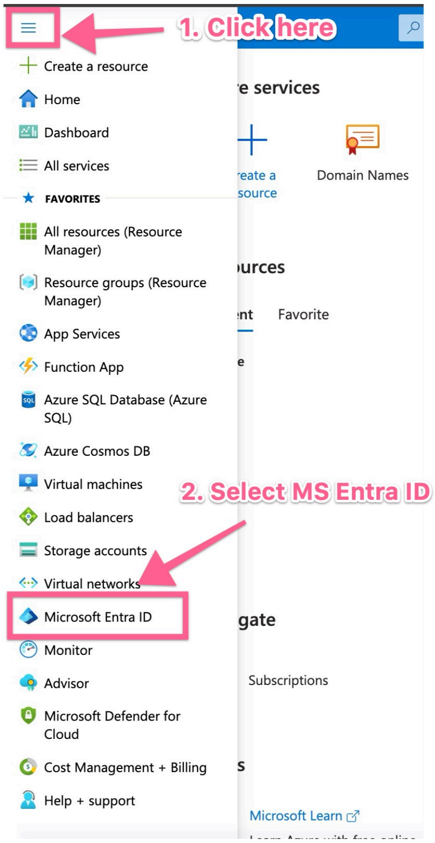
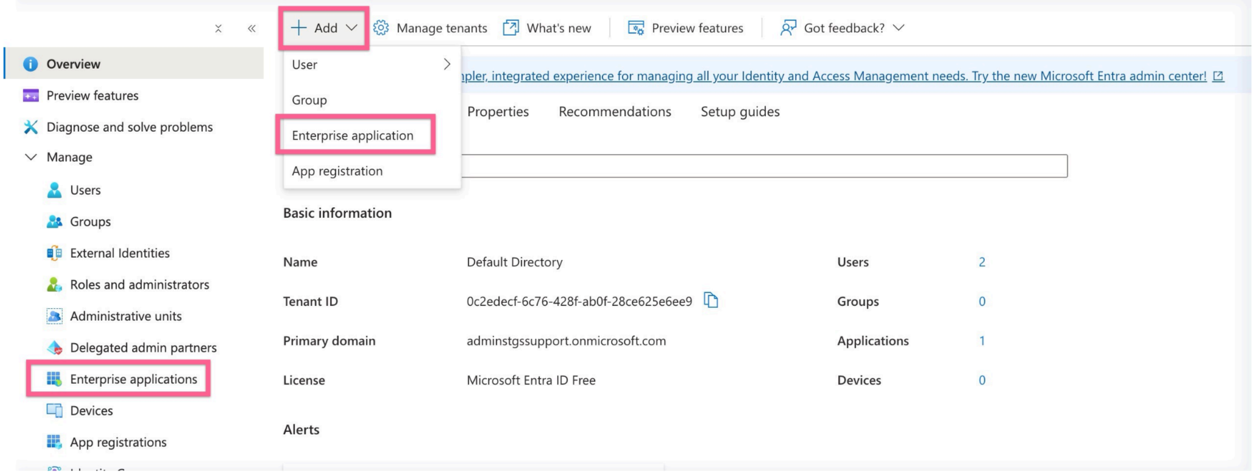
Azure SAML Configuration in Gainsight

Azure Steps:

1. Create a new enterprise application by following the below steps.



2. Select Enterprise application, click on “Add” and select “Enterprise application”

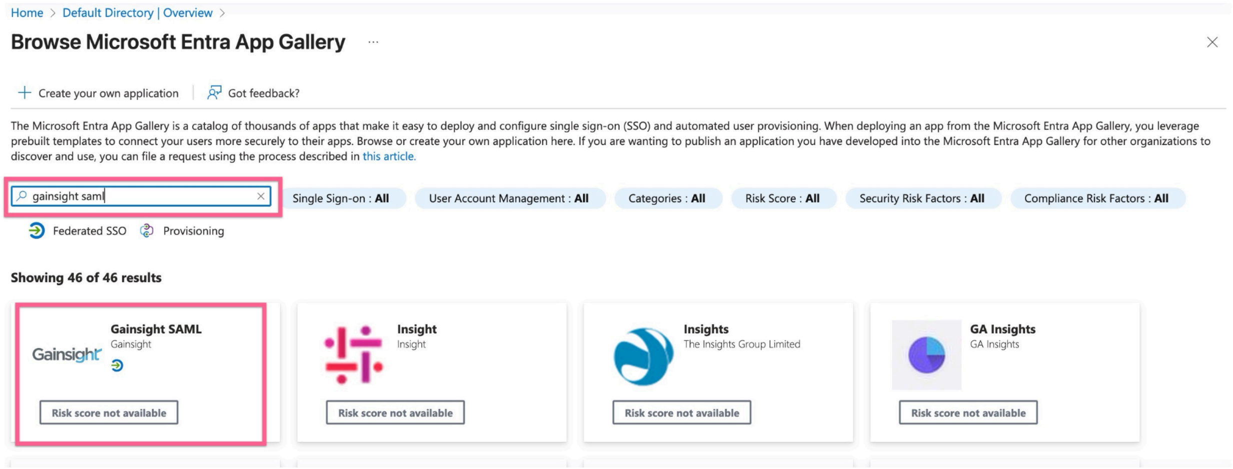


Basic information

Name	Default Directory	Users	2
Tenant ID	0c2edecf-6c76-428f-ab0f-28ce625e6ee9	Groups	0
Primary domain	adminstgssupport.onmicrosoft.com	Applications	1
License	Microsoft Entra ID Free	Devices	0

Alerts

3. Search for “Gainsight SAML” and select the application.



Home > Default Directory | Overview >

Browse Microsoft Entra App Gallery ···

+ Create your own application | Got feedback?

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the Microsoft Entra App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra App Gallery for other organizations to discover and use, you can file a request using the process described in this article.

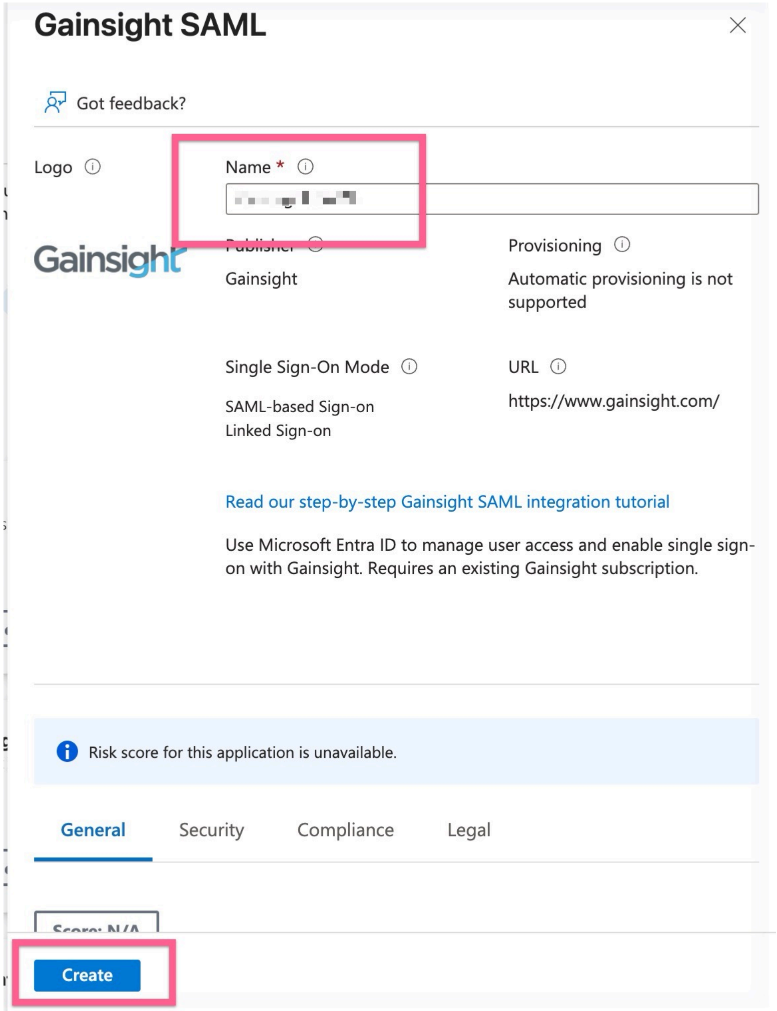
Search: gainsight saml

Single Sign-on : All
User Account Management : All
Categories : All
Risk Score : All
Security Risk Factors : All
Compliance Risk Factors : All
Federated SSO
Provisioning

Showing 46 of 46 results

Application	Publisher	Risk score
Gainsight SAML	Gainsight	Risk score not available
Insight	Insight	Risk score not available
Insights	The Insights Group Limited	Risk score not available
GA Insights	GA Insights	Risk score not available

4. Provide a name to the application and click on “create”.



Gainsight SAML

Logo

Name * [redacted]

Publisher: Gainsight

Provisioning: Automatic provisioning is not supported

Single Sign-On Mode: SAML-based Sign-on
Linked Sign-on

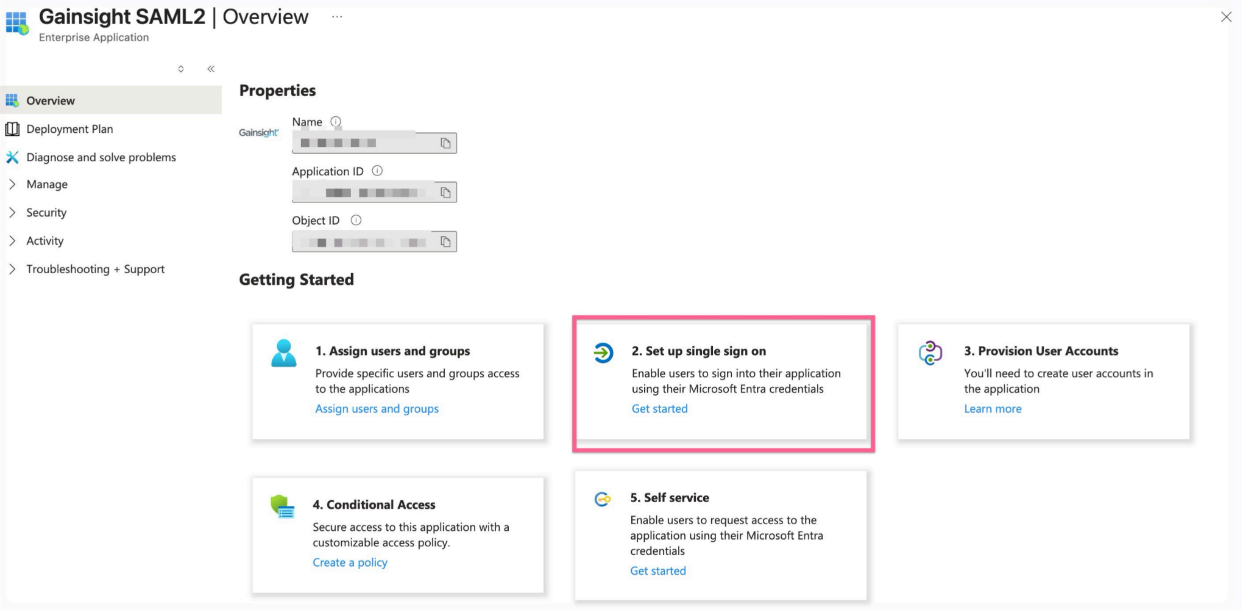
URL: https://www.gainsight.com/

Read our step-by-step Gainsight SAML integration tutorial

Use Microsoft Entra ID to manage user access and enable single sign-on with Gainsight. Requires an existing Gainsight subscription.

Risk score for this application is unavailable.

5. Open the application and Select “Set up single sign on”



Gainsight SAML2 | Overview ···

Enterprise Application

Properties

Name [redacted]

Application ID [redacted]

Object ID [redacted]

Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

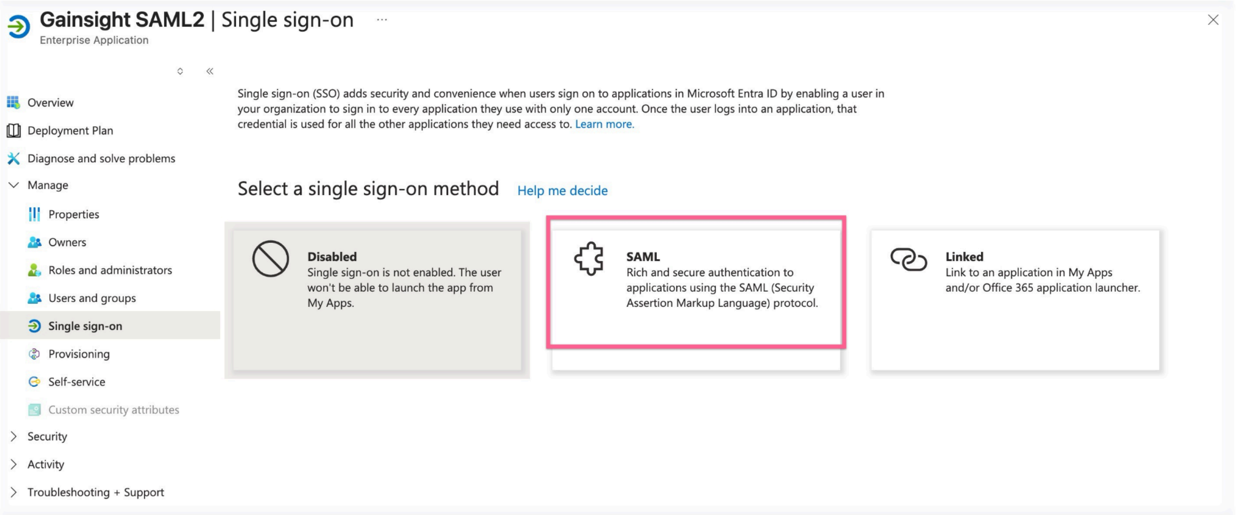
2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

3. Provision User Accounts
You'll need to create user accounts in the application
Learn more

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Microsoft Entra credentials
Get started

6. Then select “SAML”.



Gainsight SAML2 | Single sign-on ···

Enterprise Application

Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. Learn more.

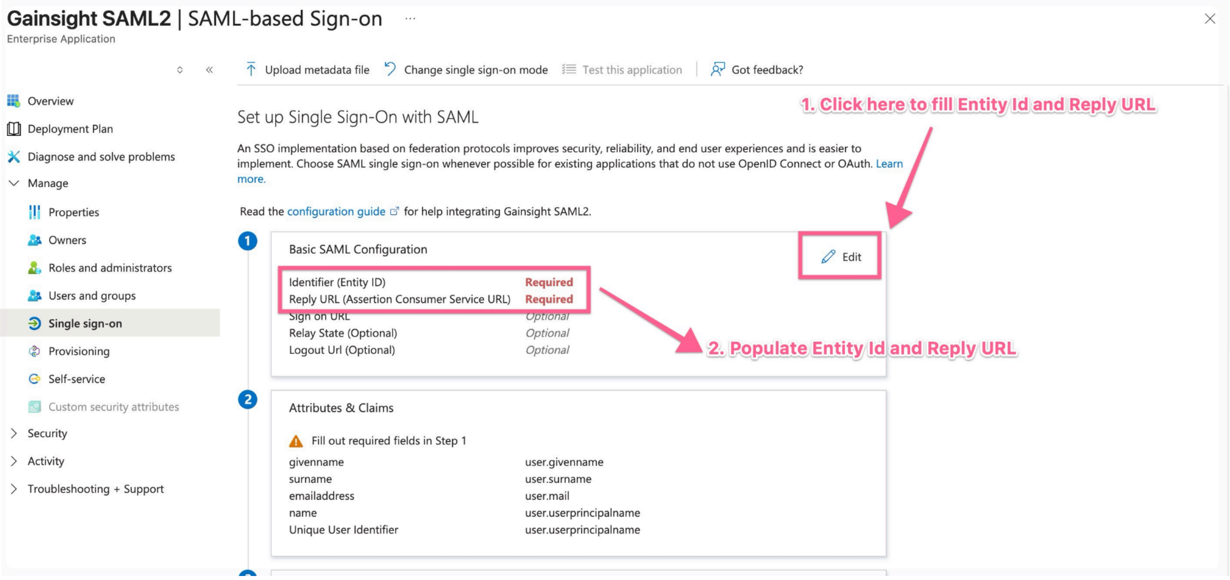
Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Linked
Link to an application in My Apps and/or Office 365 application launcher.

7. In “Basic SAML Configuration”, click on Edit and fill Entity ID and Reply URL


Gainsight SAML2 | SAML-based Sign-on
Enterprise Application
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
Overview
Deployment Plan
Diagnose and solve problems
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes
Security
Activity
Troubleshooting + Support
Edit
1. Click here to fill Entity Id and Reply URL
2. Populate Entity Id and Reply 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 Gainsight SAML2.

1 Basic SAML Configuration

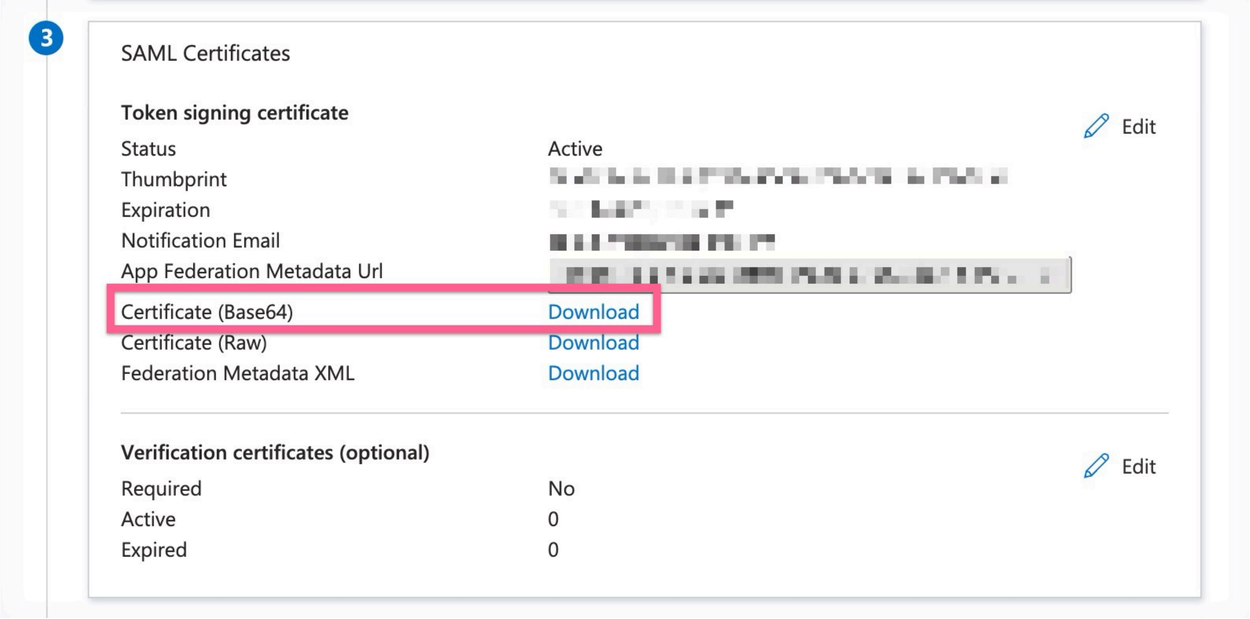
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

2 Attributes & Claims

Fill out required fields in Step 1

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

8. Navigate to Step 3, download the Certificate(Base64).



3 SAML Certificates

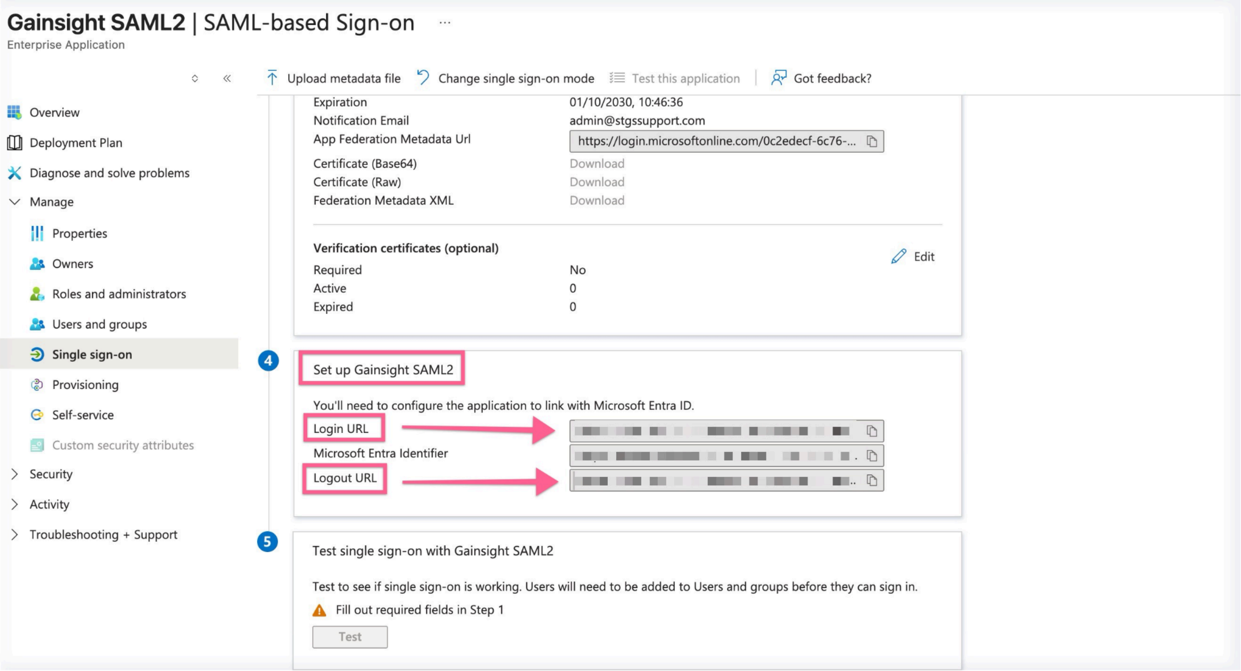
Token signing certificate

Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

9. Then navigate to Step 4 in the same page and copy Login URL and Logout URL



Expiration	01/10/2030, 10:46:36
Notification Email	admin@stgssupport.com
App Federation Metadata Url	https://login.microsoftonline.com/0c2edecf-6c76-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

Set up Gainsight SAML2

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

Login URL	[redacted]
Microsoft Entra Identifier	[redacted]
Logout URL	[redacted]

Test single sign-on with Gainsight SAML2

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

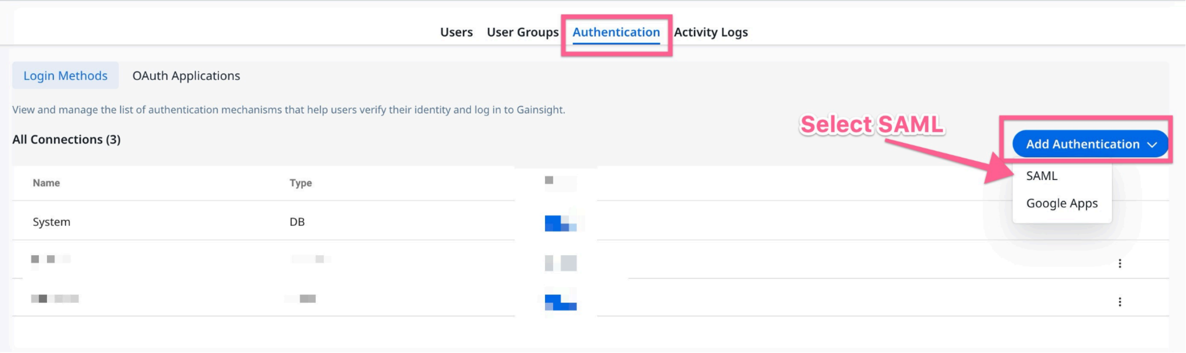
⚠ Fill out required fields in Step 1

Notes:

1. Make sure the user is assigned to the app and try logging in on GS Side.
2. User Attribute & Claims, check for claim name if they want to use something different. You can add a new claim if you want. You can use url or attribute name="<copy this>"

Gainsight:

1. Navigate to User management -> Authentication -> Click on “Add Authentication” and select SAML.

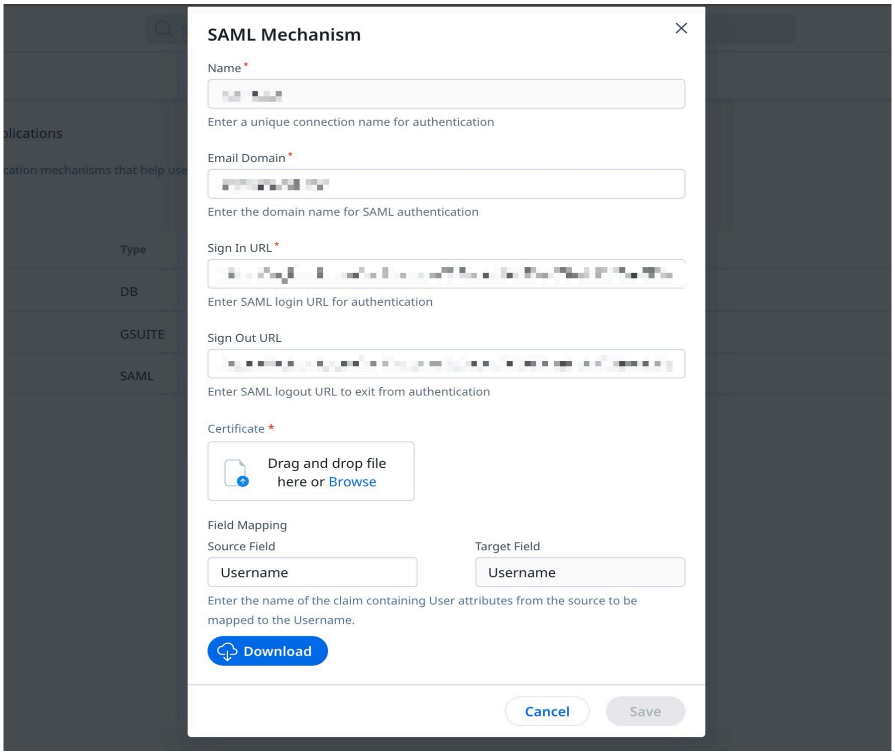


View and manage the list of authentication mechanisms that help users verify their identity and log in to Gainsight.

All Connections (3)

Name	Type	
System	DB	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

2. Below form opens up.


plications
cation mechanisms that help use
Type
DB
GSUITE
SAML
×
Drag and drop file here or Browse
Download
Cancel
Save

SAML Mechanism

Name *
[redacted]
Enter a unique connection name for authentication

Email Domain *
[redacted]
Enter the domain name for SAML authentication

Sign In URL *
[redacted]
Enter SAML login URL for authentication

Sign Out URL
[redacted]
Enter SAML logout URL to exit from authentication

Certificate *

Field Mapping

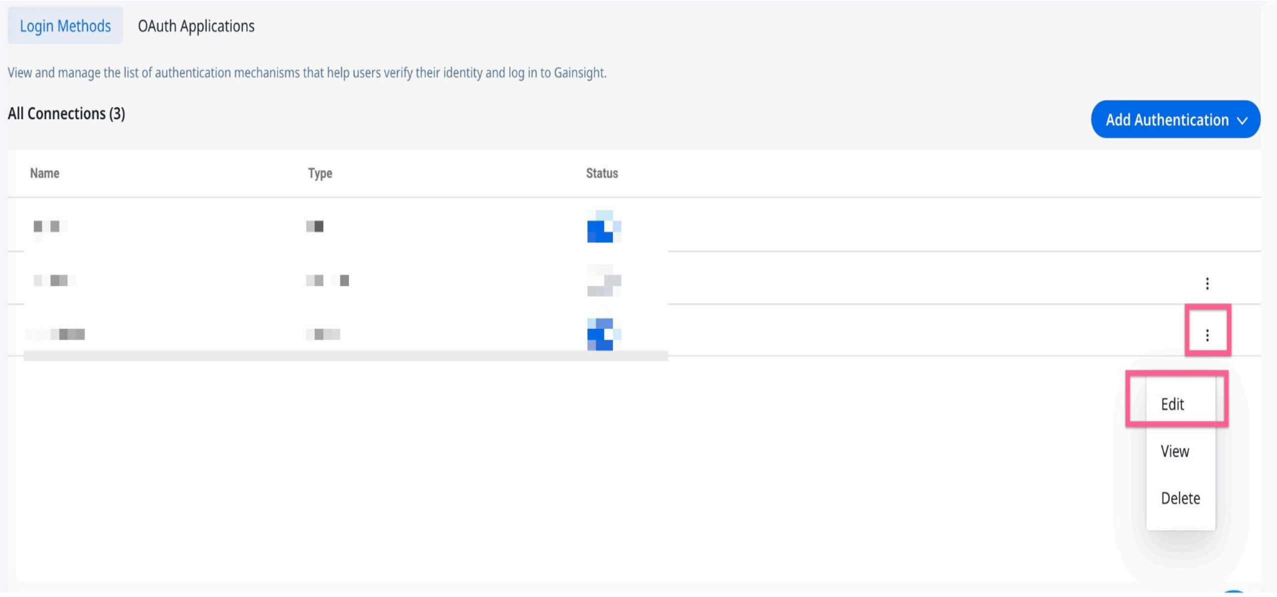
Source Field	Target Field
Username	Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username.

Name: Give any unique name other than existing methods.
Email domain: Enter domain which matches with User email.
Sign In URL: Fill Login URL from step 8 under Azure section.
Sign Out URL: Fill Logout URL from step 8 under Azure section.
Certificate: Upload the file which is downloaded from Azure in Step 7 under Azure section.
Field Mapping: Let it be Username(Do not make any changes).

Click “Save”

3 Once saved, go to the list and click on ellipsis as in the below screenshot and click “Edit”

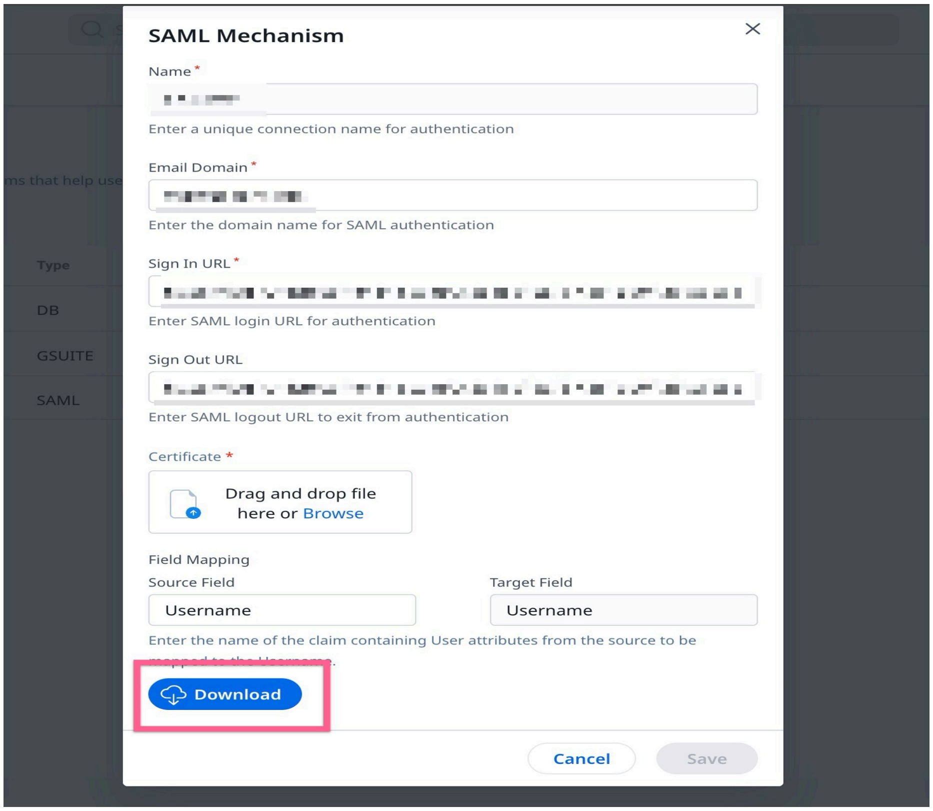


View and manage the list of authentication mechanisms that help users verify their identity and log in to Gainsight.

All Connections (3)

Name	Type	Status
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

4. Click on the “Download” option to get the metadata file.



SAML Mechanism

Name *
[redacted]
Enter a unique connection name for authentication

Email Domain *
[redacted]
Enter the domain name for SAML authentication

Sign In URL *
[redacted]
Enter SAML login URL for authentication

Sign Out URL
[redacted]
Enter SAML logout URL to exit from authentication

Certificate *
Drag and drop file here or Browse

Field Mapping
Source Field: Username
Target Field: Username
Enter the name of the claim containing User attributes from the source to be mapped to the Username.

5. Once downloaded, open the file in any text editor and search for below Occurrences.
   1. **entityID**
      It’s value would be something like “`urn:auth0:gainsight:<ID>`”
   2. **AssertionConsumerService**
      It’s value would be something like “`https://secured.gainsightcloud.com/login/callback connection=<ID>`”

6. In Azure, Navigate to the “Basic SAML Configuration” and make below changes.
   1. Identifier (Entity ID): update with **entityID** from step 5.
   2. Reply URL (Assertion Consumer Service URL):
      update with **AssertionConsumerService** from step 5 and save it.