



BeyondTrust

Privileged Remote Access SecureAuth Arculix Integration

Table of Contents

Integrate BeyondTrust Privileged Remote Access and SecureAuth Arculix	3
Configure BeyondTrust for Integration with Arculix	3
Configure SecureAuth Arculix for SAML (SP-initiated) Integration	7

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.



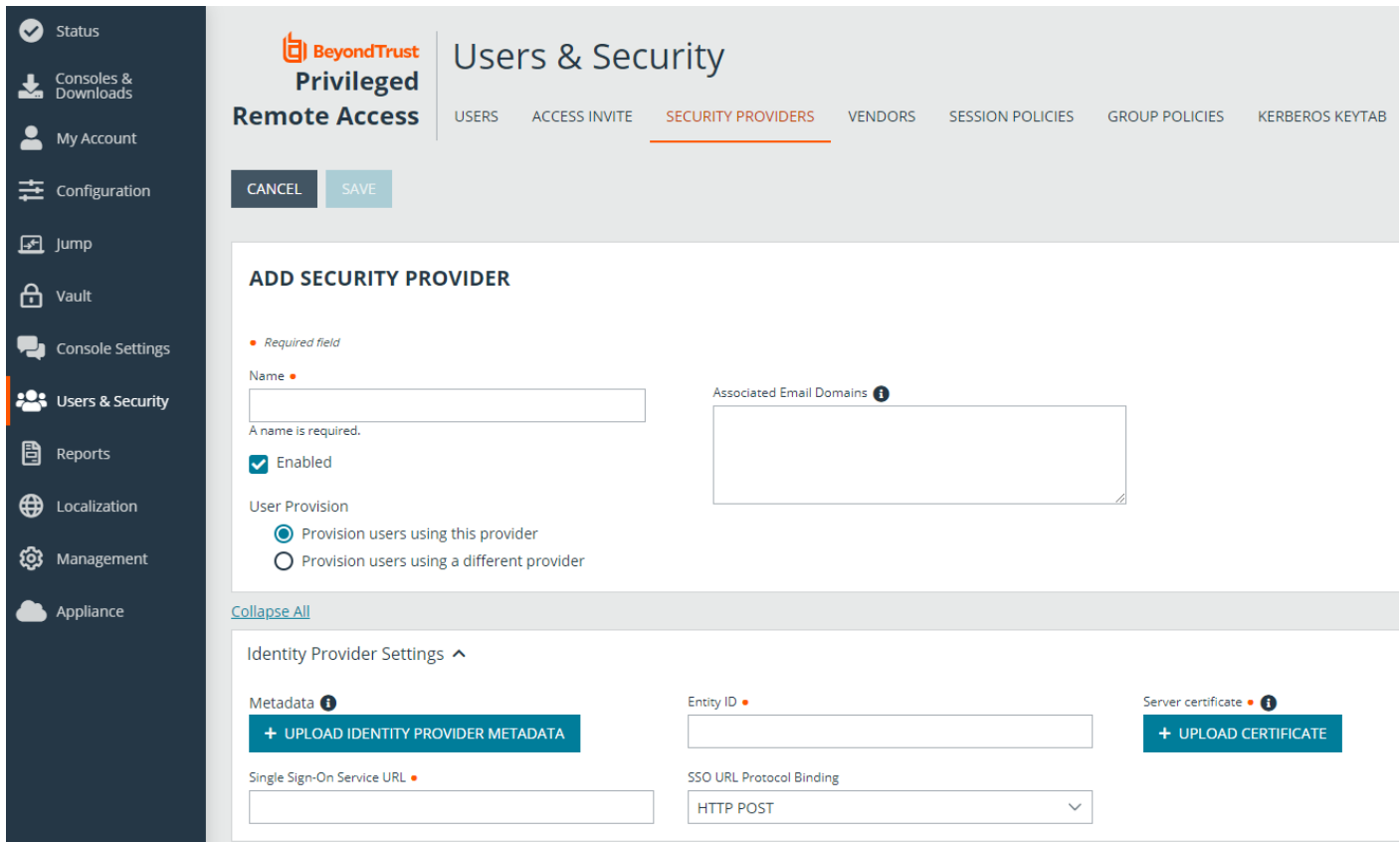
For more information, please see

- [Arculix SAML \(SP-initiated\) integration at https://docs.secureauth.com/arculix/en/arculix-saml--sp-initiated--integration.html.](https://docs.secureauth.com/arculix/en/arculix-saml--sp-initiated--integration.html)
- [Manage users in Arculix at https://docs.secureauth.com/arculix/en/manage-users.html.](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.](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 .](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.](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**.

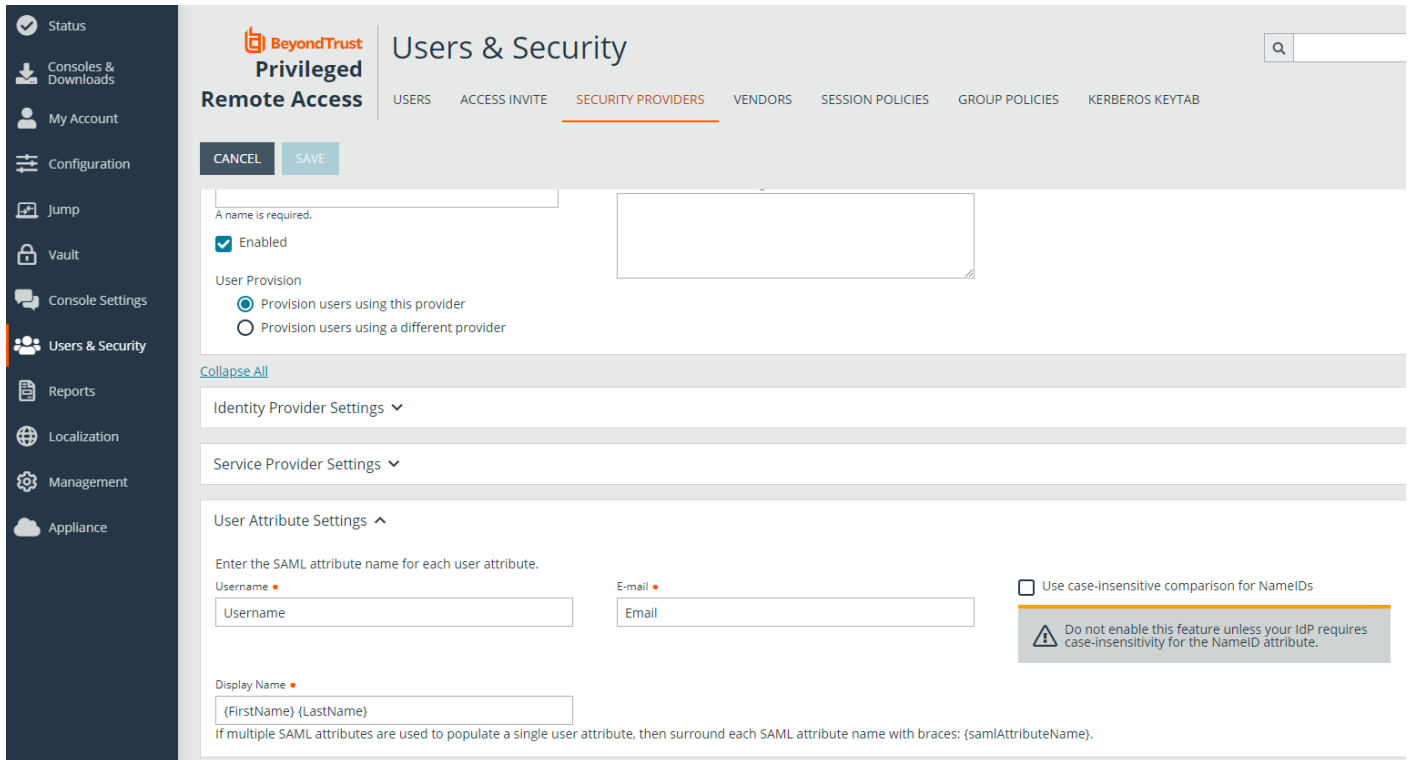


The screenshot shows the 'Users & Security' section of the BeyondTrust Privileged Remote Access console. The 'SECURITY PROVIDERS' tab is active. The 'ADD SECURITY PROVIDER' form includes the following fields and options:

- Name**: A required text input field with a red asterisk. Below it, a message states 'A name is required.'
- Associated Email Domains**: A text area with an information icon.
- Enabled**: A checked checkbox.
- User Provision**: Two radio button options: 'Provision users using this provider' (selected) and 'Provision users using a different provider'.
- Identity Provider Settings**: A section with a collapse arrow, containing:
 - Metadata**: A blue button labeled '+ UPLOAD IDENTITY PROVIDER METADATA' with an information icon.
 - Entity ID**: A text input field with a red asterisk and an information icon.
 - Server certificate**: A blue button labeled '+ UPLOAD CERTIFICATE' with a red asterisk and an information icon.
 - Single Sign-On Service URL**: A text input field with a red asterisk.
 - SSO URL Protocol Binding**: A dropdown menu currently set to '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.



BeyondTrust Privileged Remote Access Users & Security

USERS ACCESS INVITE **SECURITY PROVIDERS** VENDORS SESSION POLICIES GROUP POLICIES KERBEROS KEYTAB

A name is required.

Enabled

User Provision

Provision users using this provider

Provision users using a different provider

[Collapse All](#)

Identity Provider Settings ▾


Service Provider Settings ▾

User Attribute Settings ▲

Enter the SAML attribute name for each user attribute.

Username • E-mail •

Use case-insensitive comparison for NameIDs

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

Display Name •

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

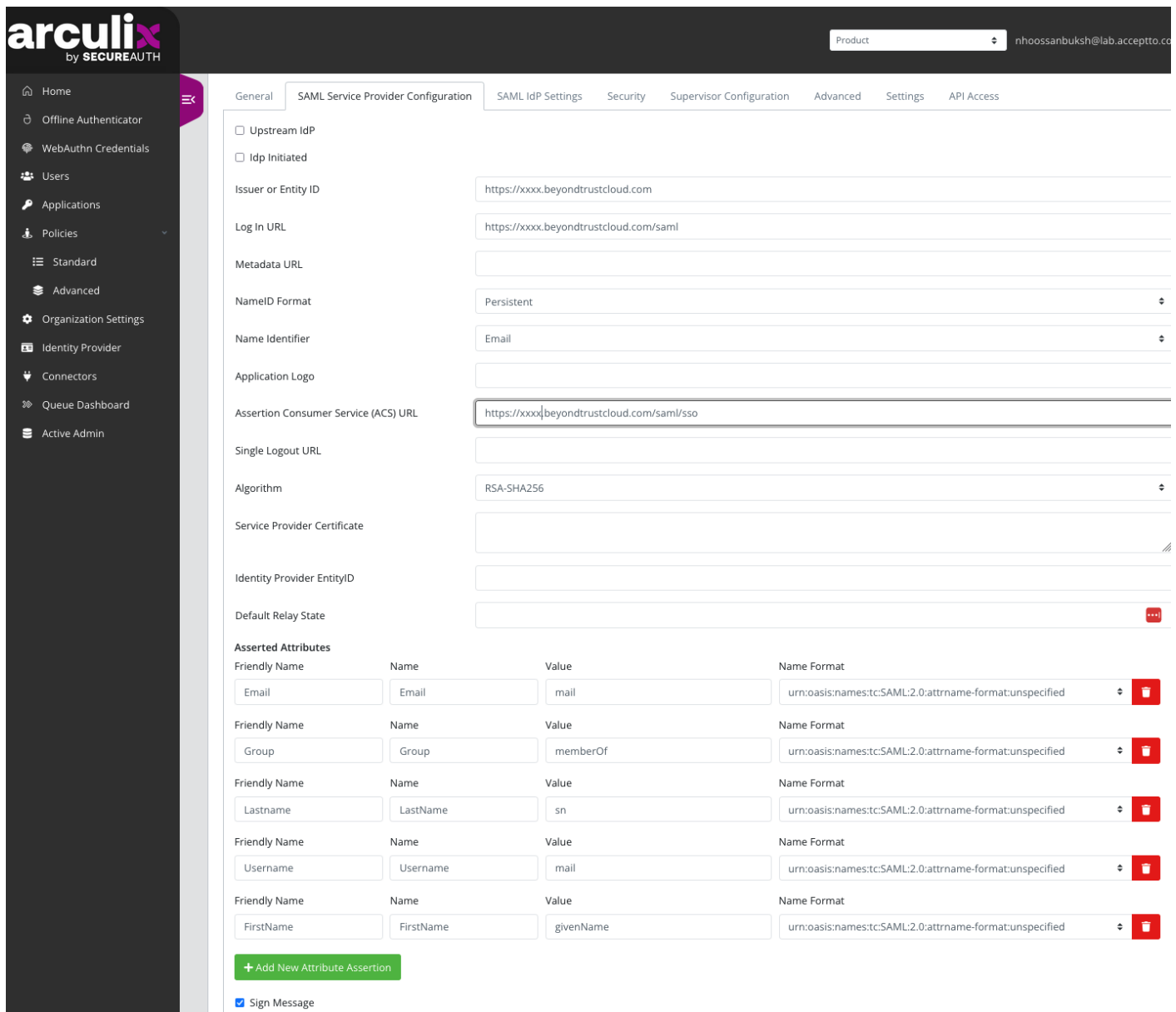
8. Configure **Authorization Settings** to match Arculix and assign the default Group Policy.

The screenshot shows the 'Users & Security' configuration page in the BeyondTrust console. The left sidebar contains navigation options: Status, Consoles & Downloads, My Account, Configuration, Jump, Vault, Console Settings, **Users & Security**, Reports, Localization, Management, and Appliance. The main content area is titled 'Users & Security' and includes tabs for USERS, ACCESS INVITE, SECURITY PROVIDERS (selected), VENDORS, SESSION POLICIES, GROUP POLICIES, and KERBEROS KEYTAB. Below the tabs are 'CANCEL' and 'SAVE' buttons. A radio button option 'Provision users using a different provider' is present. A 'Collapse All' link is also visible. The 'Identity Provider Settings' section is expanded, showing fields for Metadata (with an '+ UPLOAD IDENTITY PROVIDER METADATA' button), Entity ID, Server certificate (with an '+ UPLOAD CERTIFICATE' button), Single Sign-On Service URL, and SSO URL Protocol Binding (set to HTTP POST). Below this are sections for 'Service Provider Settings' and 'User Attribute Settings', both collapsed. The 'Authorization Settings' section is expanded, showing 'Lookup Groups' (with 'Lookup groups using this provider' selected), 'Group Lookup Attribute Name' (set to 'Groups'), 'Delimiter', and 'Available Groups'. A note states: 'if left blank, SAML users must be manually assigned to group policies after their first successful authentication.' At the bottom, there is a 'Default Group Policy' dropdown menu set to '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**.



The screenshot shows the Arculix web interface for SAML Service Provider Configuration. The left sidebar contains navigation options like Home, Offline Authenticator, WebAuthn Credentials, Users, Applications, Policies, Standard, Advanced, Organization Settings, Identity Provider, Connectors, Queue Dashboard, and Active Admin. The main content area is titled 'SAML Service Provider Configuration' and includes tabs for General, SAML IDP Settings, Security, Supervisor Configuration, Advanced, Settings, and API Access. The configuration form includes fields for Issuer or Entity ID, Log In URL, Metadata URL, NameID Format (set to Persistent), Name Identifier (set to Email), Assertion Consumer Service (ACS) URL, Single Logout URL, Algorithm (set to RSA-SHA256), Service Provider Certificate, Identity Provider EntityID, and Default Relay State. Below these are 'Asserted Attributes' with columns for Friendly Name, Name, Value, and Name Format. Five attributes are listed: Email, Group, Lastname, Username, and FirstName. A '+ Add New Attribute Assertion' button and a checked 'Sign Message' checkbox are also visible.

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.

