Overview: Brainshark uses basic SAML which has the ability to create an account upon login and set identified variables (If autocreate is enabled in Brainshark) . Once the account is created, any future updates in Azure do NOT update the user in Brainshark. Microsoft doesn't natively support sending a claim with the Manager of the user.

Access link to STAGING: https://staging.brainshark.com/CompanyName

Access link to PROD: https://www.brainshark.com/CompanyName

Steps to Enable Basic SAML in Microsoft Entra: https://entra.microsoft.com

1. Add the Application:
   - Log in to the Microsoft Entra admin center as a Cloud Application Administrator.
   - Navigate to Identity > Applications > Enterprise applications > All applications.
   - Click New application.
   - Select Non-gallery application.
   - Enter a name for the application "Brainshark" and click Add.
2. Configure Single Sign-On:
   - Select the newly added application.
   - In the Manage section, select Single sign-on.
   - Choose SAML.
3. Edit Basic SAML Configuration:
   - Click the Edit button under Basic SAML Configuration.
   - Fill in the required fields:
     - **Staging Environment**
       - Identifier (Entity ID): https://staging.brainshark.com/brainshark/brainshark.services.auth/

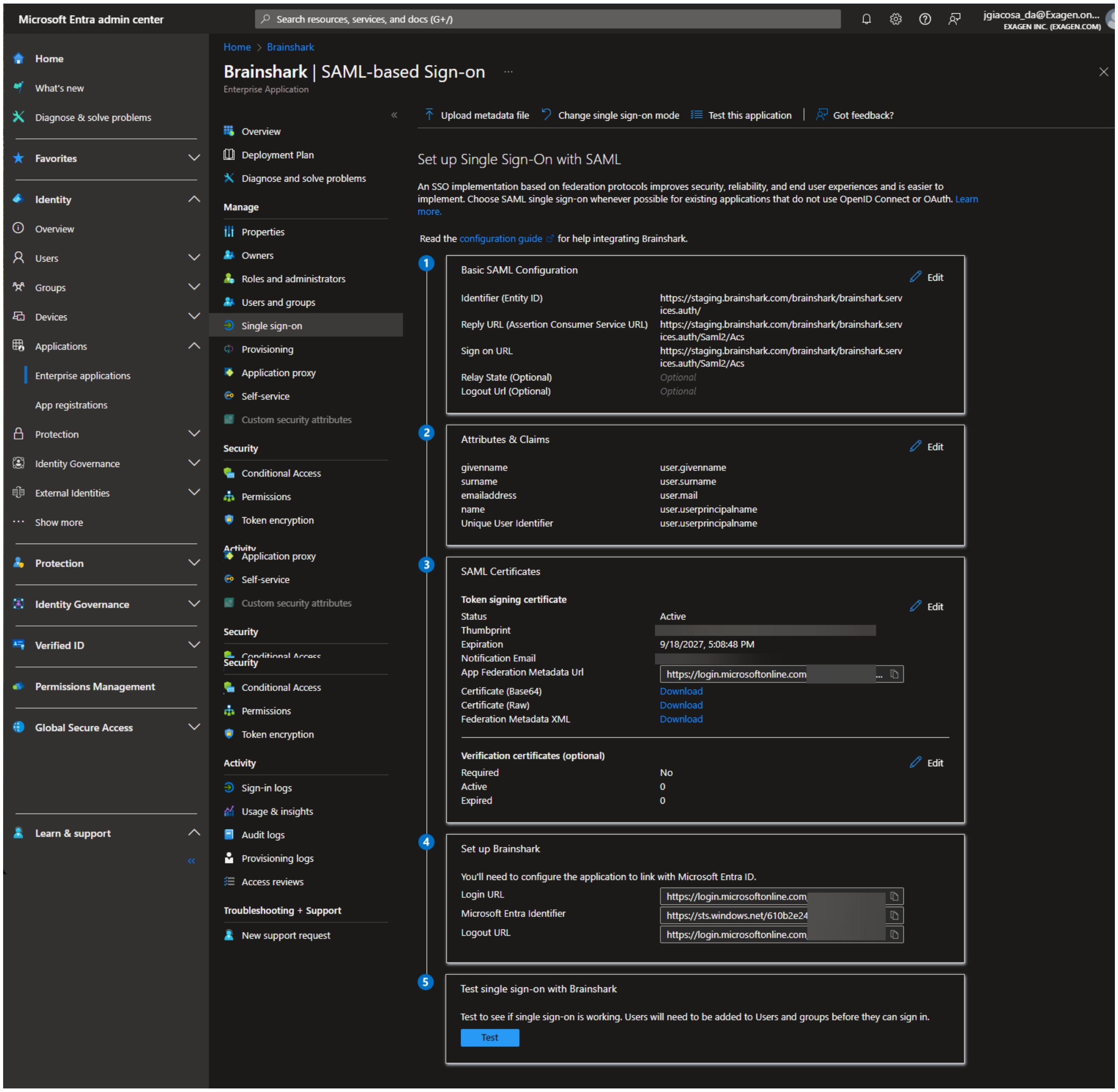
        - Reply URL (Assertion Consumer Service URL): https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
        - Sign on URL: https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
    - **<u>Production Environment</u>**
        - Identifier (Entity ID): https://www.brainshark.com/brainshark/brainshark.services.auth/
        - Reply URL (Assertion Consumer Service URL): https://www.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
        - Sign on URL: https://www.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs

1. Download Federation Metadata XML:
    - Under SAML Certificates
    - Verify the Notification Email is set to "UserID@Domain.com"
    - click Download for Federation Metadata XML.
    - Save this file for later use.
2. Configure the Application:
    - These Steps are performed by Brainshark support team

Additional Considerations:

- **Attribute Mappings:** If necessary, Brainshark can configure attribute mappings to map attributes from Microsoft Entra to Brainshark attributes.
- **Signing Certificates:** You may need to upload the Brainshark certificate to Microsoft Entra if you are requiring the Authn request to be signed. Brainshark always requires that the SAML responses are signed.

- **Testing:** After configuring SAML, test the integration to ensure it's working correctly.



Brainshark | SAML-based Sign-on

Enterprise Application

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 Brainshark.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	https://staging.brainshark.com/brainshark/brainshark.services.auth/
Reply URL (Assertion Consumer Service URL)	https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
Sign on URL	https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims — Edit

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

3 SAML Certificates

Token signing certificate — Edit

Status	Active
Thumbprint	[redacted]
Expiration	9/18/2027, 5:08:48 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com[redacted]...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) — Edit

Required	No
Active	0
Expired	0

4 Set up Brainshark

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	https://login.microsoftonline.com[redacted]
Microsoft Entra Identifier	https://sts.windows.net/610b2e24
Logout URL	https://login.microsoftonline.com

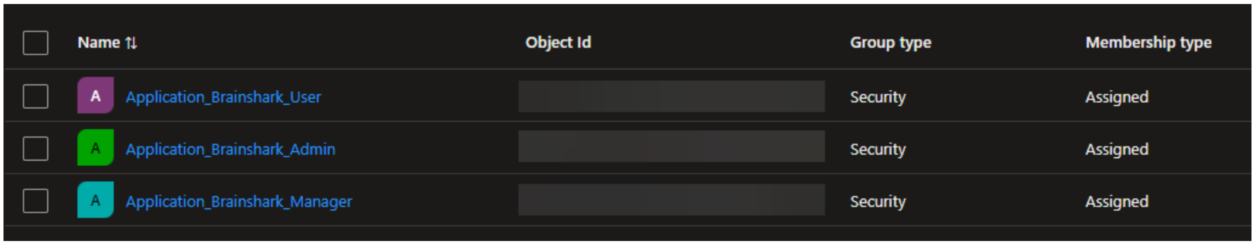
5 Test single sign-on with Brainshark

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

Test

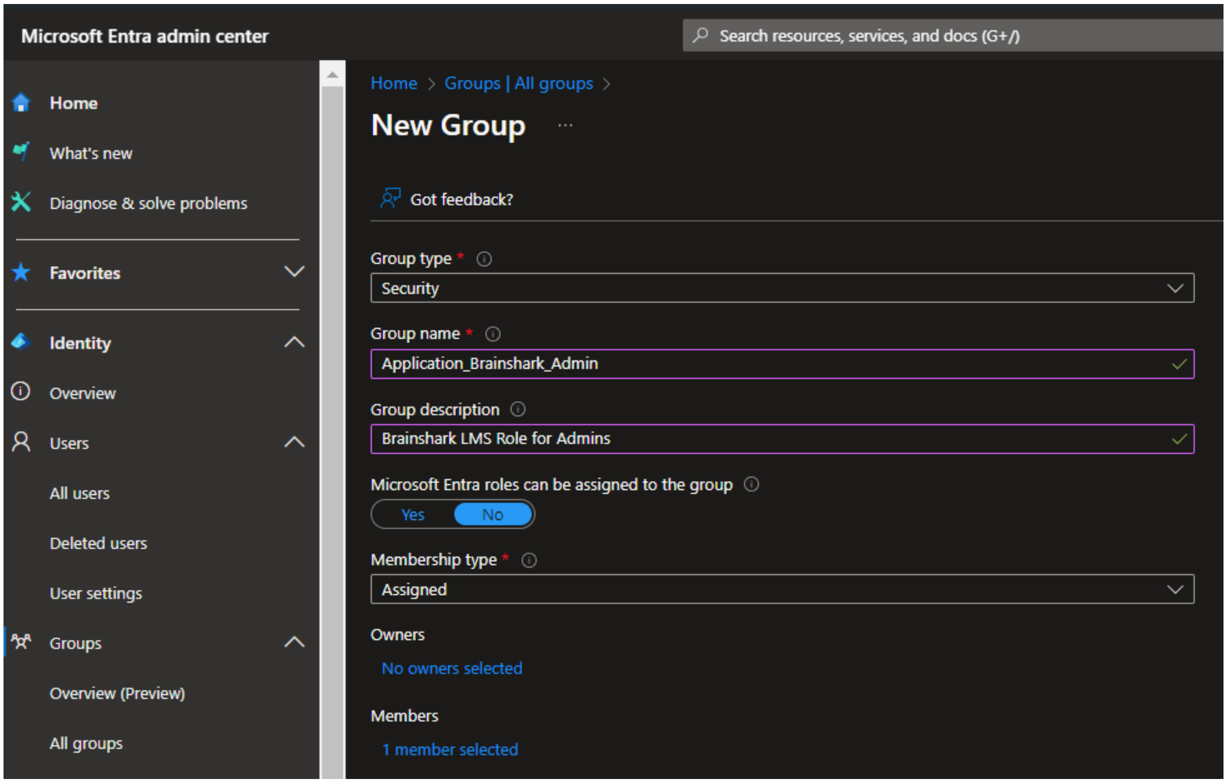
Create Entra Security Groups

Azure/Entra Security Group	Brainshark Role	Object ID
Application_Brainshark_Admin	Admin	
Application_Brainshark_Manager	Manager	
Application_Brainshark_User	User	



□	Name ⇅	Object Id	Group type	Membership type
□	A Application_Brainshark_User	[redacted]	Security	Assigned
□	A Application_Brainshark_Admin	[redacted]	Security	Assigned
□	A Application_Brainshark_Manager	[redacted]	Security	Assigned

- **For Testing - Assigned "User 1"**



Group type * : Security

Group name * : Application_Brainshark_Admin

Group description : Brainshark LMS Role for Admins

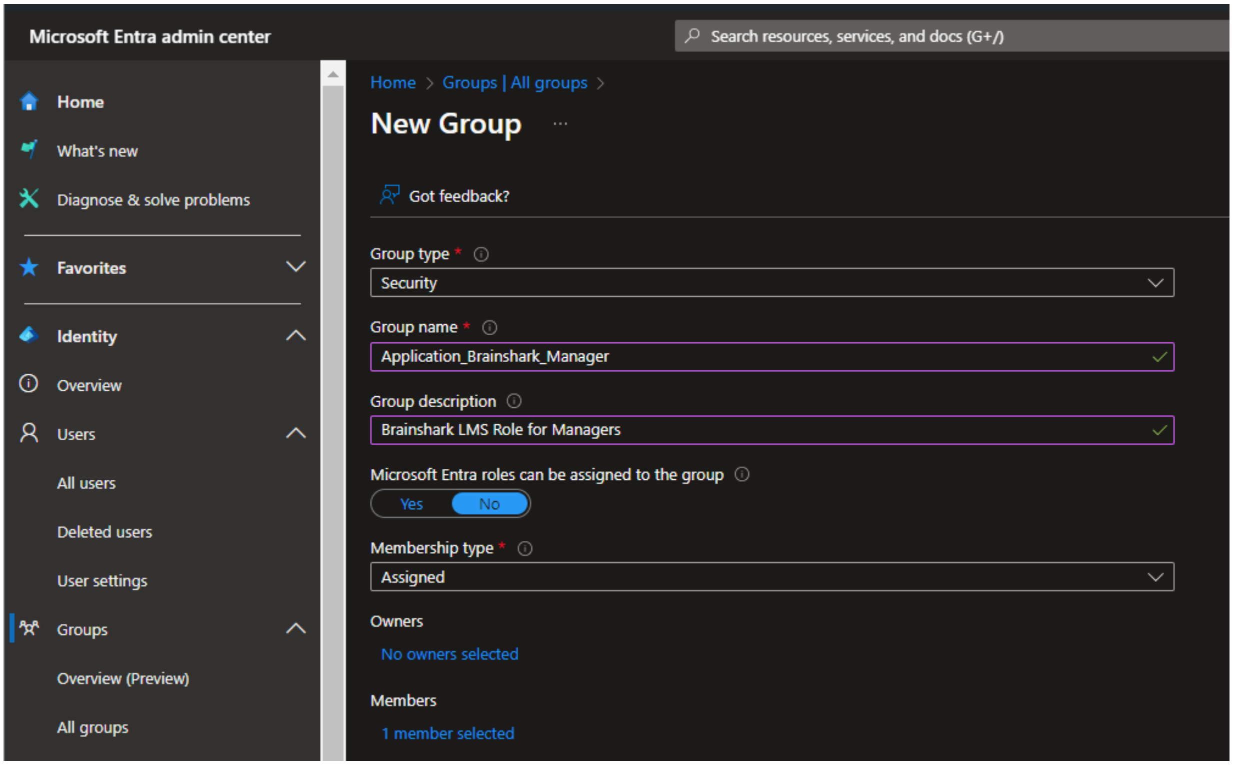
Microsoft Entra roles can be assigned to the group : Yes [✓ No]

Membership type * : Assigned

Owners : No owners selected

Members : 1 member selected

- **For Testing - Assigned "User 2"**



New Group

Group type * : Security

Group name * : Application_Brainshark_Manager

Group description : Brainshark LMS Role for Managers

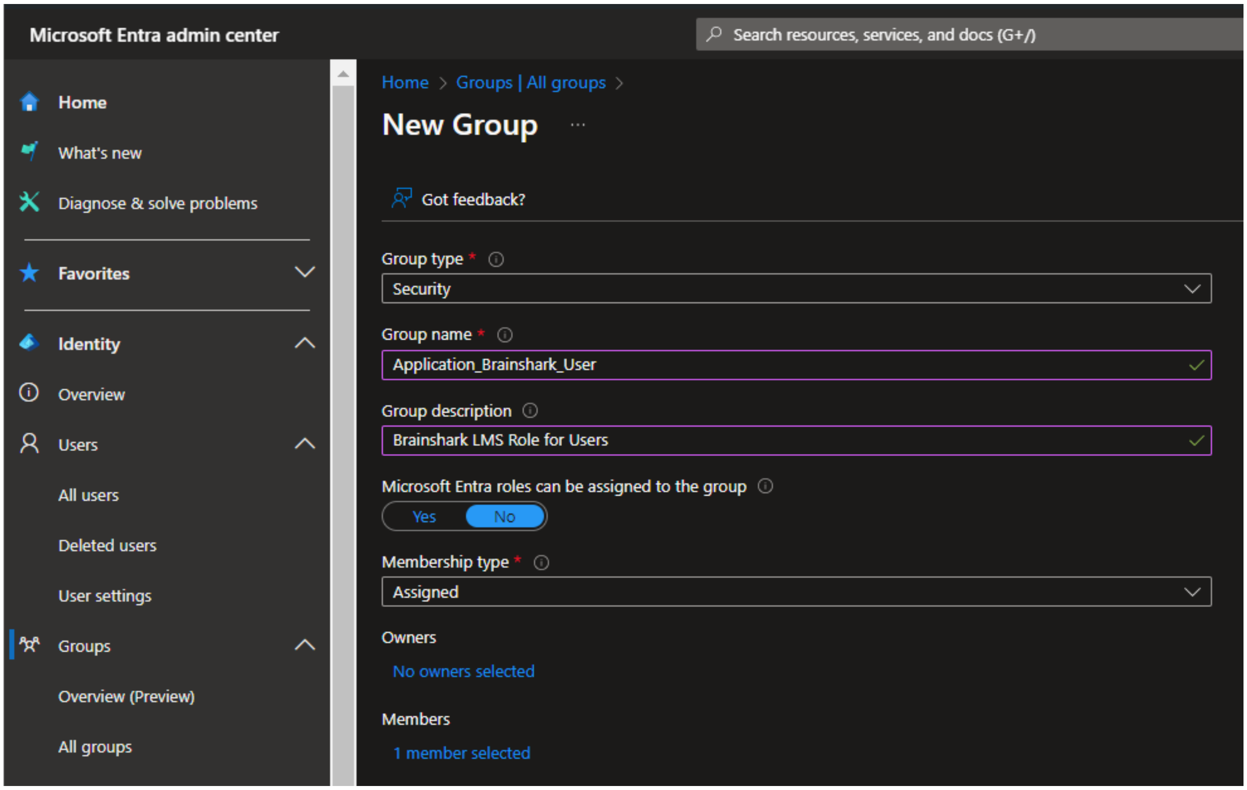
Microsoft Entra roles can be assigned to the group: Yes [✓ No]

Membership type * : Assigned

Owners: No owners selected

Members: 1 member selected

- **For Testing - Assigned "User 3"**



New Group ···

Group type * Security

Group name * Application_Brainshark_User

Group description Brainshark LMS Role for Users

Microsoft Entra roles can be assigned to the group Yes [✓ No]

Membership type * Assigned

Owners

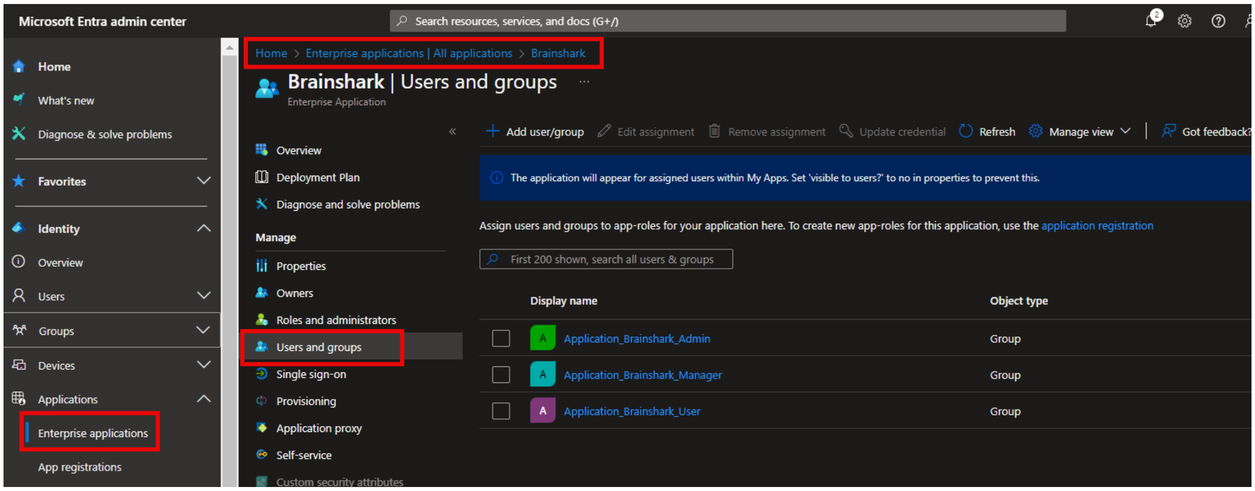
No owners selected

Members

1 member selected

Add the Groups to the Brainshark Enterprise Application

- Navigate to Enterprise Application | Brainshark | Users and Groups
- Select Add user/group
- Select appropriate Groups



The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the application registration

	Display name	Object type
□	Application_Brainshark_Admin	Group
□	Application_Brainshark_Manager	Group
□	Application_Brainshark_User	Group

Attributes & Claims

Microsoft Documentation: Customize SAML token claims - Microsoft identity platform | Microsoft Learn

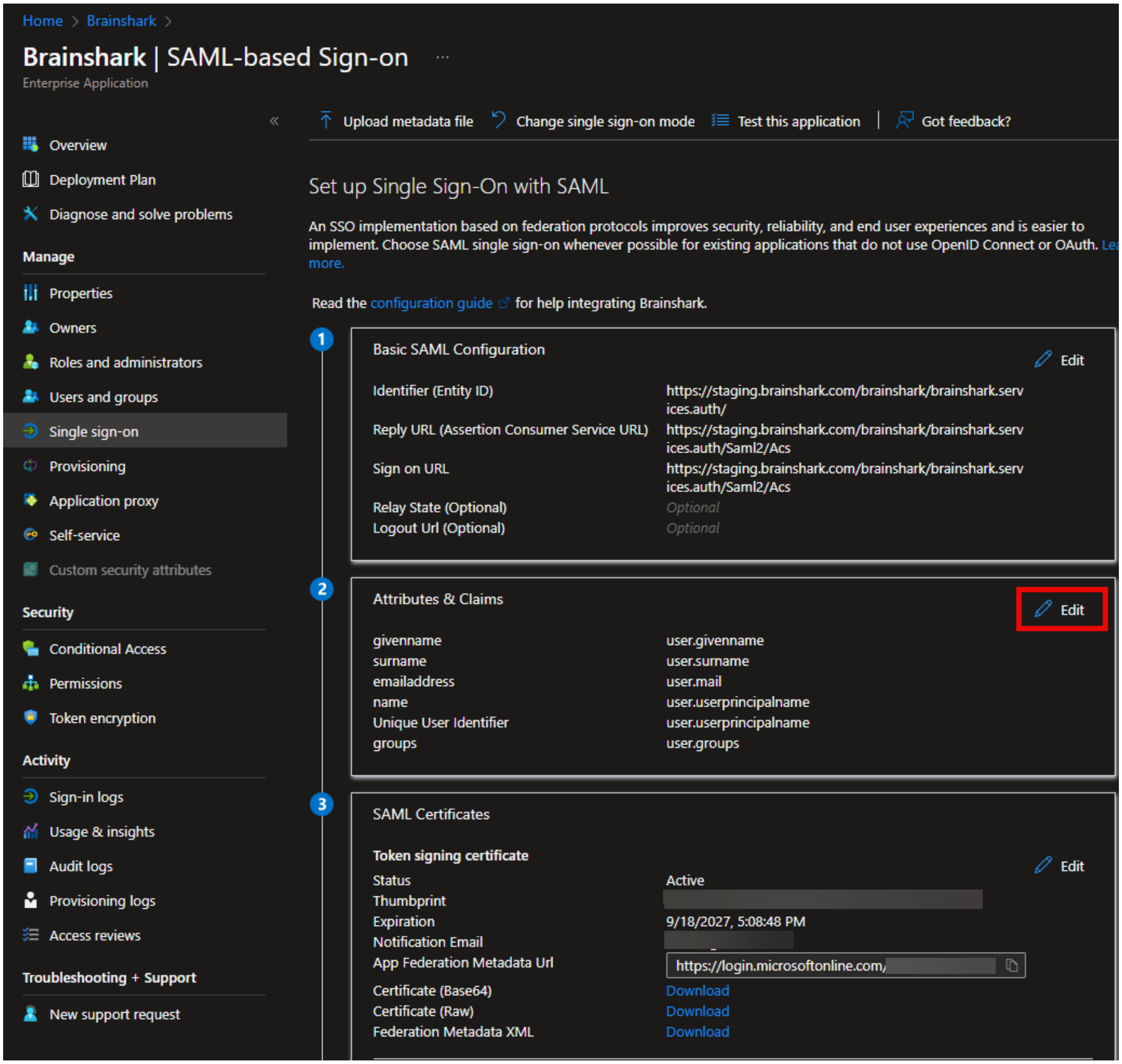
Video: Overview of group assignment and claims in Entra ID | Microsoft

- Claims Mapping Policy 5 minutes in

Add a group claim

Group claims are used to make authorization decisions to access a resource by an app or a service provider. To add group claims;

- Navigate to Enterprise Application | Brainshark | Single sign-on
- Edit "Attributes & Claims"



Home > Brainshark >

Brainshark | SAML-based Sign-on ...

Enterprise Application

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. Lea more.

Read the configuration guide for help integrating Brainshark.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	https://staging.brainshark.com/brainshark/brainshark.services.auth/
Reply URL (Assertion Consumer Service URL)	https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
Sign on URL	https://staging.brainshark.com/brainshark/brainshark.services.auth/Saml2/Acs
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims — Edit

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

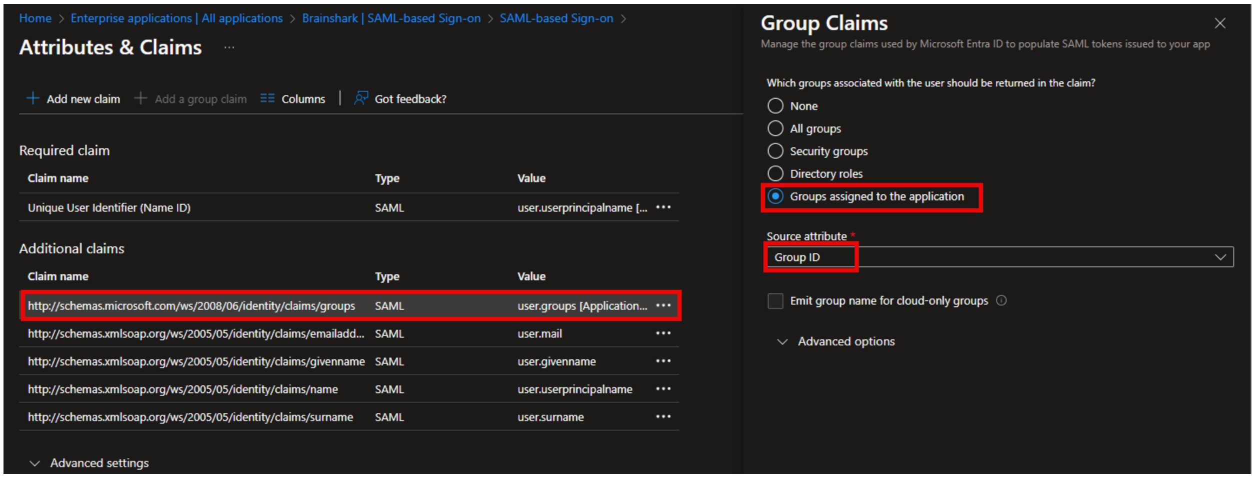
3 SAML Certificates

Token signing certificate — Edit

Status	Active
Thumbprint	[redacted]
Expiration	9/18/2027, 5:08:48 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Add a Group Claim

- Select "Add a group claim"
- Select "Groups assigned to the application"
- Select Attribute: Group ID



Home > Enterprise applications | All applications > Brainshark | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

Add new claim
Add a group claim
Columns
Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [Application...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

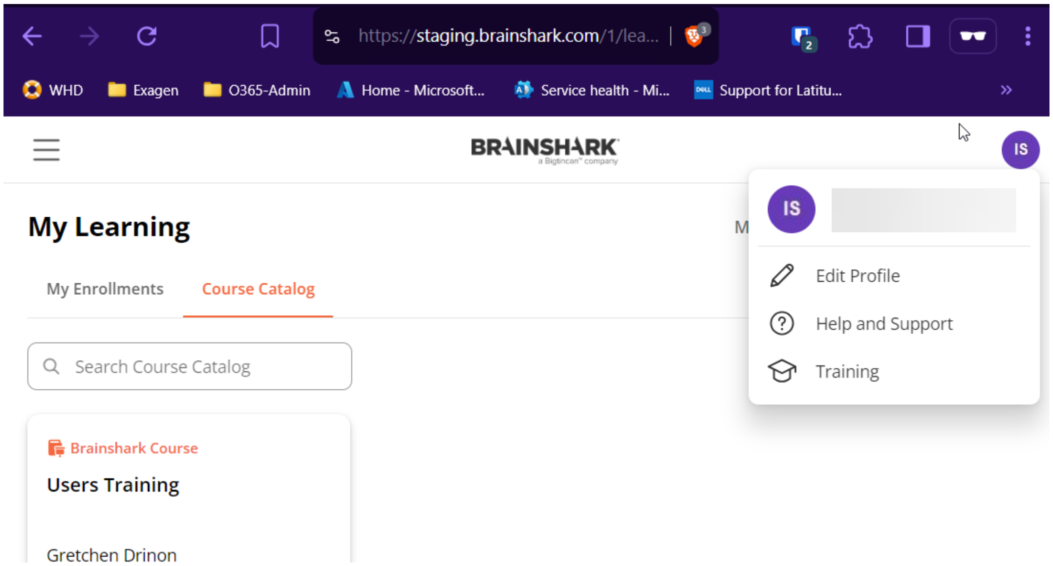
○ None
○ All groups
○ Security groups
○ Directory roles
● Groups assigned to the application

Source attribute *: Group ID

□ Emit group name for cloud-only groups

TEST SUCCESS: https://staging.brainshark.com/CompanyName

Security Group	**User**	**Brainshark Role**	**Connection**
Application_Brainshark_Admin	User 1	Admin	SUCCESS
Application_Brainshark_Manager	User 2	Manager	SUCCESS
Application_Brainshark_User	User 3	User	SUCCESS
NOT ASSIGNED To ABOVE GRP	User 4	N/A	FAIL (Expected)



IS [redacted]

Edit Profile

Help and Support

Training

My Learning

My Enrollments

Course Catalog

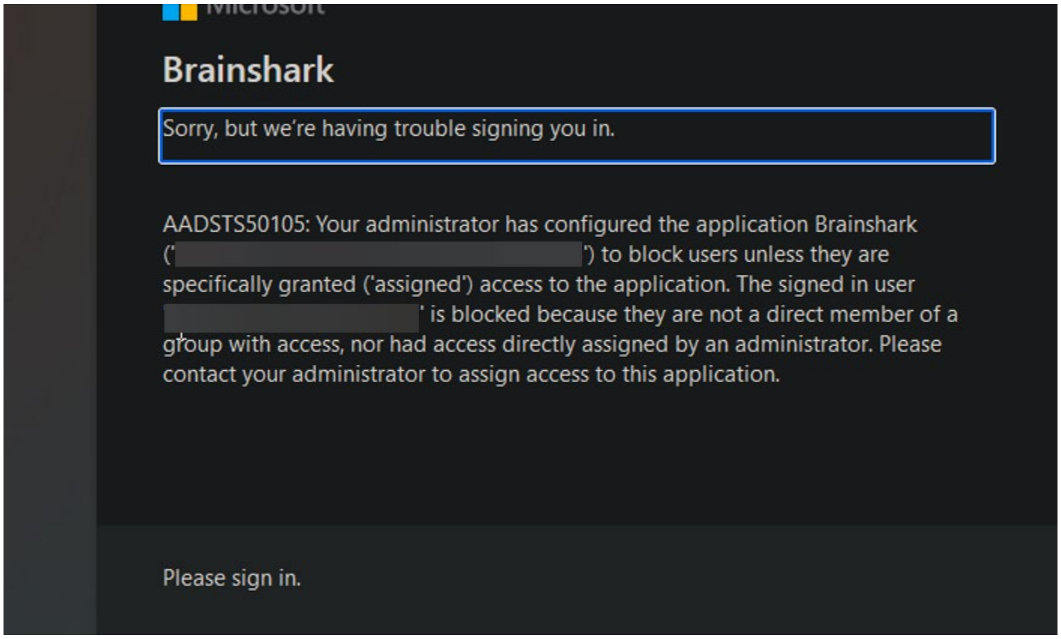
Search Course Catalog

Brainshark Course

Users Training

Gretchen Drinon

Non-Provisioned User = Fail (Expected) this is good



Brainshark

Sorry, but we're having trouble signing you in.

AADSTS50105: Your administrator has configured the application Brainshark ('[redacted]') to block users unless they are specifically granted ('assigned') access to the application. The signed in user [redacted]' is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application.

Please sign in.

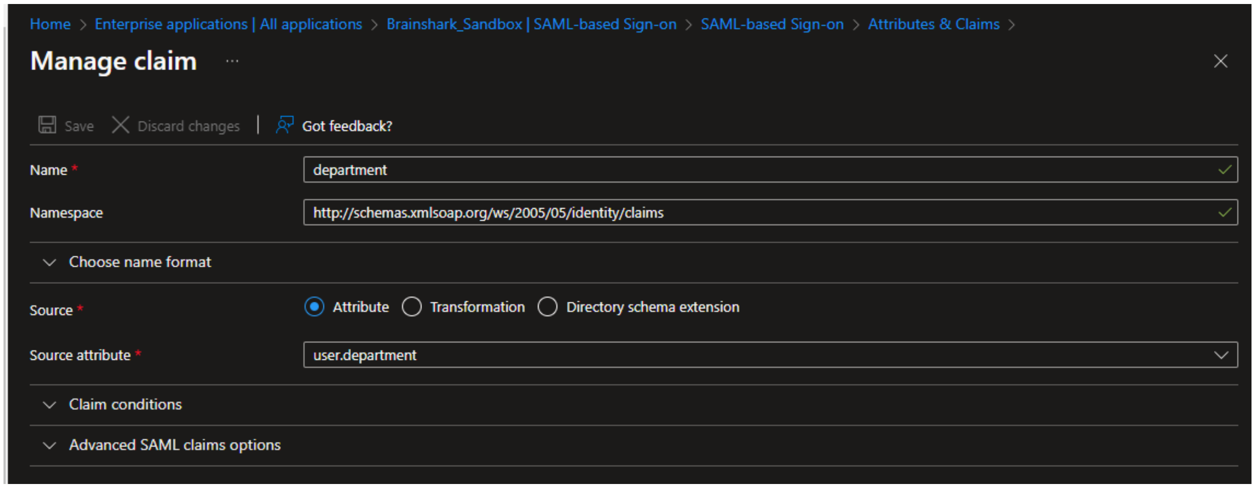
2nd TEST

Security Group	User	Brainshark Role	Connection

Application_Brainshark_Admin	User 1	Admin	ADMIN
Application_Brainshark_Manager	User 2	Manager	MANAGER
Application_Brainshark_User	User 3	User	USER
NOT ASSIGNED To ABOVE GRP	User 4	N/A	N/A

Pass Department and Manager Fields

DEPARTMENT


Home > Enterprise applications | All applications > Brainshark_Sandbox | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >
Manage claim ...
Save
Discard changes
Got feedback?
Choose name format
Claim conditions
Advanced SAML claims options

Name * department

Namespace http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Source * ● Attribute ○ Transformation ○ Directory schema extension

Source attribute * user.department