BeyondTrust

Password Safe
SecureAuth Arculix Integration

TC:4/10/2024

SecureAuth Arculix & BeyondTrust Password Safe

Arculix by SecureAuth allows BeyondTrust customers to securely enable efficient access to privileged credentials and sessions managed by Password Safe, while providing a flexible and frictionless user experience.

This integration is supported for both Password Safe and Password Safe Cloud.

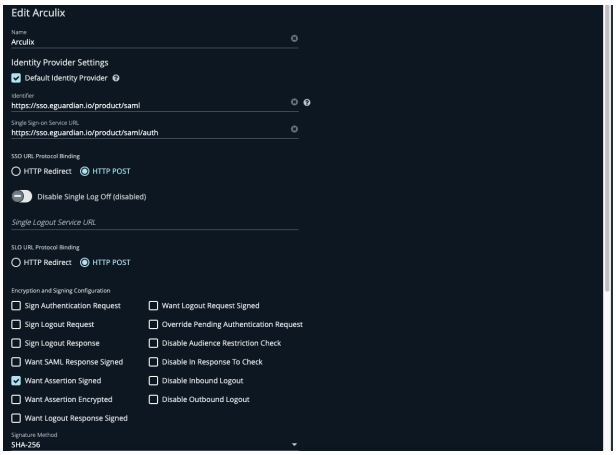
Prerequisites

- A working test user with the Arculix mobile app that can connect to the Arculix Security Assertion Markup Language (SAML) Applications portal. See the Arculix Manage Users documentation here: https://docs.secureauth.com/arculix/en/manage-users.html
- This integration is based on Arculix SAML (IdP-initiated) integration, see documentation here: https://docs.secureauth.com/arculix/en/arculix-saml--idp-initiated--integration.html
- More information about configuring Password Safe, e.g. User Mapping types, can be found here: https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/security-provider.htm

Configure a SAML Provider in Password Safe

To add Arculix as a SAML provider:

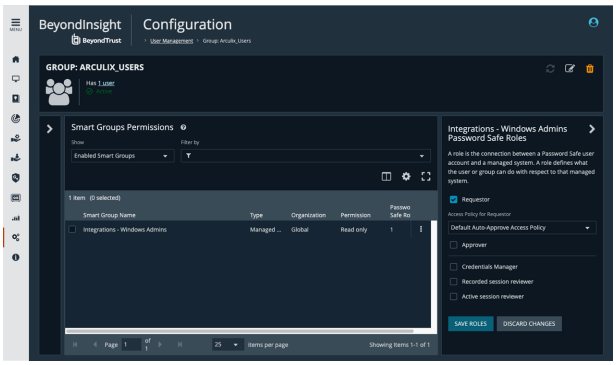
1. As an Administrator, navigate to **Configuration > SAML Configuration**.



2. To find the **Identifier URL**, **Single Sign-on Service URL**, and the **Certificate**, refer to the Arculix documentation link above.
3. Configure the **Encryption and Signing Configuration** to align with the configuration in Arculix.
4. Import the **Identity Provider** certificate from Arculix.

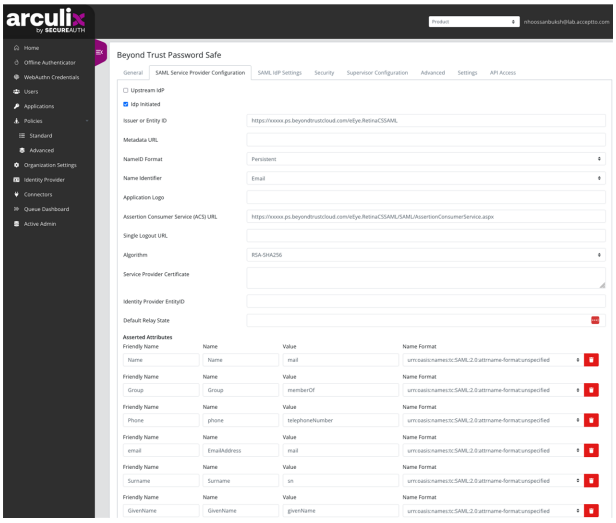
5. Create a local group in Password Safe and assign one or more Managed Account Smart Groups with Read Only permission, and one or more Password Safe roles.

   Managed Account Smart Groups are groups of privileged accounts that members of the group can access for credential check-out and/or session check-out.



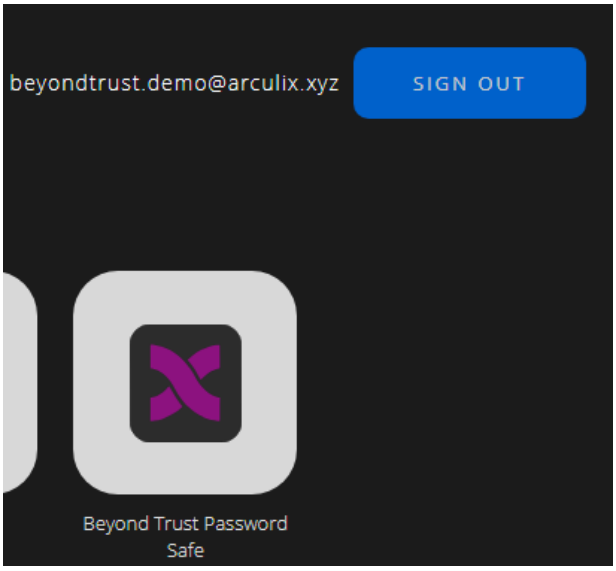
Configure Arculix SAML (IdP-initiated) Integration

1. Create an application. Use a recognizable name, for example BeyondTrust Password Safe.
2. Set type to **SAML Service Provider**.
3. Check the **IdP Initiated** box.
4. From the **Name Identifier** menu, select **Email**.
5. For **Issuer or Entity ID**, use the generated Entity ID from the SAML configuration in Password Safe, under the **Service Provider Settings** section.
6. For ACS URL, use the generated **Assertion Consumer Service** URL from the SAML configuration in Password Safe, under the **Service Provider Settings** section.
7. Include the following assertion attributes:
   - Name: for example, beyondtrust.demo@arculix.xyz
   - EmailAddress
   - GivenName
   - Surname
   - Group: This needs to correspond to a group name in Password Safe. The group can be Local, Active Directory (DN, UPN, SID), etc. See Password Safe SAML documentation link above for more information on group mapping types.
8. Download the SAML certificate for your organization.
9. Assign the new application to a test user.

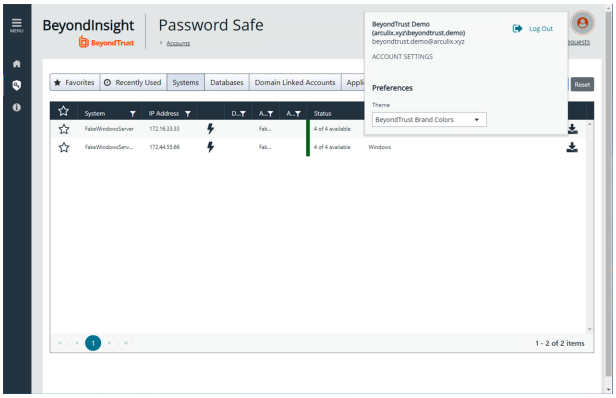


Test the Logon from the Arculix Portal

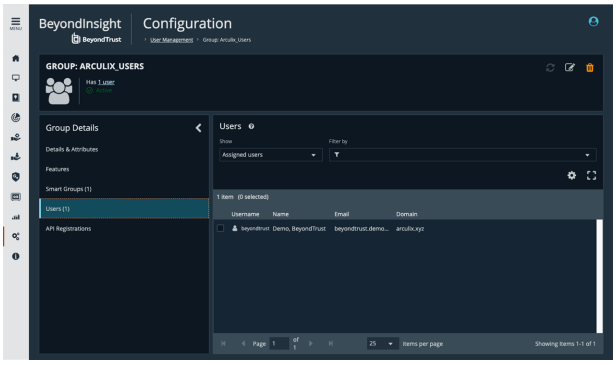
After you complete all the steps listed above, click the Password Safe app in the Arculix portal for the test user and leverage single sign-on to authenticate to Password Safe.



The test user should have access to the assigned Smart Groups of Privileged Accounts.



After the first authentication, the test user is added as a member to the Password Safe group.



For more information about this integration or to send feedback, please email integrations@beyondtrust.com