



# BeyondTrust

## **Remote Support SecureAuth Arculix Integration**

## Table of Contents

---

<b>Integrate BeyondTrust Remote Support and SecureAuth Arculix</b> .....	<b>3</b>
Configure BeyondTrust for Integration with Arculix .....	3
<b>Configure SecureAuth Arculix for SAML (SP-initiated) Integration</b> .....	<b>7</b>

# Integrate BeyondTrust Remote Support and SecureAuth Arculix

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

This integration is based on Arculix SAML (SP-initiated) integration, and is supported for Representatives and Public Portals.

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 Remote Support for Arculix users to authenticate to Remote Support.



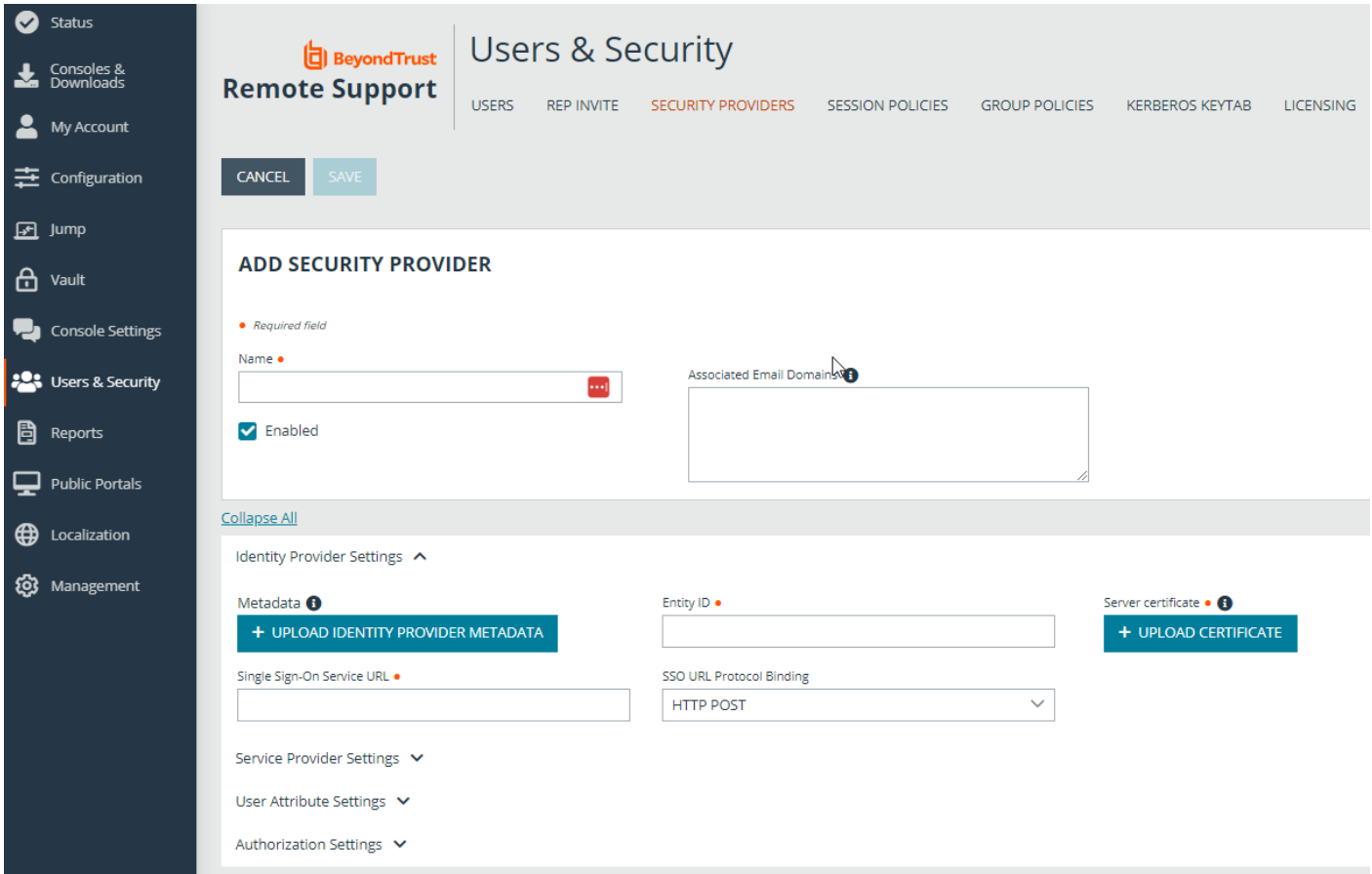
For more information, please see

- [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 Remote Support at https://www.beyondtrust.com/docs/remote-support/documents/authentication/rs-saml-authentication.pdf](https://www.beyondtrust.com/docs/remote-support/documents/authentication/rs-saml-authentication.pdf).
- [Group Policies: Apply User Permissions to Groups of Users in BeyondTrust Remote Support at https://www.beyondtrust.com/docs/remote-support/documents/user/rs-admin.pdf](https://www.beyondtrust.com/docs/remote-support/documents/user/rs-admin.pdf).

## Configure BeyondTrust for Integration with Arculix

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

1. Click **Users & Security**, then click **Security Providers**.
2. Click **+ADD**.
3. Select **SAML For Representatives** or **SAML for Public Portals**. Steps and images below are for SAML for representatives. The process is similar for public portals.

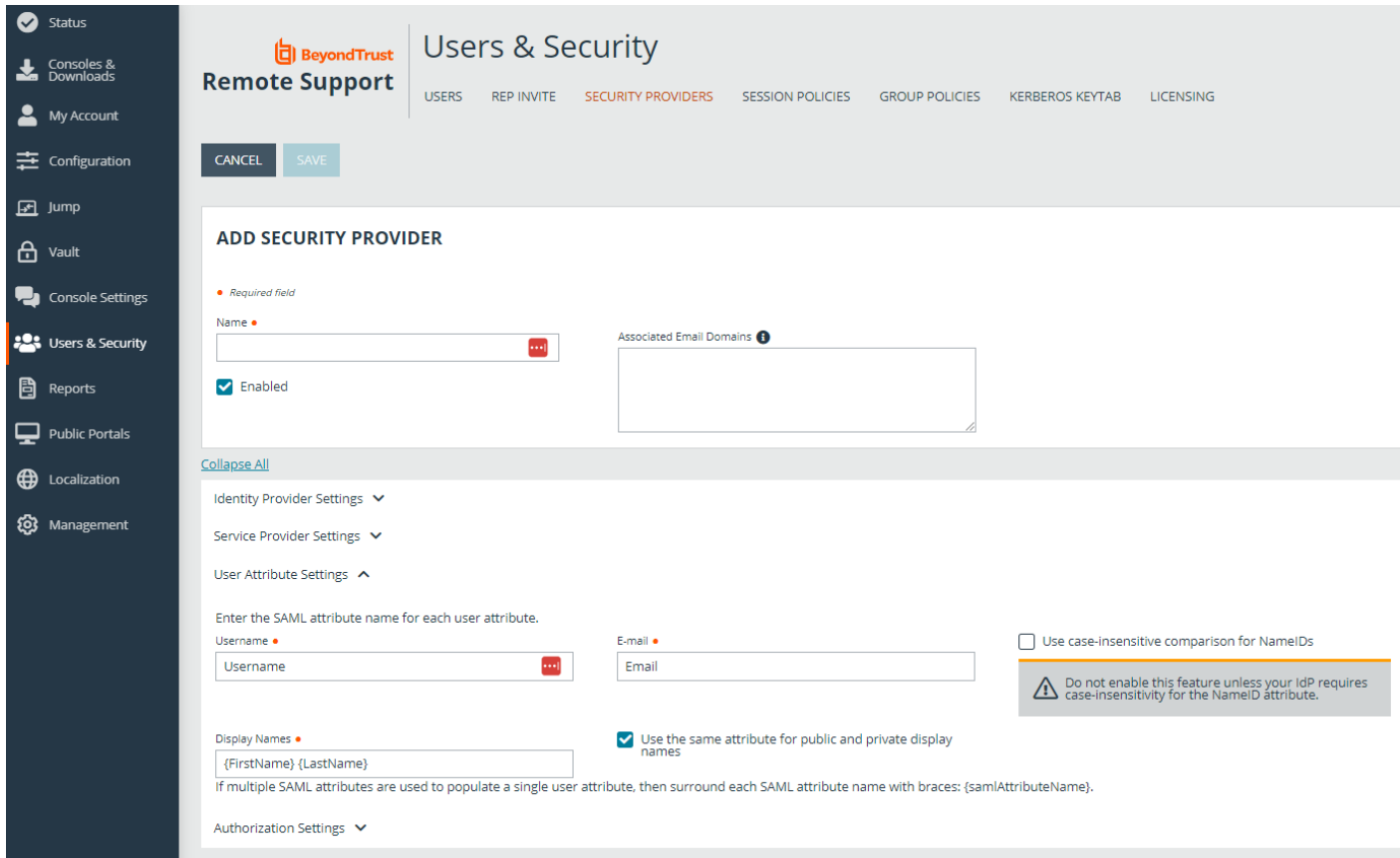


The screenshot shows the 'Users & Security' configuration page in the BeyondTrust Remote Support interface. The page is titled 'ADD SECURITY PROVIDER' and includes a 'CANCEL' and 'SAVE' button at the top. The main form area contains the following fields and options:

- Name**: A required text input field with a red asterisk and a dropdown menu icon.
- Enabled**: A checked checkbox.
- Associated Email Domains**: A large text area for entering email domains, with an information icon.
- Identity Provider Settings**: A section with a dropdown arrow, containing:
  - Metadata**: A button labeled '+ UPLOAD IDENTITY PROVIDER METADATA'.
  - Entity ID**: A required text input field with a red asterisk.
  - Server certificate**: A button labeled '+ UPLOAD CERTIFICATE'.
  - Single Sign-On Service URL**: A required text input field with a red asterisk.
  - SSO URL Protocol Binding**: A dropdown menu currently set to 'HTTP POST'.
- Service Provider Settings**: A dropdown menu.
- User Attribute Settings**: A dropdown menu.
- Authorization Settings**: A dropdown menu.

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.



**Users & Security**

USERS REP INVITE **SECURITY PROVIDERS** SESSION POLICIES GROUP POLICIES KERBEROS KEYTAB LICENSING

CANCEL SAVE

### ADD SECURITY PROVIDER

• Required field

Name •

Associated Email Domains ⓘ

Enabled

[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

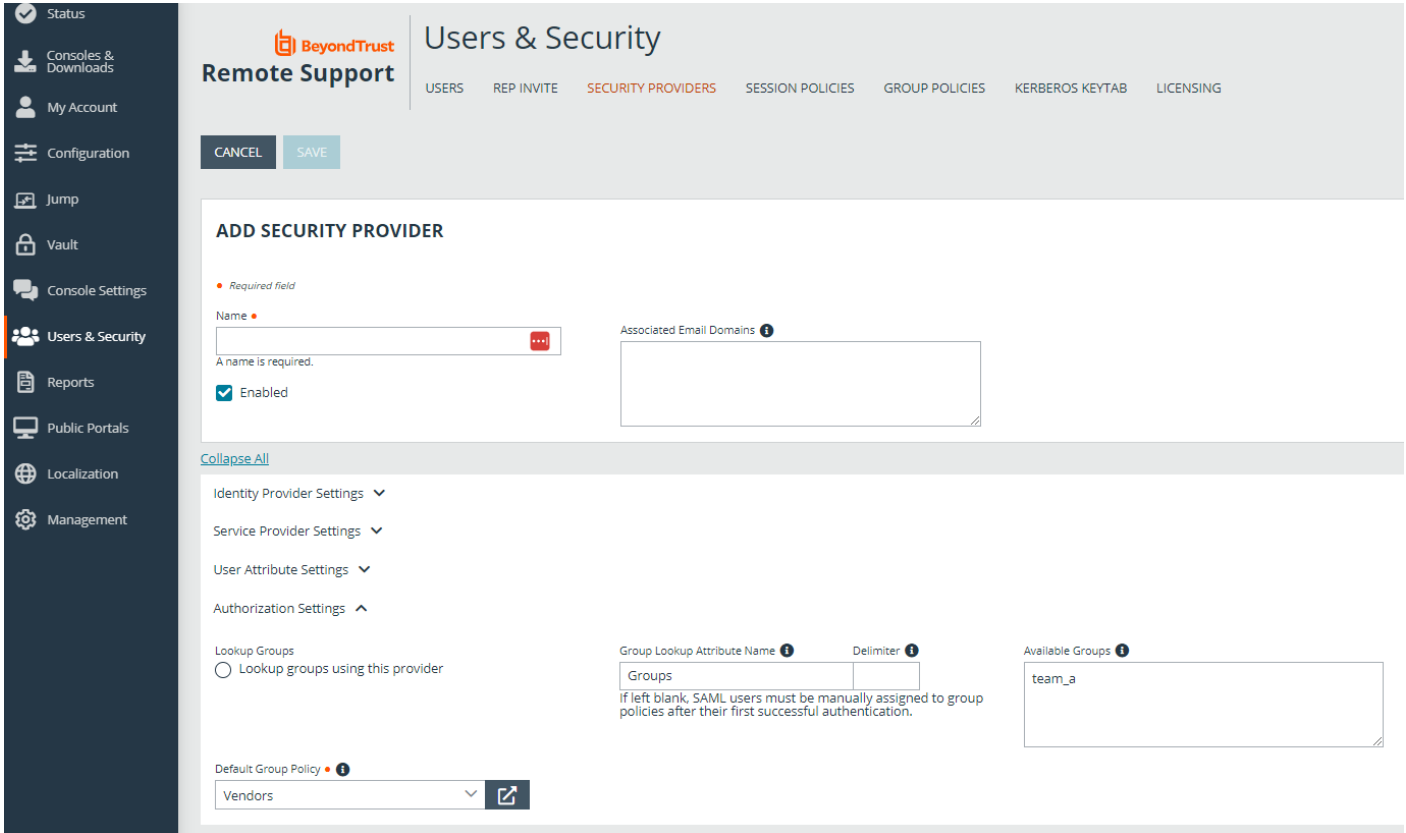
Display Names •   Use the same attribute for public and private display names

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

Authorization Settings ▾

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

8. Configure **Authorization Settings** to match Arculix and assign the default Group Policy. This step is not applicable to **SAML for Public Portals**.

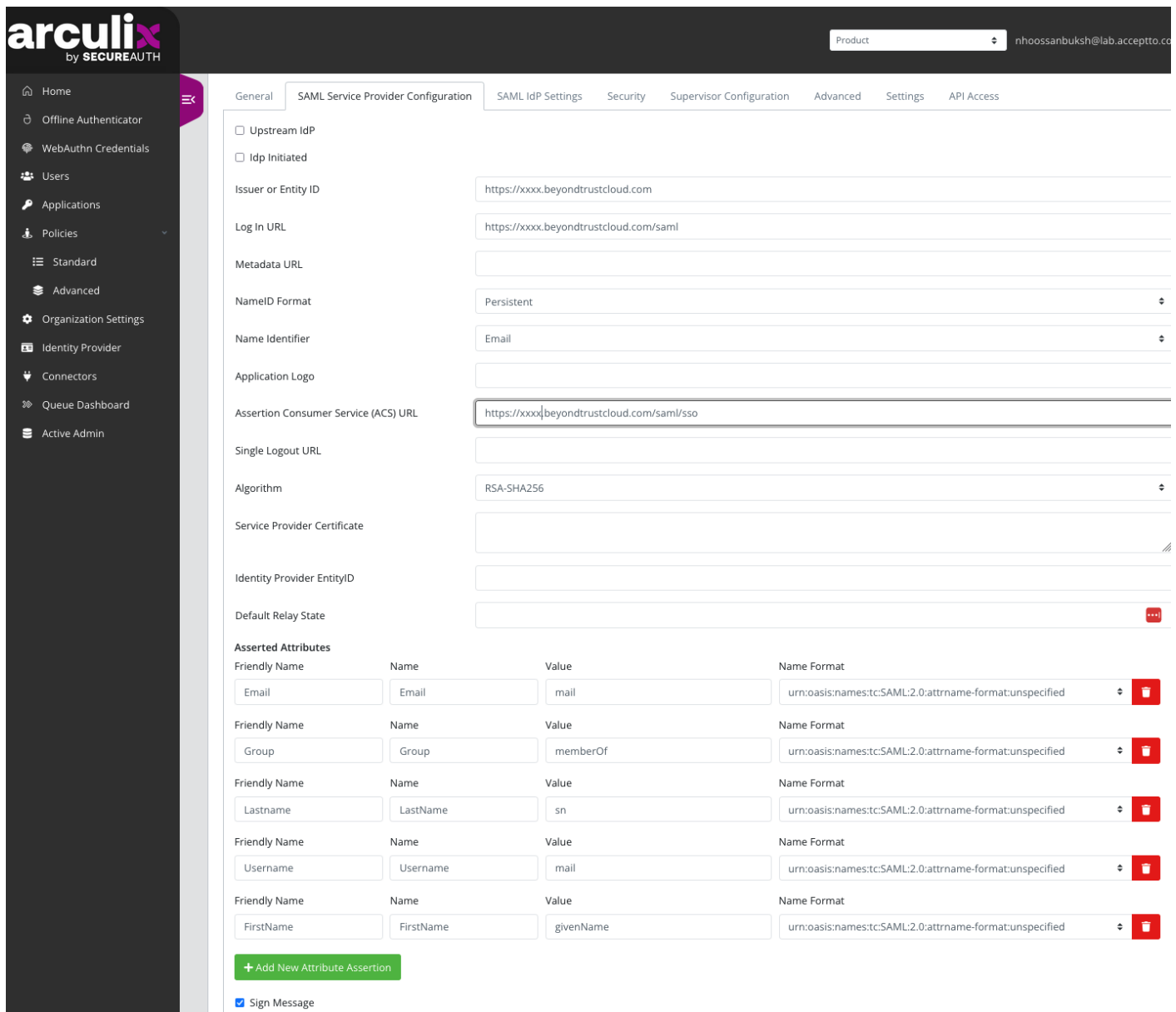


The screenshot shows the 'Users & Security' configuration page in the BeyondTrust Remote Support interface. The page is titled 'ADD SECURITY PROVIDER' and includes a sidebar with navigation options like Status, Consoles & Downloads, My Account, Configuration, Jump, Vault, Console Settings, Users & Security (selected), Reports, Public Portals, Localization, and Management. The main content area has tabs for USERS, REP INVITE, SECURITY PROVIDERS (active), SESSION POLICIES, GROUP POLICIES, KERBEROS KEYTAB, and LICENSING. There are 'CANCEL' and 'SAVE' buttons at the top left. The 'ADD SECURITY PROVIDER' section contains a 'Name' field with a red asterisk and a red 'x' icon, a note 'A name is required.', an 'Associated Email Domains' text area, and a checked 'Enabled' checkbox. Below this is a 'Collapse All' link and a list of settings: Identity Provider Settings, Service Provider Settings, User Attribute Settings, and Authorization Settings. The 'Authorization Settings' section is expanded, showing 'Lookup Groups' with a radio button for 'Lookup groups using this provider', 'Group Lookup Attribute Name' (Groups), 'Delimiter', and 'Available Groups' (team\_a). A 'Default Group Policy' dropdown is set to 'Vendors'.

# Configure SecureAuth Arculix for SAML (SP-initiated) Integration

Log in to your Arculix instance and follow these steps:

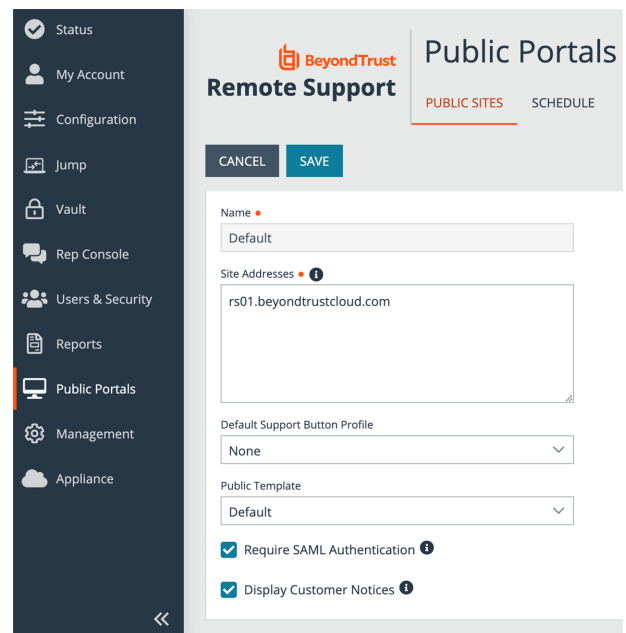
1. Create a new Application. Use a recognizable name, such as BeyondTrust Remote Support.
2. Click **SAML Service Provider Configuration**.



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 a table for defining attributes like 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 Remote Support, in the **Service Provider Settings**.
6. For **Assertion Consumer Service (ACS) URL**, use generated **Assertion Consumer Service URL** from the SAML Configuration in Remote Support, 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 Remote Support.
8. For **SAML for Public Portals**, one more configuration step is required in BeyondTrust Remote Support.
  - Click **Public Portals**, then click **Public Sites**.
  - Edit the portal.
  - Ensure **Require SAML Authentication** and **Display Customer Notices** are checked.
  - This step does not apply to **SAML for Representatives**.



9. Assign the new application to a test user.



10. Test the application:

- a. Click the App in the Arculix portal for the test user.
- b. Single Sign-On authenticates to Remote Support.
- c. The test user should have access to Remote Support as per the Group Policy.

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.

