BeyondTrust

Password Safe and Microsoft Entra ID Provision and Set up Single Sign-On

TC:4/10/2024

Provision and Set up Single Sign-On

There are three parts to configuring single sign-on between Password Safe and Microsoft Entra ID (formerly Microsoft Azure AD):

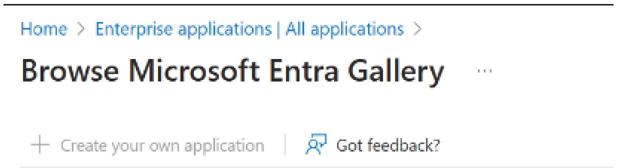
- Create an Enterprise Application for Password Safe
- Configure Authentication and Authorization
- Configure Single Sign-On using Entra ID SAML Identity Provider

Create an Enterprise Application for Password Safe

You can use this document as an alternative to this section: https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/authentication/groups/entra-id.htm

To create an application in Entra ID:

1. From **Enterprise applications**, create an application, and then select **Create your own application**.

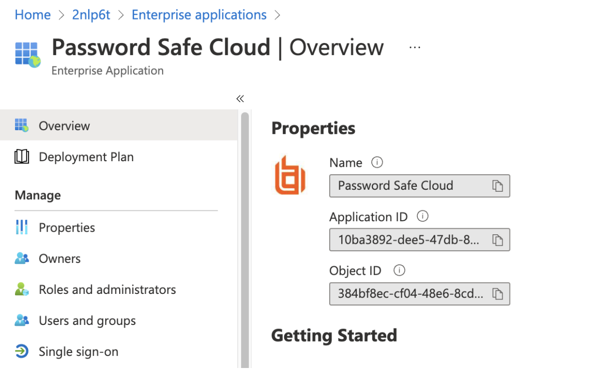


Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery ...

2. Provide a name for the application, and select the **Non-gallery** option.

3. Once the application is created, on the **Properties** page, assign a logo.



Home > 2nlp6t > Enterprise applications >

Password Safe Cloud | Overview ...

Enterprise Application

Properties

Name: Password Safe Cloud

Application ID: 10ba3892-dee5-47db-8...

Object ID: 384bf8ec-cf04-48e6-8cd...

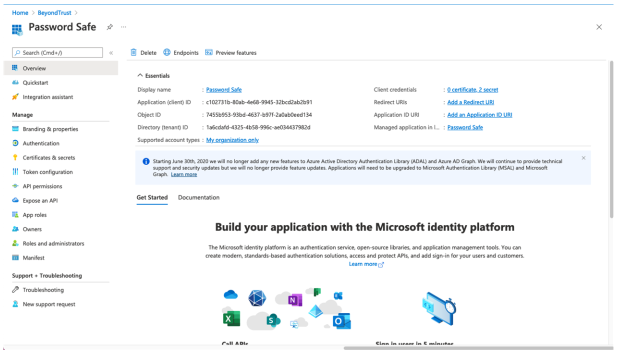
Getting Started

Configure Authentication and Authorization

To configure authentication and authorization:

1. Configure a service account for the Entra ID instance.
2. Create an app registration for your application.

3. Note the **Application (client) ID** and **Directory (tenant) ID**. You will copy these values later in Password Safe during the SAML configuration.



Essentials

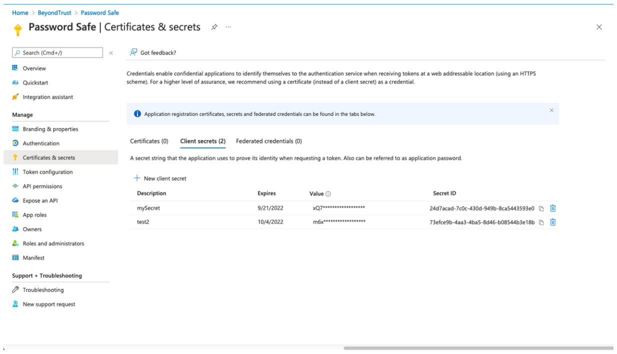
Display name	: Password Safe	Client credentials	: 0 certificate, 2 secret
Application (client) ID	: c102731b-80ab-4e68-9945-32bcd2ab2b91	Redirect URIs	: Add a Redirect URI
Object ID	: 7455b953-93bd-4637-b97f-2a0ab0eed134	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 1a6cdafd-4325-4b58-996c-ae034437982d	Managed application in l...	: Password Safe
Supported account types	: My organization only		

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

4. On the **Certificates & secrets** page, under the application registration, create a client secret. Take note of the **Value** (client secret).



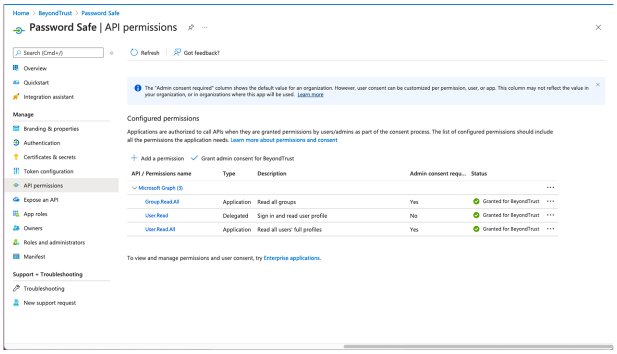
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
mySecret	9/21/2022	xQ7******************	24d7acad-7c0c-430d-949b-8ca5443593e0
test2	10/4/2022	m6x******************	73efce9b-4aa3-4ba5-8d46-b08544b3e18b

5. Add API permissions to application registration.



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

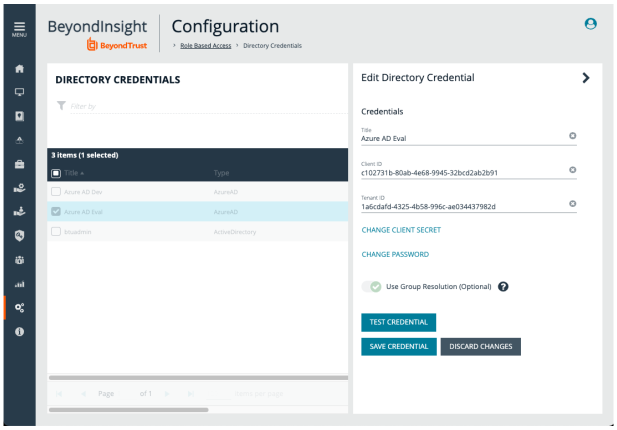
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
Group.Read.All	Application	Read all groups	Yes	✓ Granted for BeyondTrust
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for BeyondTrust
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for BeyondTrust

To view and manage permissions and user consent, try Enterprise applications.

6. After a service account is created, store the credentials in a Directory Credential object in Password Safe. Use the client and tenant IDs, and the client secret.



3 items (1 selected)

Title	Type
☐ Azure AD Dev	AzureAD
☑ Azure AD Eval	AzureAD
☐ btuadmin	ActiveDirectory

Credentials

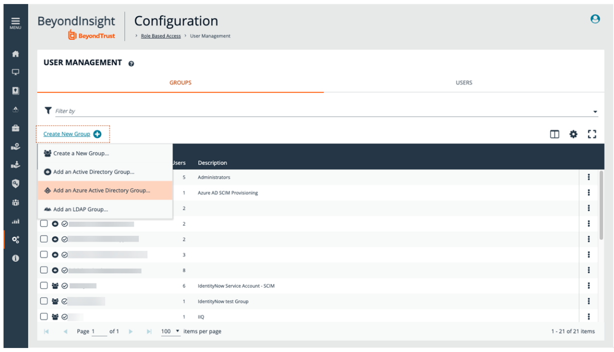
Title: Azure AD Eval

Client ID: c102731b-80ab-4e68-9945-32bcd2ab2b91

Tenant ID: 1a6cdafd-4325-4b58-996c-ae034437982d

✓ Use Group Resolution (Optional)

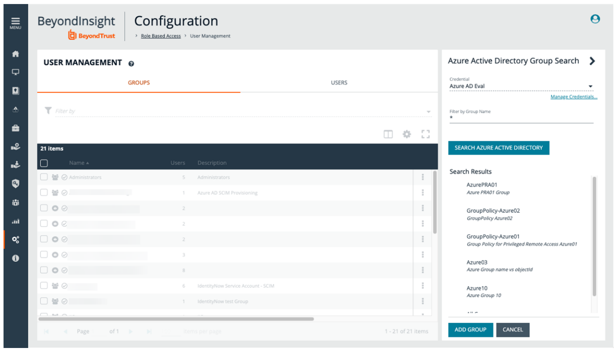
7. At this point, test the credential. Under **User Management**, create an Entra ID group.



Name	Users	Description
	5	Administrators
	1	Azure AD SCIM Provisioning
	2	
[redacted]	2	
[redacted]	2	
[redacted]	3	
[redacted]	8	
[redacted]	6	IdentityNow Service Account - SCIM
[redacted]	1	IdentityNow test Group
[redacted]	1	IIQ

Page 1 of 1 100 items per page 1 - 21 of 21 items

8. With the previously created directory credential, browse and import Entra ID groups.



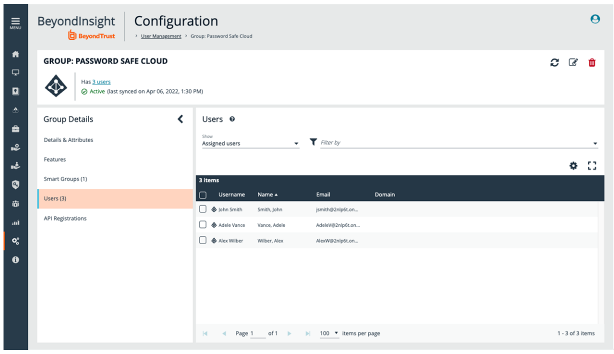
Credential: Azure AD Eval

Filter by Group Name: *

Search Results

- AzurePRA01 — *Azure PRA01 Group*
- GroupPolicy-Azure02 — *GroupPolicy Azure02*
- GroupPolicy-Azure01 — *Group Policy for Privileged Remote Access Azure01*
- Azure03 — *Azure Group name vs objectId*
- Azure10 — *Azure Group 10*

9. Members in Entra ID and Password Safe are synchronized. Adding a new member to the group in Entra ID creates a new account in Password Safe with the permissions associated to the provisioning group.



GROUP: PASSWORD SAFE CLOUD

Has 3 users
Active (last synced on Apr 06, 2022, 1:30 PM)

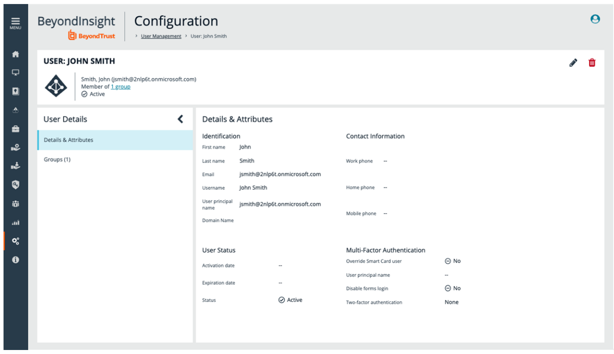
Show: Assigned users

3 items

Username	Name	Email	Domain
John Smith	Smith, John	jsmith@2nlp6t.on...	
Adele Vance	Vance, Adele	AdeleV@2nlp6t.on...	
Alex Wilber	Wilber, Alex	AlexW@2nlp6t.on...	

Page 1 of 1 100 items per page 1 - 3 of 3 items

10. The screen capture shows a new account provisioned in Password Safe when an Entra ID user is added to Entra ID group after the group is imported.



USER: JOHN SMITH

Smith, John (jsmith@2nlp6t.onmicrosoft.com)
Member of 1 group
Active

Details & Attributes

Identification

First name	John
Last name	Smith
Email	jsmith@2nlp6t.onmicrosoft.com
Username	John Smith
User principal name	jsmith@2nlp6t.onmicrosoft.com
Domain Name	

Contact Information

Work phone	--
Home phone	--
Mobile phone	--

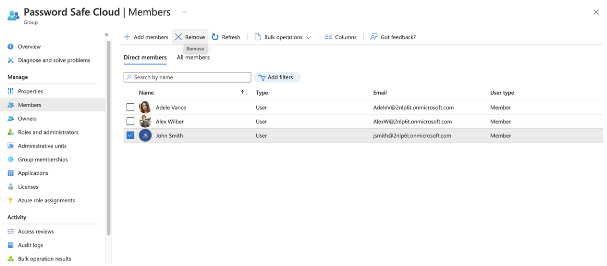
User Status

Activation date	--
Expiration date	--
Status	Active

Multi-Factor Authentication

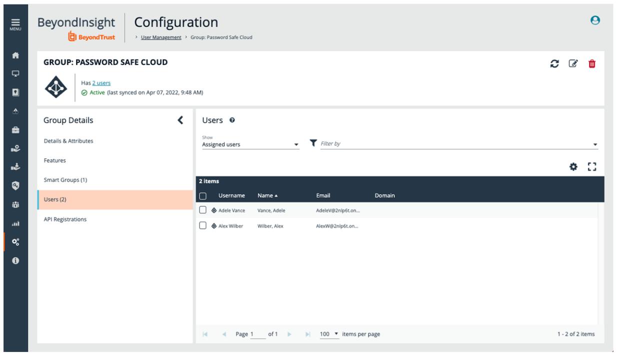
Override Smart Card user	No
User principal name	--
Disable forms login	No
Two-factor authentication	None

11. Adding and removing members in Entra ID results in provisioning or deprovisioning of access in Password Safe.



	Name	Type	Email	User type
☐	Adele Vance	User	AdeleV@2nlp6t.onmicrosoft.com	Member
☐	Alex Wilber	User	AlexW@2nlp6t.onmicrosoft.com	Member
☑	JS John Smith	User	jsmith@2nlp6t.onmicrosoft.com	Member

12. After scheduled or manual synchronization, the removed member is removed from the group.



GROUP: PASSWORD SAFE CLOUD

Has 2 users
Active (last synced on Apr 07, 2022, 9:48 AM)

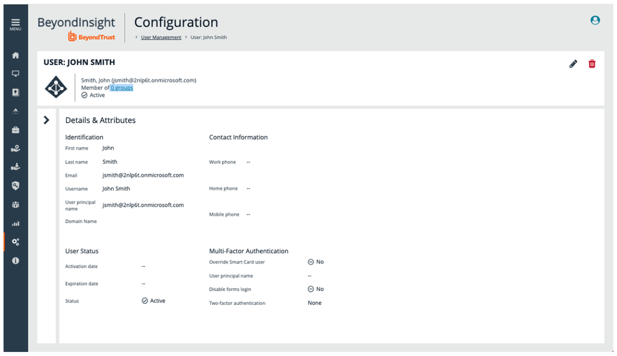
Show: Assigned users

2 items

☐	Username	Name ▲	Email	Domain
☐	Adele Vance	Vance, Adele	AdeleV@2nlp6t.on...	
☐	Alex Wilber	Wilber, Alex	AlexW@2nlp6t.on...	

Page 1 of 1 100 items per page 1 - 2 of 2 items

13. The account remains in Password Safe, but the removed user cannot access their account and cannot start a Password Safe session.



USER: JOHN SMITH

Smith, John (jsmith@2nlp6t.onmicrosoft.com)
Member of 0 groups
Active

Identification

First name John
Last name Smith
Email jsmith@2nlp6t.onmicrosoft.com
Username John Smith
User principal name jsmith@2nlp6t.onmicrosoft.com
Domain Name

Contact Information

Work phone --
Home phone --
Mobile phone --

User Status

Activation date --
Expiration date --
Status Active

Multi-Factor Authentication

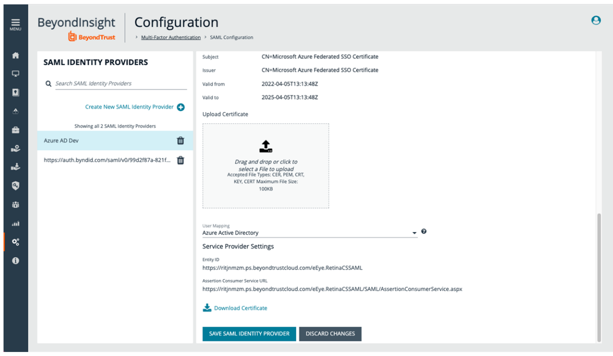
Override Smart Card user No
User principal name --
Disable forms login No
Two-factor authentication None

Note: *Entra ID group memberships for a user are synchronized every time the user logs in. For example, a user that has been removed from all Groups can no longer log in to Password Safe.*

Configure Single Sign-On Using Entra ID SAML Identity Provider

Now go to the application created for Password Safe in Entra ID, under **Enterprise applications**. You must configure SAML in Password Safe, and the corresponding single sign-on configuration in the Entra ID application.

1. The screen capture shows SAML configuration in Password Safe (BeyondInsight). Take note of **Entity ID** and **Assertion Consumer Service URL**.
2. Set **User Mapping** to Entra ID.


MENU
BeyondInsight
BeyondTrust
Configuration
Multi-Factor Authentication
SAML Configuration
SAML IDENTITY PROVIDERS
Search SAML Identity Providers
Create New SAML Identity Provider
Showing all 2 SAML Identity Providers
Upload Certificate
Drag and drop or click to select a File to upload
Accepted File Types: CER, PEM, CRT, KEY, CERT Maximum File Size: 100KB
Download Certificate
SAVE SAML IDENTITY PROVIDER
DISCARD CHANGES

Azure AD Dev

https://auth.byndid.com/saml/v0/99d2f87a-821f...

Subject	CN=Microsoft Azure Federated SSO Certificate
Issuer	CN=Microsoft Azure Federated SSO Certificate
Valid from	2022-04-05T13:13:48Z
Valid to	2025-04-05T13:13:48Z

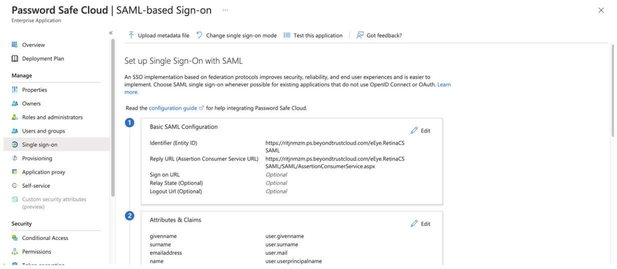
User Mapping: Azure Active Directory

Service Provider Settings

Entity ID: https://ritjnmzm.ps.beyondtrustcloud.com/eEye.RetinaCSSAML

Assertion Consumer Service URL: https://ritjnmzm.ps.beyondtrustcloud.com/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx

3. The screen capture shows single sign-on configuration for Entra ID App. Enter the Password Safe **Entity ID** and **Assertion Consumer Service URL**.



Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Password Safe Cloud.

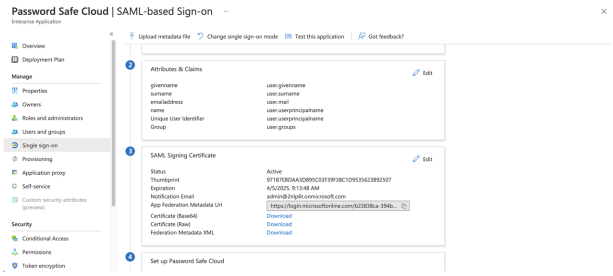
1 Basic SAML Configuration

Identifier (Entity ID)	https://ritjnmzm.ps.beyondtrustcloud.com/eEye.RetinaCSSAML
Reply URL (Assertion Consumer Service URL)	https://ritjnmzm.ps.beyondtrustcloud.com/eEye.RetinaCSSAML/SAML/AssertionConsumerService.aspx
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname

4. Add the group (**user.groups**) to **Attributes**.
5. Download **Certificate (Base64)** to import in Password Safe SAML configuration.



2 Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups

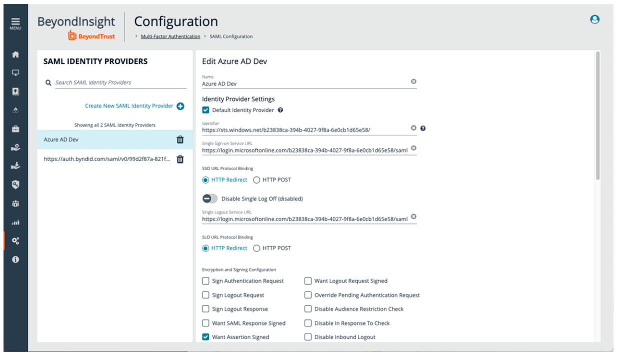
3 SAML Signing Certificate

Status	Active
Thumbprint	971B7EBDAA3D895C03F39F38C1D9535623B92507
Expiration	4/5/2025, 9:13:48 AM
Notification Email	admin@2nlp6t.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/b23838ca-394b...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Password Safe Cloud

6. Take note of the **Login URL**, **Entra ID Identifier**, and **Logout URL**.

7. Complete the configuration in Password Safe by entering the **Identifier** (Entra ID Identifier), **Single Sign-On Service URL**(login URL) and **Single Logout Service URL** (logout URL).


MENU
BeyondInsight
BeyondTrust
Configuration
Multi-Factor Authentication
SAML Configuration
SAML IDENTITY PROVIDERS
Search SAML Identity Providers
Create New SAML Identity Provider
Showing all 2 SAML Identity Providers

Azure AD Dev

https://auth.byndid.com/saml/v0/99d2f87a-821f...

Edit Azure AD Dev

Name: Azure AD Dev

Identity Provider Settings

☑ Default Identity Provider

Identifier: https://sts.windows.net/b23838ca-394b-4027-9f8a-6e0cb1d65e58/

Single Sign-on Service URL: https://login.microsoftonline.com/b23838ca-394b-4027-9f8a-6e0cb1d65e58/saml

SSO URL Protocol Binding: ● HTTP Redirect ○ HTTP POST

Disable Single Log Off (disabled)

Single Logout Service URL: https://login.microsoftonline.com/b23838ca-394b-4027-9f8a-6e0cb1d65e58/saml

SLO URL Protocol Binding: ● HTTP Redirect ○ HTTP POST

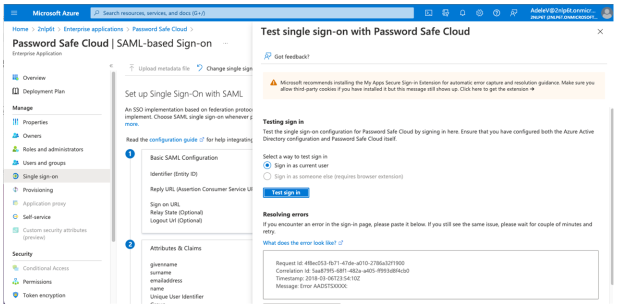
Encryption and Signing Configuration

☐ Sign Authentication Request	☐ Want Logout Request Signed
☐ Sign Logout Request	☐ Override Pending Authentication Request
☐ Sign Logout Response	☐ Disable Audience Restriction Check
☐ Want SAML Response Signed	☐ Disable In Response To Check
☑ Want Assertion Signed	☐ Disable Inbound Logout

Test SSO

To test SSO with a test user:

1. Log in as a test user and access the **Enterprise applications**.
2. Click **Test sign in** to open a new browser tab for Password Safe. SAML assertion is sent to authenticate the user.



An SSO implementation based on federation protoc implement. Choose SAML single sign-on whenever p more.

Read the configuration guide for help integrating

Test single sign-on with Password Safe Cloud

Microsoft recommends installing the My Apps Secure Sign-in Extension for automatic error capture and resolution guidance. Make sure you allow third-party cookies if you have installed it but this message still shows up. Click here to get the extension →

Testing sign in

Test the single sign-on configuration for Password Safe Cloud by signing in here. Ensure that you have configured both the Azure Active Directory configuration and Password Safe Cloud itself.

Select a way to test sign in

● Sign in as current user

○ Sign in as someone else (requires browser extension)

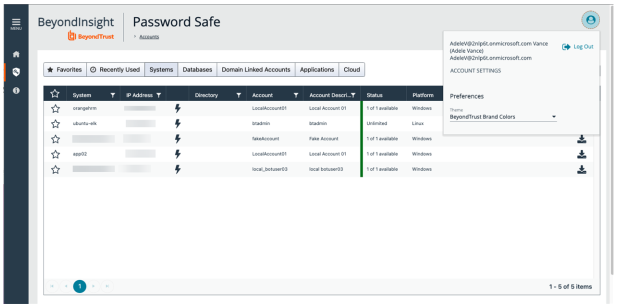
Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

What does the error look like?

```
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: 5aa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX:
```

3. The test user is authenticated (SSO) in Password Safe.



AdeleV@2nlp6t.onmicrosoft.com Vance (Adele Vance)
AdeleV@2nlp6t.onmicrosoft.com

Theme: BeyondTrust Brand Colors

☆	System	IP Address		Directory	Account	Account Descri...	Status	Platform
☆	orangehrm	[redacted]	⚡		LocalAccount01	Local Account 01	1 of 1 available	Windows
☆	ubuntu-elk	[redacted]	⚡		btadmin	btadmin	Unlimited	Linux
☆	[redacted]	[redacted]	⚡		fakeAccount	Fake Account	1 of 1 available	Windows
☆	app02	[redacted]	⚡		LocalAccount01	Local Account 01	1 of 1 available	Windows
☆	[redacted]	[redacted]	⚡		local_botuser03	local botuser03	1 of 1 available	Windows

1 - 5 of 5 items

This completes the configuration of provisioning and SSO between Entra ID and BeyondTrust Password Safe and Password Safe Cloud.

> *For more information or to send comments, please send to integrations@beyondtrust.com*