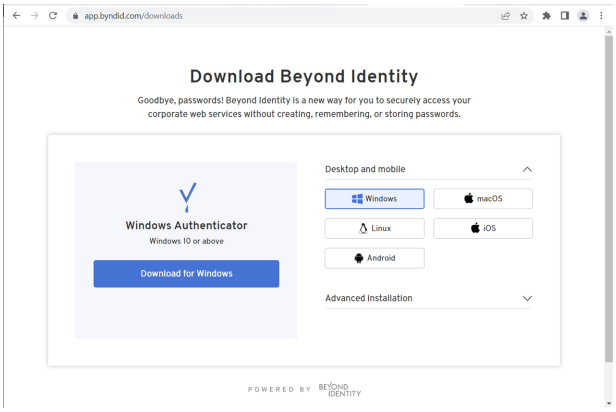


To use the Beyond Identity app, you must download and install the application, and configure it and BeyondTrust Privileged Remote Access to work together. The integration is configured using POST, not redirect.

Download the Beyond Identity App

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

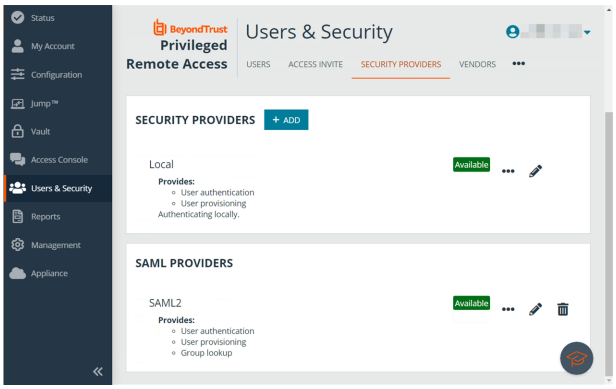
Download and install the Beyond Identity app, and then use the app to authenticate your instance of Beyond Identity.



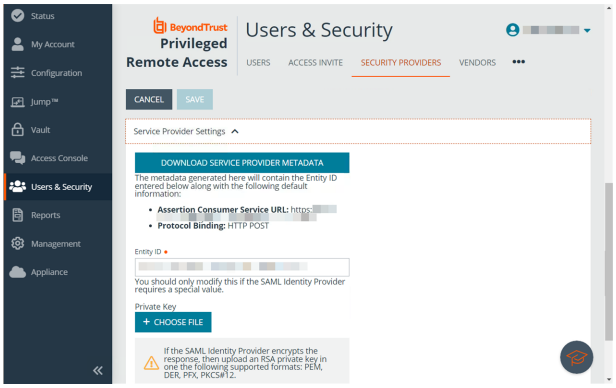
Configure Beyond Identity

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

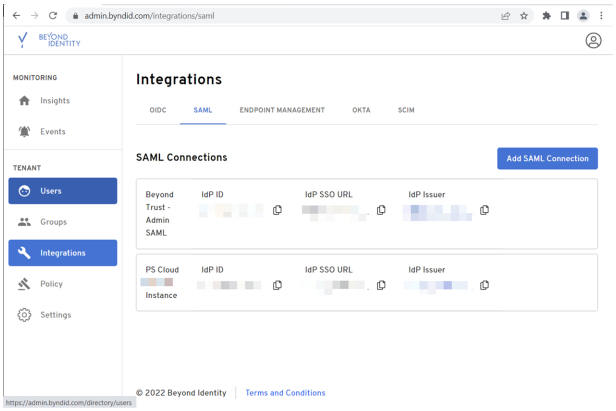
1. If Beyond Identity is already open in a browser tab, open a new browser tab for BeyondTrust Privileged Remote Access.
2. Go to the admin interface of the Privileged Remote Access instance.
3. Click **Users & Security** on the left menu, and then click the **Security Providers** tab.
4. Click **Add** and select **SAML2**.



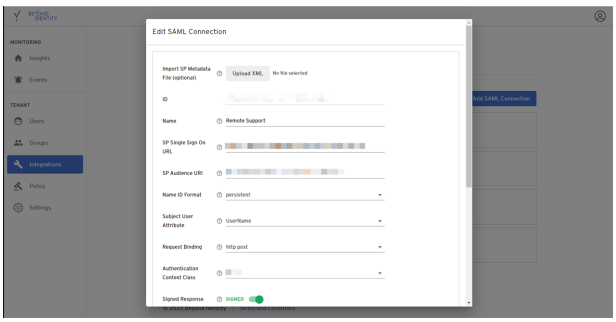
5. Scroll down and expand the **Service Provider Settings**.
6. Locate the **Assertion Consumer Service URL** and the **Entity ID**. These are required for Beyond Identity. Alternately, click **Download Service Provider Metadata**.



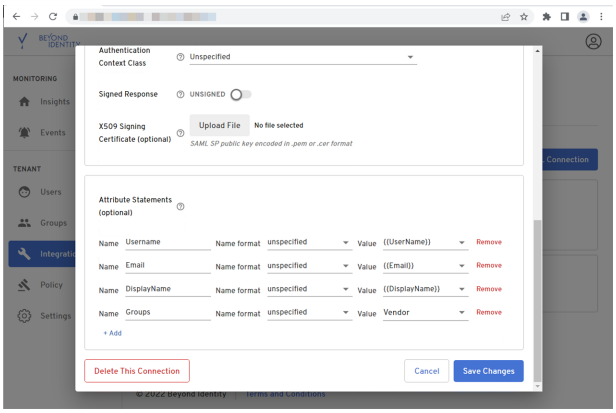
7. If Beyond Identity is not already open, open it in a new browser tab.
8. Click **Integrations** on the left menu.
9. Click the **SAML** tab.
10. Click **Add SAML Connection**.



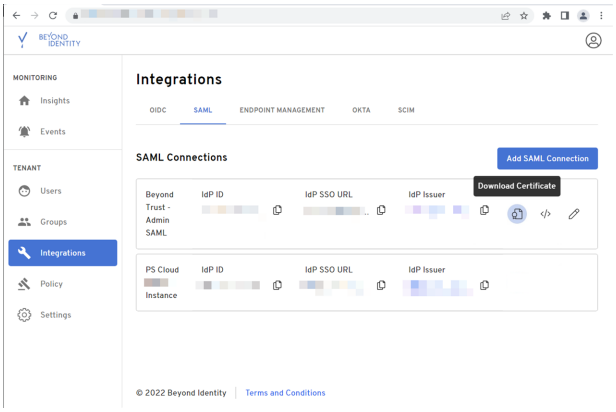
11. If you have downloaded the service provider metadata, click **Upload XML** and locate the file on your device.
12. If you have not downloaded the information, then:
    - Copy the **Assertion Consumer Service URL** in Privileged Remote Access to **SP Single Sign On URL** in Beyond Identity.
    -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



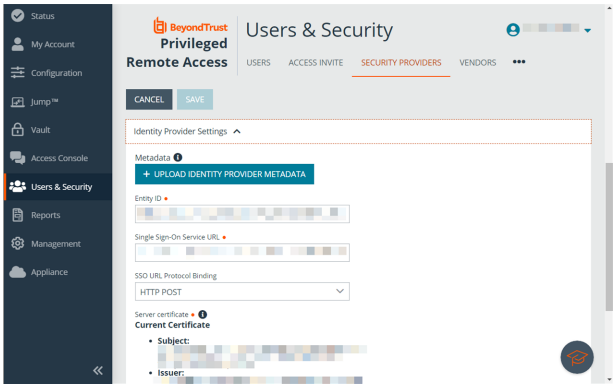
13. In Beyond Identity, configure **Attribute Statements**. Groups includes a PRA group to be assigned via the SAML assertion.



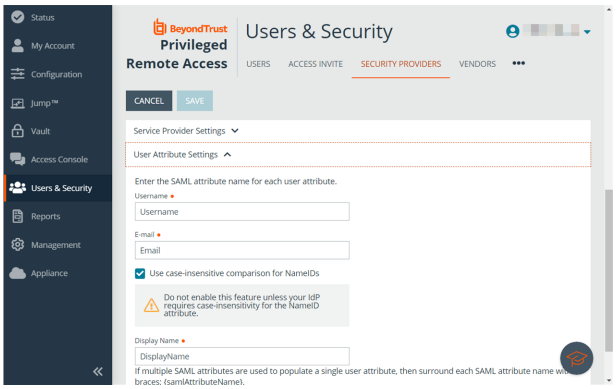
14. In Beyond Identity, click **Save Changes**.
15. In the **SAML Connections** panel, locate the connection just added.
16. For the new connection:
    - Click the **Download Certificate** icon.
    - Click the **Download Metadata** icon **</>**.



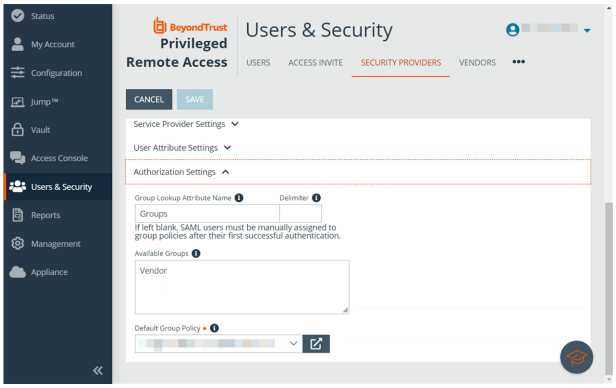
17. Return to the browser tab for the admin interface of the BeyondTrust Privileged Remote Access instance.
18. In the Privileged Remote Access admin interface:
    - Click **Upload Identity Provider Metadata** and locate the file on your device.
    - Click **Upload Certificate** (or **Replace Certificate**,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



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



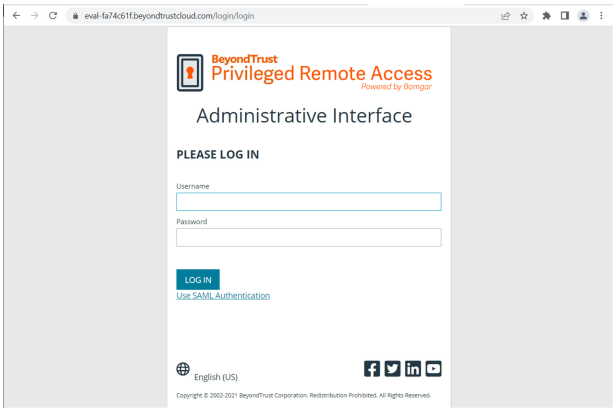
21. Scroll down and expand **Authorization Settings**.
22. Configure as required. A **Default Group Policy** must be selected.
23. Click **Save**.
24. Log out of BeyondTrust Privileged Remote Access.



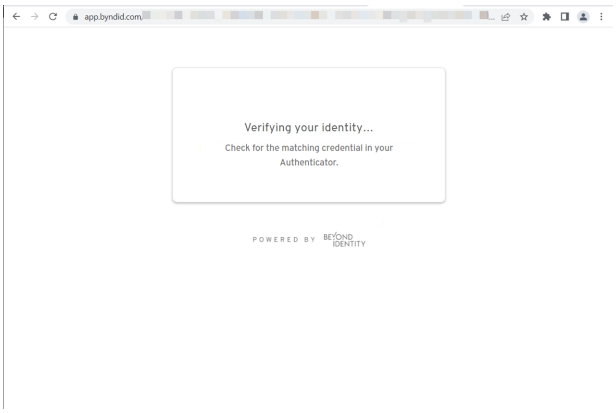
Test Beyond Identity on your Device

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.

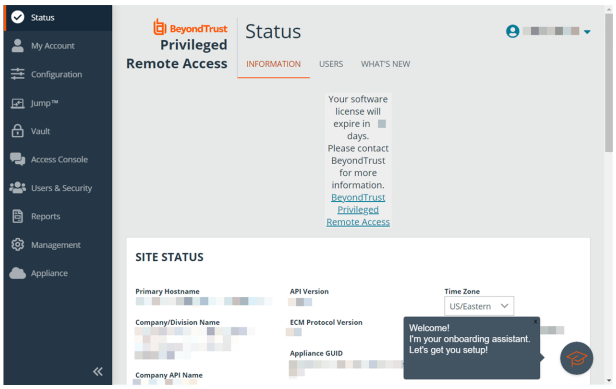
On the login page for Privileged Remote Access, click **Use SAML Authentication**.



A screen shows the Beyond Identity app verifying identity.



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



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 https://beyondtrustcorp.service-now.com/csm to chat with Support.