Privileged Remote Access SecureAuth Arculix Integration

Table of Contents

Integrate BeyondTrust Privileged Remote Access and SecureAuth Arculix

Arculix by SecureAuth allows BeyondTrust customers to securely enable efficient access to Privileged Remote Access, while providing a flexible and frictionless user experience.

This integration is based on Arculix SAML (SP-initiated) integration.

This integration requires a working Arculix test User with the Arculix mobile App that can connect to the Arculix SAML Applications portal.

Before setting up the integration, create a Group Policy in BeyondTrust Privileged Remote Access for Arculix users to authenticate to Privileged Remote Access.

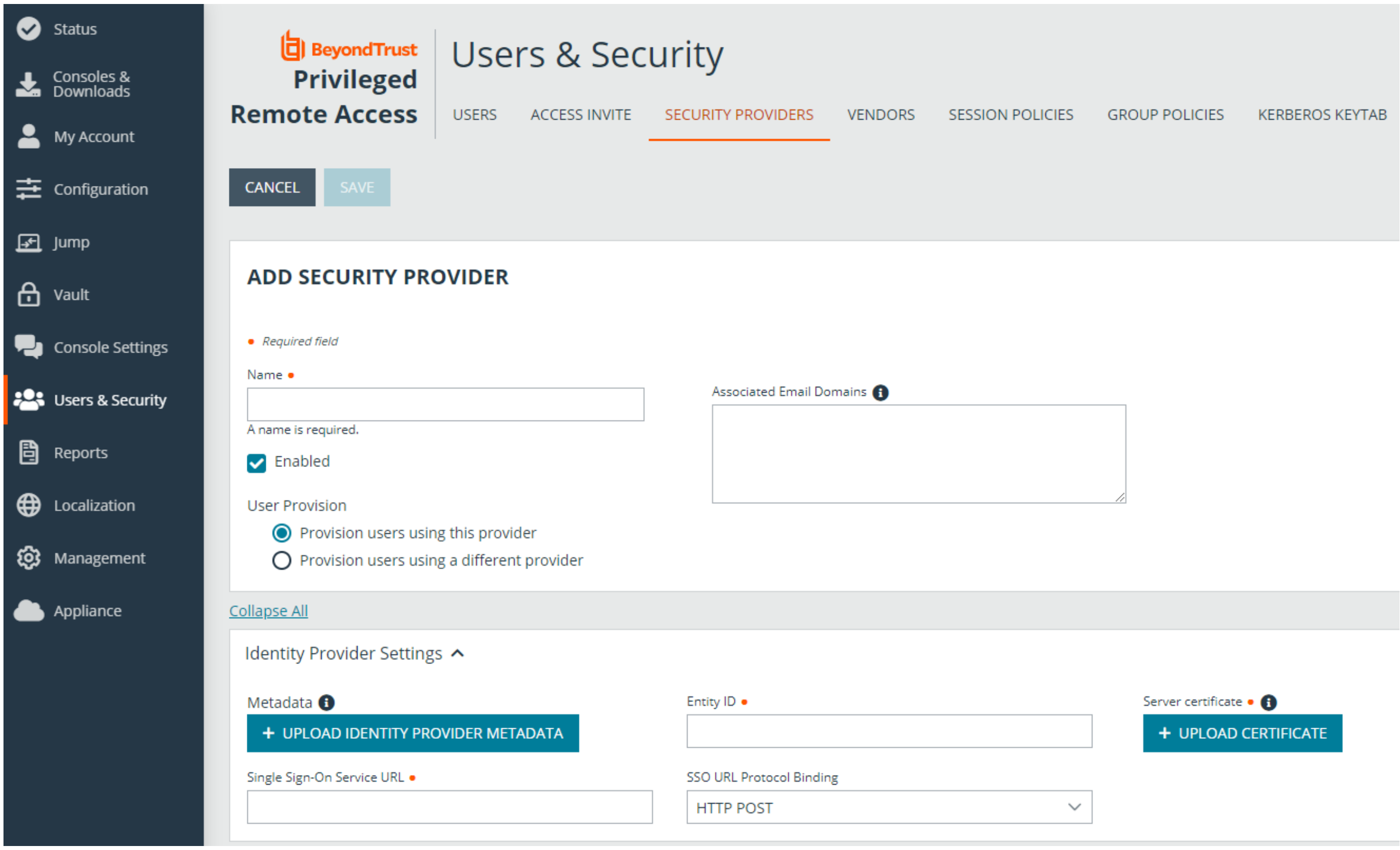
For more information, please see

- *Arculix SAML (SP-initiated) integration at https://docs.secureauth.com/arculix/en/arculix-saml--sp-initiated--integration.html.*
- *Manage users in Acrulix at https://docs.secureauth.com/arculix/en/manage-users.html.*
- *Arculix by SecureAuth overview at https://docs.secureauth.com/arculix/en/arculix-by-secureauth-overview.html.*
- *Use SAML for Single Sign-On Authentication in BeyondTrust Privileged Remote Access at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/security-providers/saml/index.htm .*
- *Group Policies: Apply User Permissions to Groups of Users in BeyondTrust Privileged Remote Access at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/admin/group-policies.htm.*

Configure BeyondTrust for Integration with Arculix

Go to the administrative **/login** interface of your BeyondTrust Privileged Remote Access instance and follow these steps:

1. Click **Users & Security**, then click **Security Providers**.
2. Click **+ADD**.
3. Select **SAML2**.



☑ Enabled

User Provision

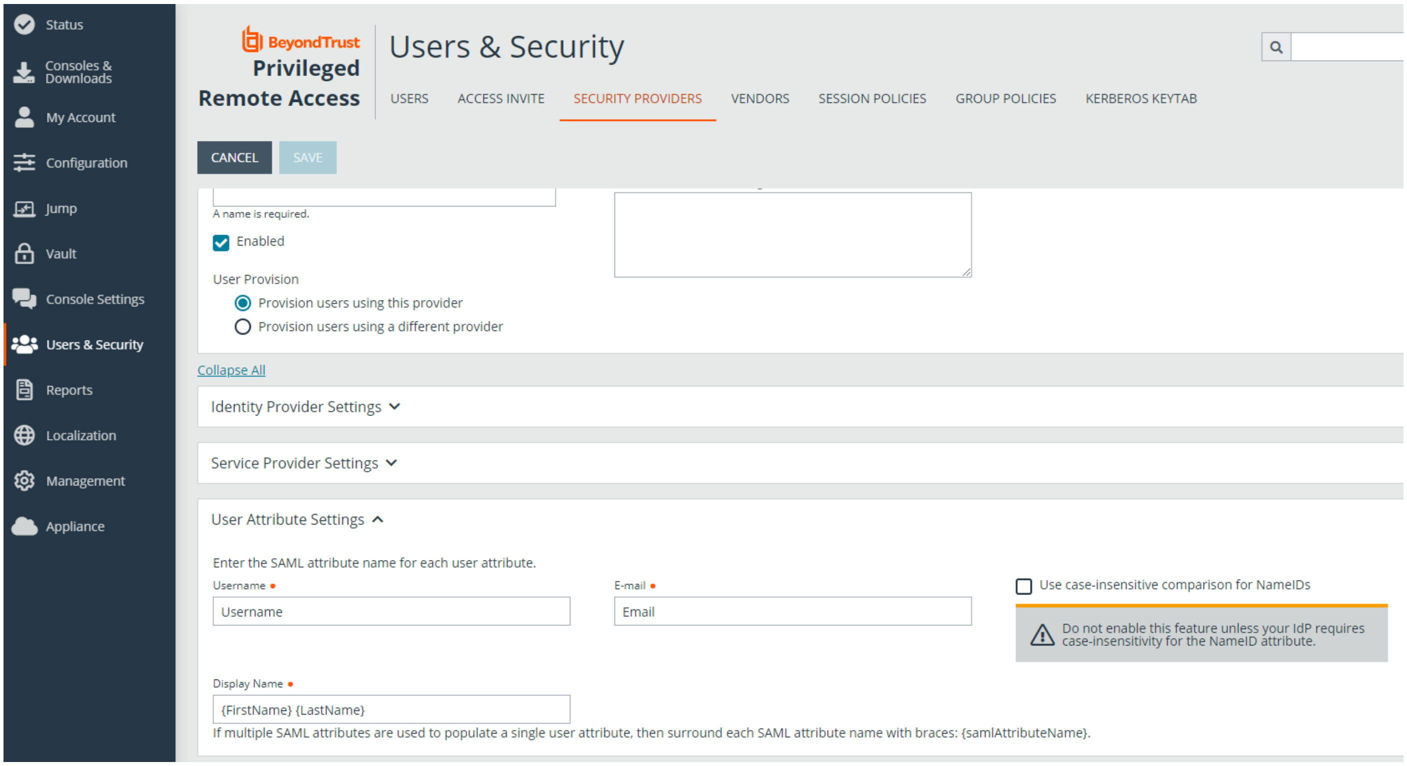
● Provision users using this provider

○ Provision users using a different provider

SSO URL Protocol Binding: HTTP POST

4. Enter your desired name, such as Arculix.
5. Refer to the Arculix documentation (link above) to obtain the **Entity ID**, **Single Sign-on Service URL**, and the **Certificate**.
6. Note the information in the **Service Provider Settings**. This is required when configuring Arculix.

7. Verify that **User Attribute Settings** match the information in Arculix.



A name is required.

☑ Enabled

User Provision

● Provision users using this provider

○ Provision users using a different provider

Enter the SAML attribute name for each user attribute.

Username •: Username

E-mail •: Email

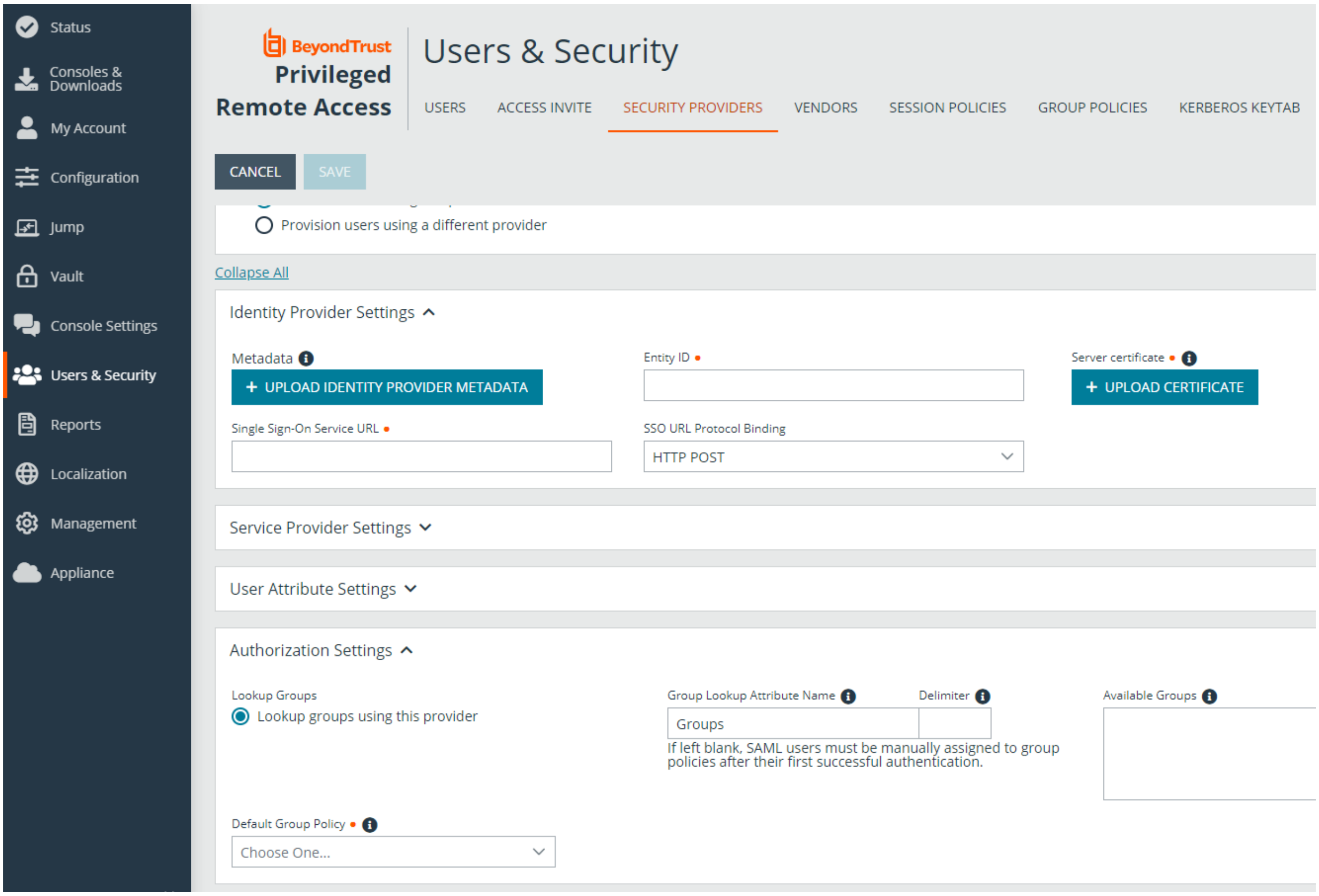
☐ Use case-insensitive comparison for NameIDs

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

Display Name •: {FirstName} {LastName}

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

8. Configure **Authorization Settings** to match Arculix and assign the default Group Policy.



○ Provision users using a different provider

Identity Provider Settings

Metadata

Entity ID •

Server certificate •

Single Sign-On Service URL •

SSO URL Protocol Binding: HTTP POST

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.

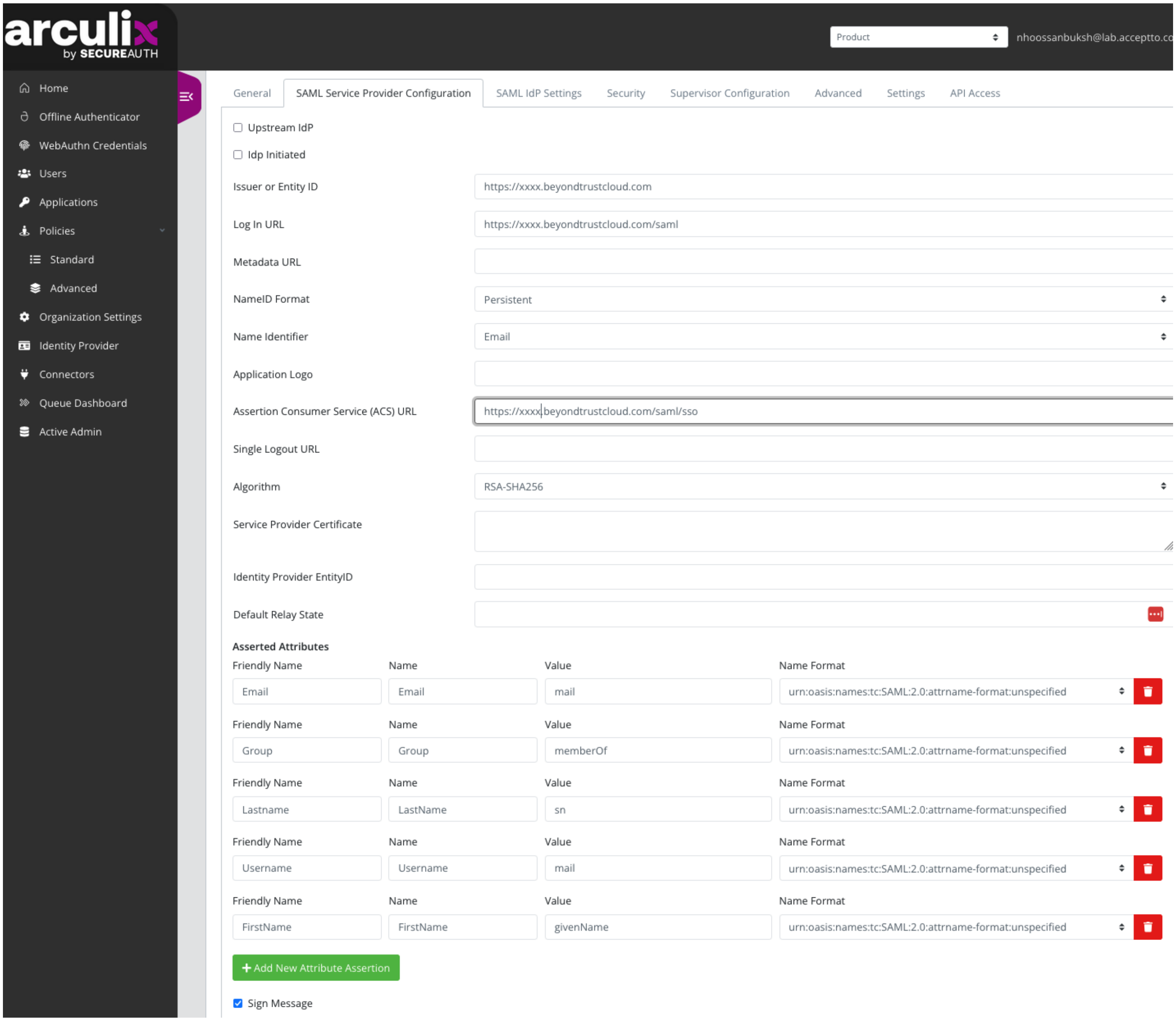
Available Groups

Default Group Policy •: Choose One...

Configure SecureAuth Arculix for SAML (SP-initiated) Integration

Log in to your Arculix instance and follow these steps:

1. Create a new Application. Use a recognizable name, such as BeyondTrust Privileged Remote Access.
2. Click **SAML Service Provider Configuration**.



☐ Upstream IdP

☐ Idp Initiated

Issuer or Entity ID: https://xxxx.beyondtrustcloud.com

Log In URL: https://xxxx.beyondtrustcloud.com/saml

Metadata URL:

NameID Format: Persistent

Name Identifier: Email

Application Logo:

Assertion Consumer Service (ACS) URL: https://xxxx.beyondtrustcloud.com/saml/sso

Single Logout URL:

Algorithm: RSA-SHA256

Service Provider Certificate:

Identity Provider EntityID:

Default Relay State:

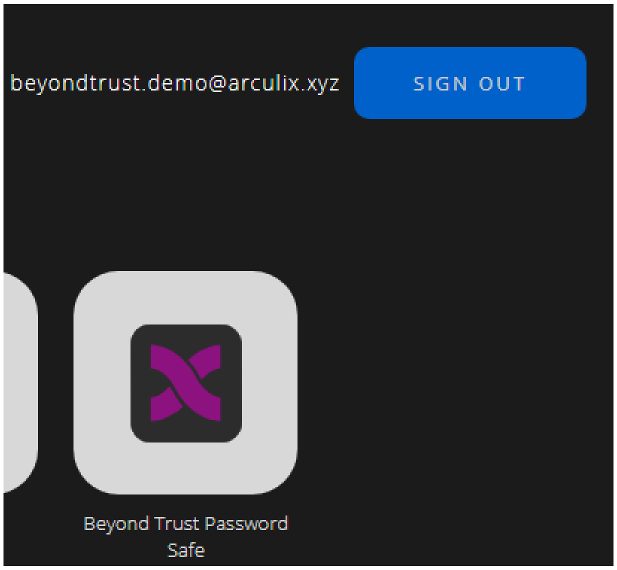
Asserted Attributes

Friendly Name	Name	Value	Name Format
Email	Email	mail	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Group	Group	memberOf	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Lastname	LastName	sn	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Username	Username	mail	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
FirstName	FirstName	givenName	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified

☑ Sign Message

3. Do not check **Upstream IdP** or **IdP Initiated**.
4. Select **Email** for the **Name Identifier**.

5. For **Issuer or Entity ID**, use generated **Entity ID** from the SAML Configuration in Privileged Remote Access, in the **Service Provider Settings**.
6. For **Assertion Consumer Service (ACS) URL**, use generated **Assertion Consumer Service URL** from the SAML Configuration in Privileged Remote Access, in the **Service Provider Settings**.
7. Include the following **Asserted Attributes**:
    - Name: e.g. beyondtrust.demo@arculix.xyz
    - EmailAddress
    - GivenName
    - Surname
    - Group: This needs to correspond to a Group Policy in Name in Privileged Remote Access.
8. Assign the new application to a test user.
9. Test the application:
    a. Click the App in the Arculix portal for the test user.
    b. Single Sign-On authenticates to Privileged Remote Access.
    c. The test user should have access to Privileged Remote Access as per the Group Policy.



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